



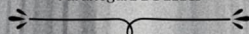
A M A N D A

سامانه هوشمند پایش تصویری

آماندا



Intelligent Processing
Paranegar Homa



۱۴۰۴



A M A N D A[®]

محصول دانش بنیان

قدرت گرفته از هوش مصنوعی



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



فهرست

بخش اول معرفی ۳

۴ مقدمه (۱)

۵ (۱-۱) مدیریت دوربین‌ها و تصاویر ضبط شده

۵ (۲-۱) برپایی فنس مجازی

۶ (۳-۱) تشخیص انواع اشیاء و اهداف

۸ (۴-۱) تشخیص و شناسایی هویت از روی چهره

۹ (۵-۱) تشخیص انواع اسلحه

۱۱ (۶-۱) تشخیص اشیاء پرنده

۱۲ (۷-۱) تشخیص دود و آتش

۱۳ (۸-۱) تشخیص به سر نداشتن کلاه ایمنی

۱۴ (۹-۱) شمارش افراد و تشخیص تجمع

۱۵ (۱۰-۱) تشخیص پلاک و پلاک‌خوانی

۱۶ (۱۱-۱) باز-ارسال تصاویر و ایجاد محدودیت در دسترسی مستقیم به دوربین‌ها

۱۷ (۱۲-۱) معماری، انعطاف‌پذیری و مقیاس‌پذیری

۱۷ (۱-۱۲-۱) ویژگی‌ها و مزایای استفاده از معماری توزیع شده

۱۸ (۱۳-۱) زیرسامانه‌های هشدار

۱۹ (۱۴-۱) آمار و گزارش‌گیری

۱۹ (۱۵-۱) ایجاد کیوسک‌های متعدد برای ثبت ورود-خروج

۲۰ (۱۶-۱) ویژگی‌های فنی سامانه

۲۱ (۱۷-۱) ویژگی‌های کاربردی سامانه

بخش دوم: راهنمای نسخه سرور سامانه ۲۵

۲۶ مقدمه (۲)

۲۷ (۱-۲) راه‌اندازی سرویس‌ها

۲۸ (۲-۲) معرفی ناحیه (زون) و واحد (یونیت)

۳۰ (۳-۲) تعریف و اتصال به دوربین‌ها

۳۵ (۱-۳-۲) بارگذاری فایل ویدیویی به جای دوربین

۳۸ (۴-۲) ایجاد نقشه و چیدن دوربین‌ها روی نقشه

۴۲ (۵-۲) تنظیمات مربوط به مدیریت ویدیوها و تصاویر



۴۳.....	۶-۲) بازپخش ویدیوهای ضبط شده
۴۴.....	۷-۲) برایایی فنس مجازی و فعال سازی هوش مصنوعی
۴۹.....	۸-۲) راهنمای ثبت نام اشخاص شناس (کارمندان-پرسنل)
۵۰.....	۸-۲-۱) راهنمای ثبت نام گروهی اشخاص با استفاده از فایل اکسل
۵۳.....	۲-۸-۲) ثبت نام مجزای اشخاص
۵۹.....	۹-۲) افزودن و ویرایش کاربر
۶۲.....	۱۰-۲) آمار و گزارش گیری
۶۳.....	۱۱-۲) راه اندازی کیوسک

۱۲-۲) ملاحظات کلیدی برای افزایش دقت و کارایی سامانه آماد..... ۶۵

۶۶.....	۱-۱۲-۲) بکارگیری توان پردازشی GPU
۶۶.....	۲-۱۲-۲) الزامات دوربین های نظارت محیطی
۶۶.....	۳-۱۲-۲) الزامات دوربین های پلاک خوان
۶۷.....	۴-۱۲-۲) الزامات دوربین های تشخیص و شناسایی چهره
۶۷.....	۵-۱۲-۲) شرایط نمونه برداری از چهره اشخاص
۶۸.....	۶-۱۲-۲) راهنمای تنظیمات مربوط به نوع تشخیص
۷۳.....	۷-۱۲-۲) انتخاب نوع جریان
۷۳.....	۸-۱۲-۲) نکات تکمیلی

بخش سوم: راهنمای نسخه ناظر سامانه ۷۴

۷۵.....	۳) مقدمه
۷۵.....	۱-۳) ورود به حساب کاربری
۷۶.....	۲-۳) تنظیمات
۷۸.....	۳-۳) تعریف ابزارهای هشدار و قوانین امنیتی
۸۱.....	۴-۳) اجرا
۸۶.....	۵-۳) ثبت نام برخط اشخاص

بخش اول

معرفی



(۱) مقدمه

پایش، نظارت و کنترل مکان‌ها و محدوده‌های امنیتی و شناسایی عوامل تهدیدآمیز و غیرطبیعی در این نواحی، از مهم‌ترین وظایف دستگاه‌های مختلف از جمله وزارتخانه‌ها، سازمان‌ها و ارگان‌ها است. این اقدامات نقش بسزایی در افزایش ضریب امنیت دارند. امروزه تلاش می‌شود با استفاده از فناوری‌های پیشرفته نرم‌افزاری و سخت‌افزاری، به بیشینه کارایی در این زمینه دست یافت.

استفاده از دوربین‌های مداربسته یکی از روش‌های متداول نظارت و کنترل است. اما علی‌رغم پیشرفت‌ها و دستاوردهای چشمگیر در این حوزه، فرآیند نظارت تصویری در بسیاری از مراکز داخل کشور همچنان به شیوه‌های سنتی و مبتنی بر عملکرد ناظر یا ناظران در اتاق مانیتورینگ انجام می‌شود. به عبارت دیگر، تحلیل و بررسی تصاویر ثبت شده توسط این دوربین‌ها و تصمیم‌گیری به موقع در واکنش به فعالیت‌های مشاهده شده، کاملاً به دقت و کارایی ناظر وابسته است. بدیهی است با افزایش تعداد دوربین‌ها و پیچیدگی وظایف نظارتی، توانایی ناظران به شدت کاهش می‌یابد. این کاهش می‌تواند منجر به موارد متعدد نقض قوانین حراستی و امنیتی شود. افزون بر این، عواملی مانند خستگی، خواب‌آلودگی، حواس‌پرتی یا ترک اتاق مانیتورینگ برای انجام امور شخصی، کارایی چنین سیستم‌هایی را زیر سؤال می‌برد. همچنین در برخی موارد، مانند حفاظت از سایت‌های خارج از محدوده شهری یا نواحی دورافتاده و پرخطر نظیر مرزها، امکان حضور مستمر و مداوم ناظر وجود ندارد. از این رو، ضروری است با بهره‌گیری از فناوری‌های پیشرفته، عملیات نظارت و کنترل را هوشمند کرده و به حداکثر کارایی دست یافت.

در این راستا، شرکت هوشمند پردازان فرانگر هما با افتخار سامانه هوشمند پایش تصویری خود تحت عنوان **آماندا^۱** را معرفی می‌نماید. این سامانه کاملاً بومی و دانش‌بنیان بوده و از قابلیت‌های بی‌نظیری برخوردار است. بومی بودن سامانه آماندا سه مزیت بسیار مهم و ارزشمند را به ارمغان می‌آورد:

(۱) امکان شخصی‌سازی-سفارشی‌سازی سامانه منطبق بر نیازمندی‌های کارفرما

(۲) امکان افزودن قابلیت تشخیصی جدید بر اساس نیاز کارفرما

(۳) امکان بررسی کدهای منبع برای حصول اطمینان از:

- عدم نشست-سرقت اطلاعات از جمله اطلاعات مربوط به دوربین‌ها و تصاویر ثبت شده
- عدم وجود بدافزار^۲
- عدم وجود بمب‌های ساعتی^۳

^۱ آماندا در زبان آذری به معنی «در امان ماندن» است.

^۲ Malware

^۳ Logic Bomb



این سامانه، به عنوان یک راه حل جامع و نوآورانه، برای نخستین بار در ایران بر پایه جدیدترین دستاوردهای علمی در حوزه فناوری اطلاعات و هوش مصنوعی طراحی و توسعه یافته است. این سیستم یکپارچه، علاوه بر ارائه مدیریت و نظارت تصویری پیشرفته، طیف گسترده‌ای از قابلیت‌های هوشمندسازی را نیز در اختیار کاربران قرار می‌دهد. در ادامه، قابلیت‌های متنوع و منحصر به فرد این سامانه معرفی خواهند شد که آن را به انتخابی بی‌رقیب برای مدیریت پیشرفته و هوشمند سیستم‌های نظارتی تبدیل می‌کند.

۱-۱) مدیریت دوربین‌ها و تصاویر ضبط شده

برای دستیابی به حداکثر کارایی در سامانه‌های نظارت تصویری، نخستین و مهم‌ترین گام، ایجاد بستری است که در آن کاربر بتواند به سادگی دوربین‌های متعدد موجود در سیستم را مدیریت کند، تصاویر ارسال شده از آنها را به صورت ویدئویی ضبط و در مواقع لازم بازپخش نماید. علاوه بر این، امکاناتی نظیر نمایش تصاویر دریافتی بر روی مانیتورهای مجزا در روی ویدیووال^۱، مشاهده وضعیت دوربین‌ها روی نقشه، ارسال تصاویر دریافت شده از طریق شبکه یا بستر وب برای مشاهده آنلاین از راه دور، از دیگر ویژگی‌های مهم چنین سامانه‌هایی به شمار می‌روند.

ما مفتخریم که تمامی این قابلیت‌ها را به شکلی بهینه و کارآمد در سامانه **آماندا** پیاده‌سازی و توسعه داده‌ایم، به گونه‌ای که کاربران با حداقل آشنایی با چنین سیستم‌هایی، می‌توانند بدون درگیر شدن با پیچیدگی‌های فنی رایج، از امکانات متنوع بخش مدیریت تصاویر (VMS^۲) این سامانه بهره‌مند شوند. این امکانات شامل تعریف دوربین‌ها، تنظیمات مربوط به ضبط تصاویر، ایجاد گروه‌های ضبط، جستجو و بازپخش ویدئوهای ضبط شده، تعریف نقشه و جانمایی دوربین‌ها روی آن، مشاهده تصاویر و وضعیت فعلی دوربین‌ها از طریق نقشه، تعریف کاربران با سطوح دسترسی متفاوت، باز-ارسال^۳ تصاویر روی بستر شبکه و اینترنت است.

۱-۲) برپایی فنس مجازی

استفاده از فنس‌های فلزی و سیم‌های خاردار، رویکردی متداول در حفاظت فیزیکی برای جلوگیری از ورود غیرمجاز به حریم‌های ممنوعه است. با این حال، هزینه خرید، نصب و نگهداری چنین تجهیزات سخت‌افزاری بسیار بالاست و با گذر زمان این هزینه‌ها به طور قابل توجهی افزایش می‌یابد.

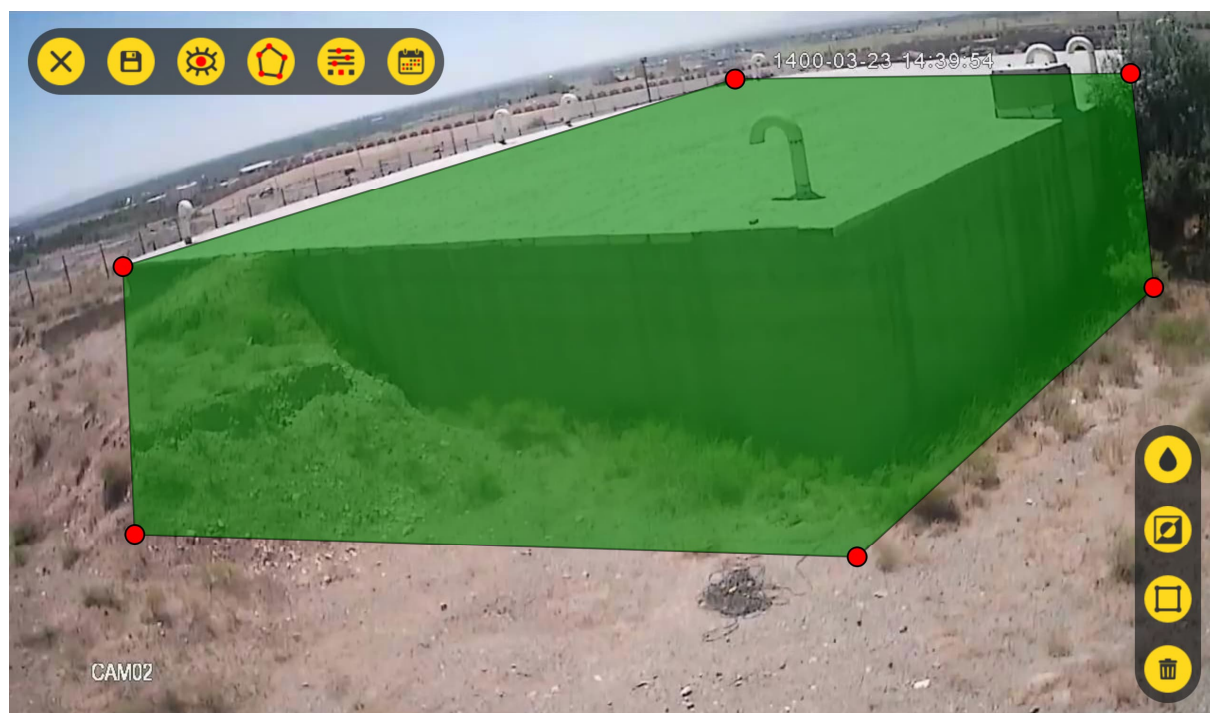
سامانه آماندا امکان تعریف و برپایی فنس‌های مجازی را به سادگی و تنها با چند کلیک در میدان دید دوربین مورد نظر فراهم می‌کند. کاربران می‌توانند این محدوده‌ها را مطابق با نیاز خود تعریف کرده و سامانه را نسبت به هرگونه نقض قوانین حفاظتی در این محدوده‌ها حساس سازند. این رویکرد نه تنها نیاز به خرید و نصب تجهیزات سخت‌افزاری گران‌قیمت را به طور کامل برطرف می‌کند، بلکه دقت و انعطاف‌پذیری بیشتری

^۱ Video Wall

^۲ Video Management System

^۳ Restream

در مدیریت حریم‌های ممنوعه به کاربران ارائه می‌دهد. شکل ۱-۱ نمونه‌ای از فنس مجازی ایجاد شده توسط کاربر را که به رنگ سبز نمایان شده است، نشان می‌دهد.



شکل ۱-۱: نمونه‌ای از حریم (فنس مجازی) ایجاد شده در سامانه آماندا (منطقه سبز رنگ)

۳-۱) تشخیص انواع اشیاء و اهداف

تشخیص سریع و به موقع تجاوز به حریم‌های ممنوعه، یکی از مهم‌ترین مؤلفه‌های حفاظت محیطی به شمار می‌رود. در روش‌های سنتی، از دستگاه‌های الکترونیکی و مکانیکی نظیر سنسورهای حساس به صدا، دما و لرزش استفاده می‌شود. این رویکردها علاوه بر هزینه‌های سنگین برای خرید و نگهداری تجهیزات، از دقت و کارایی کافی برخوردار نیستند.

در روش‌های مدرن‌تر، پردازش تصویر به‌عنوان یک راهکار جایگزین مورد توجه قرار گرفته است. در این روش، سامانه با تحلیل تصاویر دریافتی، حرکات‌های داخل حریم را شناسایی می‌کند. اما از آنجا که این سامانه‌ها قادر به تشخیص منشأ حرکت نیستند، رخدادهایی مانند لرزش دوربین، عبور جوندگان، حرکت برگ درختان یا حشرات کوچک منجر به فعال شدن بخش هشدار می‌شوند. این هشدارهای کاذب باعث کاهش اقبال عمومی به این نوع سامانه‌ها شده است.

ما مفتخریم که با استفاده از پیشرفته‌ترین فناوری‌های هوش مصنوعی، سامانه آماندا را قادر ساخته‌ایم تا اشیاء مختلف را با دقت بسیار خوبی تشخیص داده و بر اساس نوع شیء وارد شده به حریم، واکنش مناسب نشان دهد.

در حال حاضر، سامانه آماندا توانایی تشخیص بیش از ۵۰ نوع شیء مختلف از جمله انسان، چهارپا، پرنده، وسایل نقلیه و... را دارد و می‌تواند بر حسب نیاز، اشیاء و اهداف جدیدی را نیز یاد بگیرد. در شکل ۱-۲، نمونه‌ای از قابلیت سامانه آماندا در تشخیص انسان، حیوان و خودرو در تصاویر ثبت‌شده توسط دوربین‌های مداربسته نمایش داده شده است.



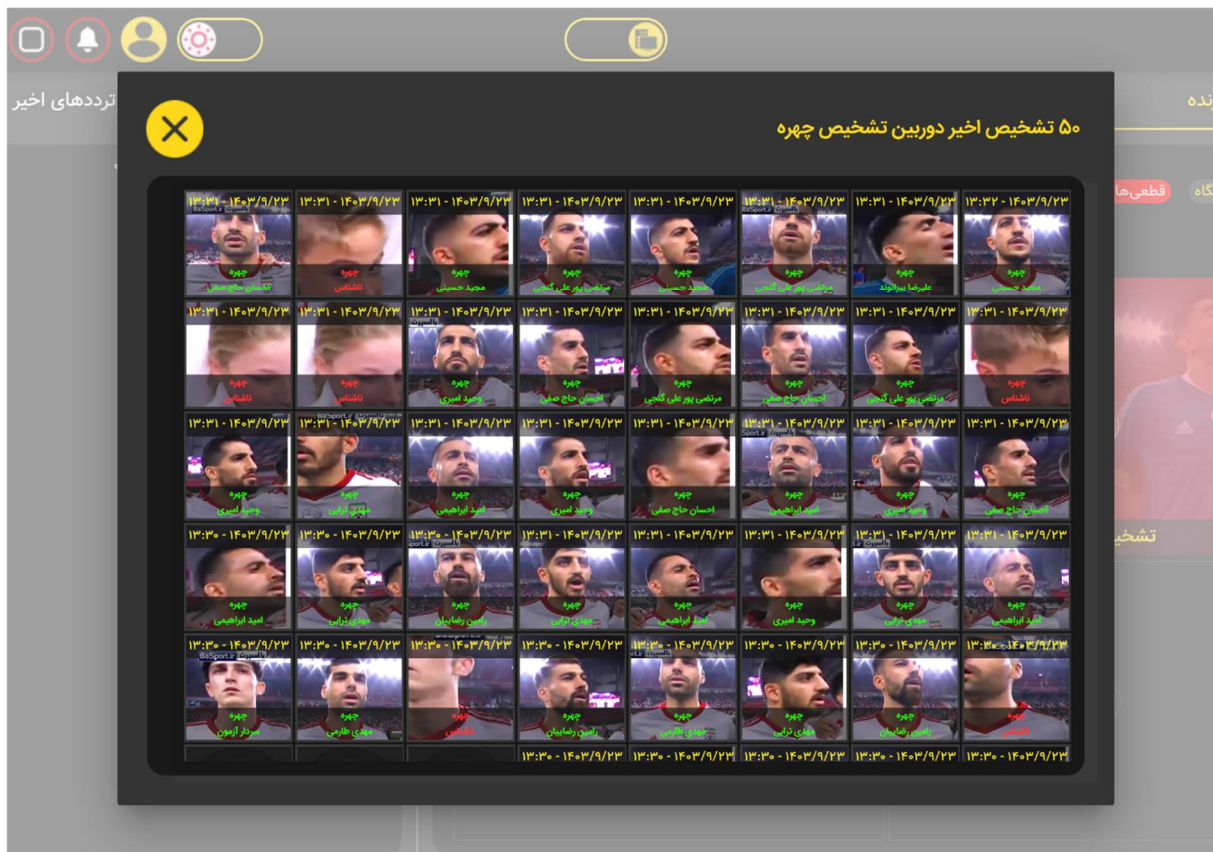


شکل ۱-۲: نمونه‌ای از توانایی سامانه آماندا در تشخیص اشیاء مختلف

۴-۱) تشخیص و شناسایی هویت از روی چهره

تشخیص هویت از طریق چهره یکی از فناوری‌های نوظهور است که در آن، فرآیند تطبیق و شناسایی افراد از روی تصاویر چهره انجام می‌شود. این فناوری معمولاً برای احراز هویت کاربران و کارکنان یا شناسایی افراد ناشناس به کار گرفته می‌شود. در سامانه آماندا، با بهره‌گیری از جدیدترین دستاوردهای این حوزه، فرآیند تشخیص چهره با دقتی فوق‌العاده و کارایی بسیار بالا حتی در شرایطی مانند چرخش سر یا حالات مختلف چهره امکان‌پذیر شده است. این سامانه قادر است تعداد زیادی از چهره‌های موجود در تصاویر دریافتی را به صورت هم‌زمان کشف و شناسایی کند.

با تعریف لیستی از کارکنان یا افراد مجاز در سامانه و حساس کردن آن نسبت به افراد ناشناس، می‌توان اطمینان حاصل کرد که هرگونه تلاش برای ورود افراد ناشناس به مناطق ممنوعه شناسایی شده و هشدارهای لازم صادر می‌شود.

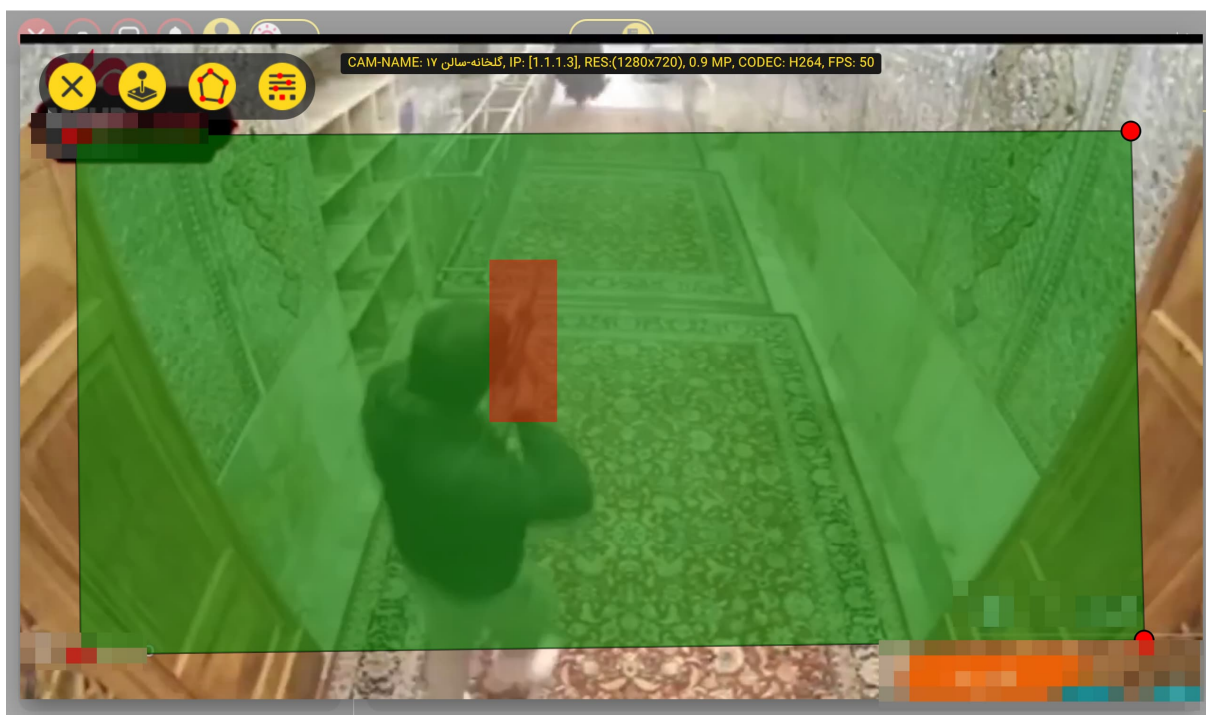


شکل ۳-۱: نمونه‌ای از توانایی سامانه آماد در تشخیص هویت افراد از روی چهره

نمونه‌ای از عملکرد سامانه در شکل ۳-۱ نشان شده است. در این نمونه، یک تصویر تصادفی از چهره‌های بازیکنان تیم ملی فوتبال با جستجو در اینترنت جمع‌آوری و برای آموزش به سامانه داده شده‌اند. همان‌طور که مشاهده می‌شود، سامانه توانسته است افراد را حتی با تغییرات اساسی در ظاهرشان (مانند گذر سن، چرخش سر و تغییرات نورپردازی) با دقت بسیار بالا تشخیص دهد.

۵-۱) تشخیص انواع اسلحه

تشخیص اینکه آیا افراد در مکان‌های حساس مسلح هستند یا خیر، موضوعی بسیار حیاتی است و می‌تواند نشان‌دهنده تهدیدات امنیتی باشد. در چنین شرایطی، افزایش آگاهی تیم امنیتی برای واکنش به موقع و مناسب به این تهدیدات، ضروری است. در موقعیت‌های بالقوه تیراندازی، زمان عاملی تعیین‌کننده است و کاهش زمان واکنش به معنای نجات جان افراد بیشتر و جلوگیری از پیامدهای جبران‌ناپذیر خواهد بود.





شکل ۱-۴: نمونه‌ای از عملکرد آماندا در تشخیص اسلحه در حالت‌های مختلف

سامانه آماندا مجهز به ماژولی اختصاصی برای شناسایی سلاح در صحنه‌های شلوغ است. این فرآیند با استفاده از الگوریتم‌های پیشرفته هوش مصنوعی انجام می‌شود و سامانه توانایی تشخیص انواع متداول سلاح‌ها در تصاویر و ویدئوها را دارد و هشدارهای لازم را به موقع صادر می‌کند. در شکل ۱-۴، عملکرد آماندا در شناسایی انواع مختلف سلاح در موقعیت‌های گوناگون و با زوایای مختلف به نمایش درآمده است. این توانایی سامانه نقش مهمی در افزایش ایمنی و پیشگیری از وقایع ناگوار ایفا می‌کند.

۱-۶) تشخیص اشیاء پرنده

در سال‌های اخیر، استفاده از پهپادها و هلی‌شات‌ها برای انجام عملیات جاسوسی یا تخریبی به شکل چشمگیری افزایش یافته است. با وجود اینکه رادارها ابزار موثری برای شناسایی هواپیماها هستند، اما این فناوری به دلیل هزینه‌های بسیار بالا، برای تشخیص پهپادها چندان مقرون به صرفه نیست. علاوه بر این، ارتفاع پایین پرواز پهپادها، امکان شناسایی آن‌ها توسط رادار را به شدت کاهش می‌دهد. از این رو، حفاظت از حریم هوایی در برابر تجاوز این اشیاء پرنده، به‌ویژه در مناطق وسیع، به یکی از چالش‌های جدی تیم‌های حفاظتی تبدیل شده است.

خوشبختانه، این چالش در سامانه آماندا به شکلی کارآمد برطرف شده است. این سامانه با بهره‌گیری از هوش مصنوعی پیشرفته، تصاویر دریافت‌شده از دوربین‌ها را تحلیل کرده و انواع مختلف پهپادها و اشیاء پرنده را با دقت و سرعت بالا شناسایی می‌کند. در شکل ۱-۵، نمونه‌ای از توانایی سامانه آماندا در شناسایی انواع پهپادها و هلی‌شات‌ها در شرایط جوی مختلف و در ارتفاعات پروازی گوناگون به تصویر کشیده شده است. این قابلیت نقشی حیاتی در ارتقای امنیت و پیشگیری از تهدیدات هوایی ایفا می‌کند.



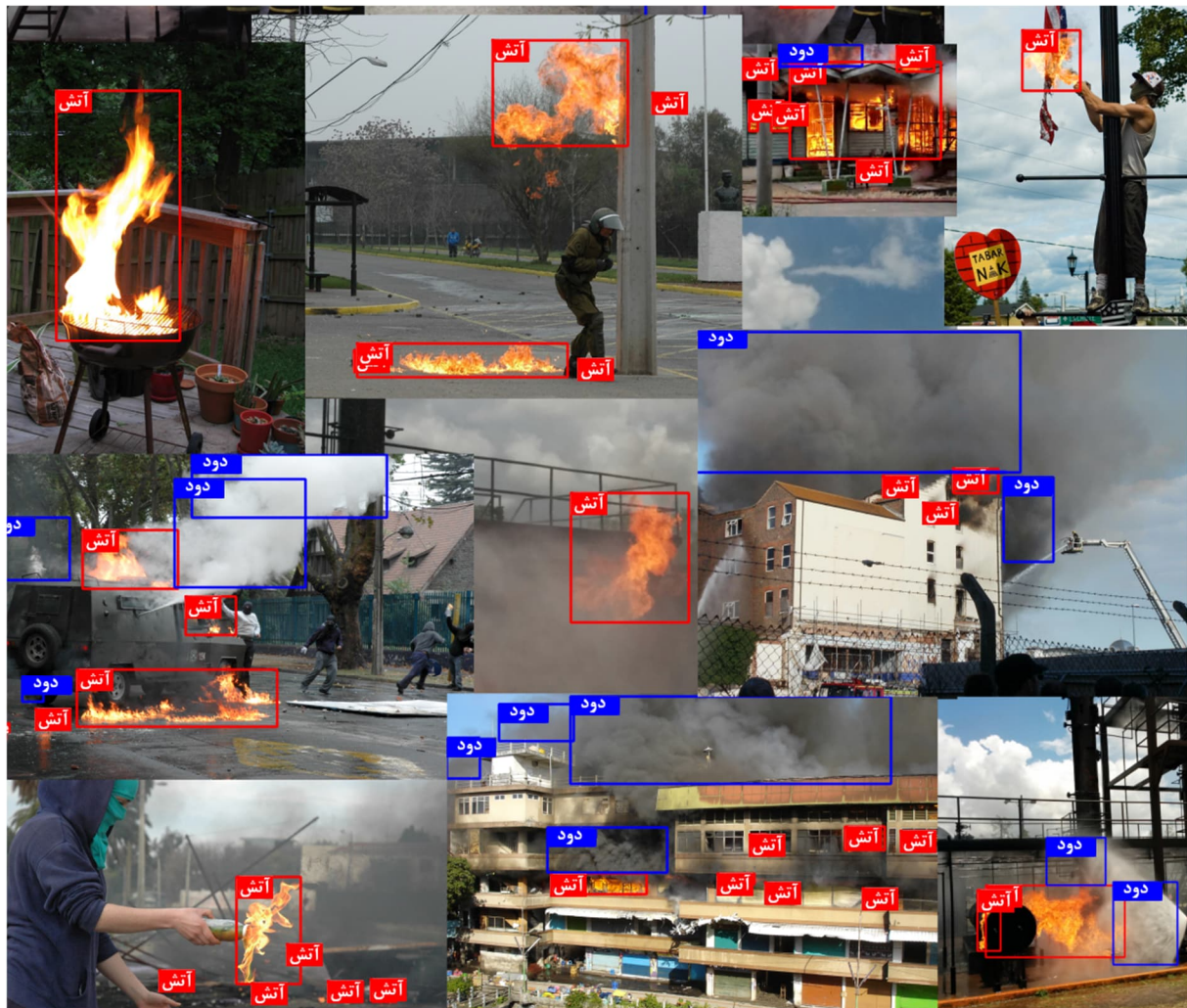
شکل ۱-۵: نمونه‌های از اشیای پرنده شناسایی شده توسط سامانه آماندا

۱-۷) تشخیص دود و آتش

یکی از مهم‌ترین دغدغه‌های بخش بهداشت و ایمنی هر سازمان (^۱HSE)، پیشگیری از وقوع آتش‌سوزی است. استفاده از سنسورهای حساس به دما و دود، روشی رایج برای شناسایی آتش‌سوزی محسوب می‌شود. با این حال، هزینه خرید، نصب، و نگهداری این سنسورها بسیار بالاست و برای پوشش مناطق وسیع مستعد آتش‌سوزی، به تعداد زیادی از این سنسورها نیاز خواهد بود که از نظر اقتصادی و عملیاتی چالش‌برانگیز است.

سامانه آماندا، با بهره‌گیری از تجزیه و تحلیل دقیق تصاویر دریافتی و استفاده از هوش مصنوعی پیشرفته، قادر است انواع دود (سفید، سیاه، و خاکستری) و شعله‌های آتش را در تصاویر شناسایی کرده و با ارسال هشدارهای به‌موقع، از وقوع یا گسترش آتش‌سوزی جلوگیری کند. در شکل ۱-۶، نمونه‌ای از عملکرد سامانه در تشخیص دود و شعله‌های آتش به تصویر کشیده شده است که نشان‌دهنده کارایی بالای این سامانه در مدیریت ایمنی و کاهش خطرات آتش‌سوزی است.

^۱ Health, Safety, Environment



شکل ۱-۶: نمونه‌ای از توانایی سامانه آماندا در شناسایی دود و آتش

۱-۸) تشخیص به سر نداشتن کلاه ایمنی

علیرغم بازرسی‌های مختلف ایمنی که در طول سال‌ها برای اطمینان از رعایت مقررات و حفظ شرایط کاری قابل قبول و ایمن انجام شده است، شرایط حاکم در سایت‌های ساختمانی همچنان یکی از خطرناک‌ترین محیط‌های کاری به شمار می‌رود و یکی از دلایل اصلی تلفات کارگران نیز به همین موضوع مربوط می‌شود. به‌طور تقریبی، یک کارگر ساختمانی در طول ۴۵ سال فعالیت خود، به احتمال یک در ۲۰۰ ممکن است جان خود را به دلایل مختلفی نظیر آتش‌سوزی، سقوط، آسیب‌های جسمی، گرفتار شدن بین اجسام و... از دست بدهد. این موضوع تا حد زیادی به نظارت بر استفاده صحیح از تجهیزات حفاظتی فردی توسط بازرسان ایمنی بستگی دارد.

سامانه آماندا با هدف کاهش تلفات ناشی از عدم استفاده از کلاه ایمنی در حین کار، کارگرانی که کلاه ایمنی به سر ندارند را به‌سرعت شناسایی کرده و هشدارهای لازم را صادر می‌کند. در شکل ۱-۷، نمونه‌ای از دقت سامانه در تشخیص کارگرانی که کلاه ایمنی به سر دارند (مشخص شده با رنگ آبی) و کارگرانی که کلاه ایمنی ندارند (مشخص شده با رنگ قرمز) نشان داده شده است.



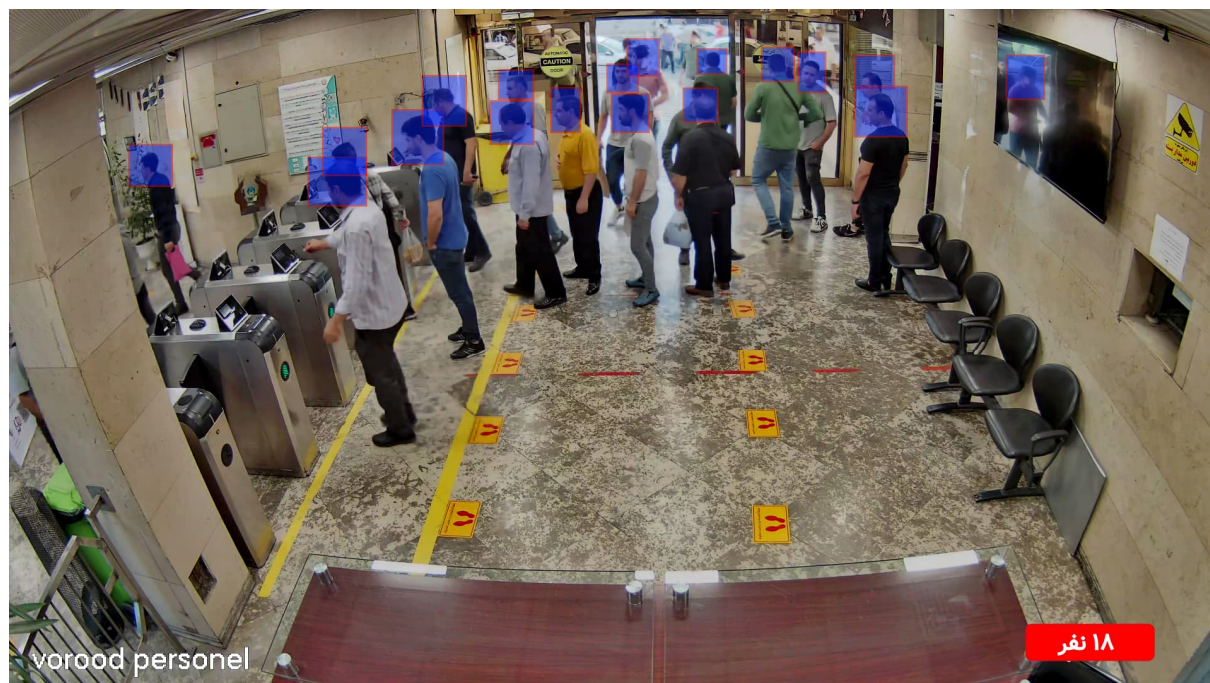
شکل ۷-۱: نمونه‌ای از کارایی سامانه آماندا در تشخیص به سر داشتن یا نداشتن کلاه ایمنی

۹-۱) شمارش افراد و تشخیص تجمع

با استفاده از هوش مصنوعی، امکان شمارش دقیق و تشخیص تجمعات در محیط‌های مختلف به‌طور چشمگیری بهبود یافته است. این تکنولوژی‌ها با دقت و سرعت بسیار بیشتر از انسان‌ها به‌طور مؤثر به ما کمک می‌کنند تا به‌طور دقیق و کامل به تراکم افراد و تجمعات آنها در مکان‌های مختلف پی ببریم.

در مواردی نظیر کنسرت‌ها، تظاهرات یا تجمعات اجتماعی، شمارش دقیق افراد به‌عنوان یک عامل اساسی در برنامه‌ریزی‌های امنیتی و مدیریت موقعیت‌ها اهمیت ویژه‌ای دارد. همچنین، در محیط‌های تجاری مانند فروشگاه‌ها و مراکز خرید، تشخیص تراکم افراد و تجمعات به مدیران این امکان را می‌دهد تا به‌موقع اقدامات لازم را در راستای بهبود دستورالعمل‌ها، مسیرها و پیشنهادات به مشتریان انجام دهند.

این قابلیت در سامانه آماندا به‌طور مطلوب پیاده‌سازی شده است، به‌گونه‌ای که پس از شناسایی تعداد معینی از افراد مجاز برای تشکیل یک تجمع حساس، هرگونه تجمع بیش از آن تعداد را کشف کرده و هشدارهای لازم را تولید می‌کند. شکل ۸-۱ نمونه‌ای از عملکرد سامانه در شمارش افراد را نشان می‌دهد.



شکل ۸-۱: نمونه‌ای از شمارش افراد در سامانه آماندا

۱-۱۰) تشخیص پلاک و پلاک‌خوانی

آگاهی از تردد خودروها و داشتن آماری دقیق از ورود و خروج و مدت زمان توقف آنها، یکی از چالش‌های اصلی نیروهای بازرسی محسوب می‌شود. همچنین، اطمینان از عدم ورود خودروهای غیرمجاز و ناشناس به مناطق حساس نیز از مشکلات جدی نیروهای بازرسی و حراست است. زمانی که تعداد و تنوع خودروها در حال تردد در محدوده زیاد شود، تشخیص خودروهای مجاز از غیرمجاز توسط نیروهای بازرسی بسیار دشوار و عملاً غیرممکن می‌شود. این چالش زمانی پیچیده‌تر می‌شود که امکان فنس کشی حریم (به دلیل شرایط جغرافیایی منطقه) برای جلوگیری از ورود خودروهای غیرمجاز وجود نداشته باشد.

برای رفع این مشکل، توانایی تشخیص پلاک و پلاک‌خوانی نیز به سامانه آماندا اضافه شده است. بدین ترتیب، با تعریف خودروهای مجاز، خودروهای ناشناس توسط سامانه شناسایی و هشدارهای لازم صادر خواهد شد. همچنین، همواره آماری از ورود، خروج و مدت زمان توقف خودروها در دسترس خواهد بود که می‌تواند به‌عنوان بخشی از فرآیند کنترل تردد مجموعه نقش مهمی ایفا کند. در شکل ۹-۱، نمونه‌ای از عملکرد سامانه در پلاک‌خوانی خودروها تحت زوایا و شرایط مختلف روشنایی نشان داده شده است.

۵۰ تشخیص اخیر دوربین پلاک (۱.۱.۱.۲)

۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۴۶ ن ۷۸۱ ۲۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۶۴ ن ۵۲۲ ۴۴	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۵۷ ن ۳۳۹ ۵۵	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۴۳ ن ۴۶۶ ۵۵	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۵۸ ن ۷۷۹ ۳۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۲۲ ن ۷۱۴ ۵۲	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۸۳ ن ۷۷۲ ۲۲	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۶۱ ن ۷۸۱ ۵۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۸۷ ن ۶۳۳ ۱۷
۴۶۵۷۸۱۲۰	۴۴۰۵۲۲۴۴	۵۷۴۳۹۹۵۵	۲۴۴۲۶۶۵۵	۵۸۳۷۷۹۴۰	۲۲۴۷۱۴۵۲	۸۳۲۷۲۶۴۴	۲۱۶۷۸۱۵۰	۸۷۴۶۳۲۷۲
پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس
۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۸۴ ن ۳۳۶ ۵۵	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۷۶ ن ۴۴۳ ۱۷۷	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۹۹ ن ۱۷۷ ۷۷	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۸۶ ن ۴۶۶ ۳۷	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۳۷ ن ۳۸۴ ۸۸	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۴۵ ن ۴۶۸ ۶۶	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۹۶ ن ۴۷۵ ۱۱۱	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۱۹ ن ۶۱۶ ۲۲	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۱۵ ن ۳۸۳ ۱۷۷
۸۴۰۳۲۶۵۵	۷۶۰۴۴۲۷۷	۹۹۶۱۷۷۷۷	۸۶۴۸۶۲۲۲	۳۷۲۲۴۸۸۸	۴۵۴۴۶۸۶۶	۹۶۴۴۷۵۱۱۱	۱۹۴۶۱۶۲۲	۱۵۲۵۲۷۷۷
پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس
۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۱۷ ن ۴۹۱ ۱۷۷	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۴۵ ن ۳۵۸ ۵۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۲۴ ن ۲۳۲ [تقواری]	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۳۱ ن ۵۷۸ ۵۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۵۴ ن ۲۲۱ ۴۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۹۶ ن ۲۲۱ ۱۹۹	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۷۷ ن ۲۳۱ ۴۴	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۷۷ ن ۳۴۵ ۴۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۹ [تقواری] ۸۲ ن ۴۶۸ ۱۵۵
۱۷۴۴۹۱۳۷	۴۵۳۲۵۹۵۰	۴۲۲۲۸۲۲۰	۳۱۴۵۷۸۵۰	۹۶۰۲۲۱۴۰	۵۲۲۲۶۱۹۹	۷۷۲۲۱۴۴۴	۷۷۲۰۳۴۵۴۰	۸۲۴۶۸۱۵۵
پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس
۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۹۹ ن ۹۷۵ ۱۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۵۴ ن ۴۴۸ ۵۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۱۵ ن ۱۶۱ [تقواری]	۱۴۰۴/۱/۵ - ۱۴۰۴/۸ [تقواری] ۴۴ ن ۴۹۸ ۹۹	۱۴۰۴/۱/۵ - ۱۴۰۴/۸ [تقواری] ۹۹ ن ۳۵۲ ۱۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۸ [تقواری] ۲۵ ن ۲۱۸ ۵۵	۱۴۰۴/۱/۵ - ۱۴۰۴/۸ [تقواری] ۶۶ ن ۲۶۸ ۴۴	۱۴۰۴/۱/۵ - ۱۴۰۴/۸ [تقواری] ۲۴ ن ۲۷۸ ۳۱	۱۴۰۴/۱/۵ - ۱۴۰۴/۸ [تقواری] ۳۸ ن ۶۳۷ ۱۲
۹۹۵۹۷۵۱۰	۵۴۴۴۲۸۵۰	۱۵۵۰۱۶۴۱۱	۴۴۴۴۹۸۹۹	۹۹۰۳۵۲۱۰	۲۵۴۲۱۸۵۵	۶۶۲۴۸۴۴۴	۲۴۰۲۷۸۳۱	۳۸۰۶۳۷۱۲
پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس	پلاک ناشناس
۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۵۴ ن ۵۵۱ ۲۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۳۳ ن ۱۶۷ ۲۲	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۷۳ ن ۷۳۳ ۴۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۵۲ ن ۴۴۵ ۱۱	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۲۳ ن ۸۷۹ ۴۰	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۴۶ ن ۴۴۴ ۴۴	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۲۱ ن ۷۵۸ ۱۱	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۳۷ ن ۷۵۲ ۱۱	۱۴۰۴/۱/۵ - ۱۴۰۴/۷ [تقواری] ۸۲ ن ۴۶

شکل ۱-۹: نمونه‌ای از توانایی سامانه آماندا در بلاکخوانی خودروه‌ها

۱-۱۱) باز-ارسال تصاویر و ایجاد محدودیت در دسترسی مستقیم به دوربین‌ها

امکان مشاهده تصاویر دوربین‌ها از کامپیوترهای دسکتاپ مستقل متصل به شبکه دوربین‌ها یا اینترنت، ویژگی بسیار جذابی است که همواره بخش‌ها و نهادهای نظارتی تمایل زیادی به استفاده از آن دارند. این ویژگی به ویژه در سامانه‌های نظارتی پیشرفته، به دلیل فراهم آوردن قابلیت نظارت آنلاین و لحظه‌ای بر وضعیت مناطق مختلف، از اهمیت بالایی برخوردار است. در سامانه آماداء، امکان دسترسی کاربران اتاق مانیتورینگ (ناظران) به تصاویر دوربین‌ها از طریق اپلیکیشن ناظر با توانایی کنترل دوربین‌ها ایجاد شده است. این قابلیت باعث می‌شود که ناظران بتوانند به راحتی به تصاویری که به طور زنده از دوربین‌ها ارسال می‌شود، بصورت غیر مستقیم و از طریق باز-ارسال تصاویر از سرور دسترسی داشته و در صورت نیاز، دوربین‌ها را برای گرفتن زاویه‌های مناسب و بهتر تنظیم کنند.

علاوه بر این، سایر کاربران نیز می‌توانند با استفاده از مرورگر وب، تصاویر دوربین‌هایی که دسترسی مجاز به آنها دارند را مشاهده کنند. این ویژگی باعث افزایش انعطاف‌پذیری و سهولت دسترسی به تصاویر در هر زمان و مکانی می‌شود. این امر به‌ویژه برای سازمان‌ها و نهادهایی که نیاز به نظارت مداوم و سریع بر موقعیت‌های مختلف دارند، بسیار مفید است.



تمامی این قابلیت‌ها با باز-ارسال تصاویر دریافتی در سرور از طریق شبکه محلی یا اینترنت، امکان‌پذیر شده است. این فرآیند امکان مشاهده و تحلیل داده‌های تصویری در زمان واقعی را برای ناظران فراهم می‌کند و می‌تواند در مواقع اضطراری یا برای بررسی‌های روزمره مفید باشد. این امکان نه تنها باعث افزایش کارایی و امنیت سیستم‌های نظارتی می‌شود، بلکه از لحاظ مدیریتی نیز امکان نظارت بیشتر و هوشمندتر را برای کاربران فراهم می‌آورد.

۱۲-۱) معماری، انعطاف‌پذیری و مقیاس‌پذیری

سامانه آماندا از دو معماری متفاوت پشتیبانی می‌کند:

(۱) **معماری متمرکز:** در این معماری تمامی فرآیندها از جمله مدیریت و نظارت تصویری و تشخیص‌های هوشمند بطور متمرکز در سرور انجام می‌گیرد.

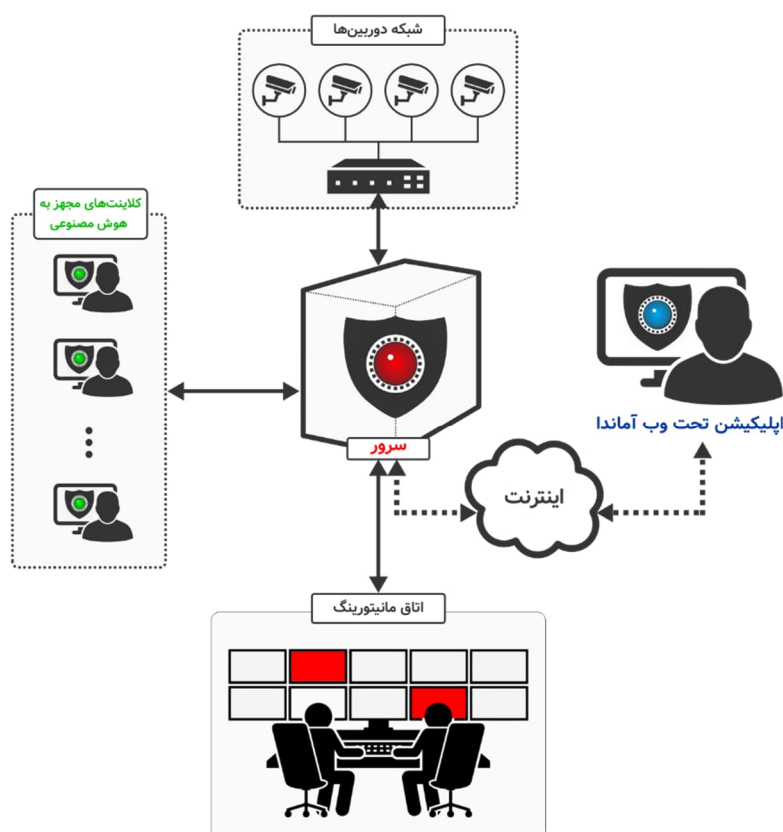
(۲) **معماری توزیع شده:** در معماری توزیع شده، عملیات پردازش هوش مصنوعی بجای متمرکزسازی بر روی سرور، به سمت کلاینت‌ها توزیع می‌شود. در این رویکرد، توان پردازشی کلاینت‌ها به صورت مستقیم برای اجرای الگوریتم‌های هوش مصنوعی مورد استفاده قرار می‌گیرد، و خروجی این پردازش‌ها شامل اطلاعات مرتبط با اهداف تشخیص داده شده به سرور ارسال می‌شود. این اطلاعات در سرور تجمیع و یکپارچه شده و در اختیار اپراتورهای مستقر در اتاق مانیتورینگ قرار می‌گیرد. در شکل ۱-۱۰ شمای معماری هوش مصنوعی توزیع شده، نشان داده شده است.

۱-۱۲-۱) ویژگی‌ها و مزایای استفاده از معماری توزیع شده

- **کاهش هزینه‌های زیرساخت:** با بهره‌گیری از توان پردازشی کلاینت‌ها، نیازی به سرورهای گران‌قیمت مجهز به کارت‌های گرافیکی پیشرفته وجود ندارد. یک سرور استاندارد برای مدیریت و نظارت کافی خواهد بود.
- **مقیاس‌پذیری ساده:** امکان اضافه‌کردن کلاینت‌های جدید در هر زمان وجود دارد. این کلاینت‌ها توان پردازشی بیشتری برای انجام عملیات هوش مصنوعی فراهم می‌کنند، بدون اینکه نیازی به تغییرات اساسی در سرور باشد.
- **افزایش پایداری سیستم:** انتقال بار پردازشی از سرور به کلاینت‌ها خطر از کارافتادن سرور به دلیل بار زیاد پردازشی را کاهش می‌دهد و اطمینان از عملکرد پایدار سیستم را فراهم می‌کند.
- **اطلاع‌رسانی جامع:** اپراتور اتاق مانیتورینگ می‌تواند به صورت متمرکز، اطلاعات تمامی اهداف تشخیص‌شده توسط کلاینت‌ها را مشاهده کند. این ویژگی باعث افزایش دقت و سرعت در مدیریت حوادث و رخدادها می‌شود.

- **کاهش پهنای باند مورد نیاز:** بجای ارسال تمام داده‌های تصویری به سرور، تنها اطلاعات پردازش شده و مرتبط با تشخیص‌ها ارسال می‌شود که به‌طور قابل توجهی از مصرف پهنای باند می‌کاهد.

- **انعطاف‌پذیری در طراحی و پیاده‌سازی:** کلاینت‌ها می‌توانند به صورت ماژولار و مطابق نیاز به سیستم اضافه شوند، و هر کلاینت با توان پردازشی خود به مجموعه کمک می‌کند.



شکل ۱-۱۰: شمای معماری هوش مصنوعی توزیع شده در سامانه آماندا

این معماری، رویکردی مدرن و اقتصادی برای مدیریت و نظارت تصویری مبتنی بر هوش مصنوعی است که با بهره‌گیری بهینه از منابع موجود، عملکرد سیستم را بهبود می‌بخشد و نیازهای نظارتی در مقیاس بزرگ را به‌طور مؤثر پاسخ می‌دهد.

۱-۱۳) زیرسامانه‌های هشدار

یکی از اصلی‌ترین و مهم‌ترین بخش‌های هر سامانه نظارتی، بخش اعلام هشدارهای آن است. با توجه به شرایط حاکم بر مکان‌ها و فضاهای تحت نظارت، بهره‌گیری از انواع روش‌های هشدار می‌تواند کارایی سامانه را به حداکثر برساند. بخش هشدار سامانه آماندا از روش‌های متنوع زیر برای اعلام نقض قوانین حراستی و ایمنی بهره می‌برد.



فعال کردن آژیر خطر در محدوده: این کار با الحاق یک مبدل سخت‌افزاری به سامانه انجام می‌شود که در مواقع ضروری صدای آژیر خطر را فعال می‌کند.



پیجینگ و پخش فایل صوتی دلخواه: این اقدام با تعریف فایل‌های صوتی دلخواه برای هر دوربین انجام می‌شود، به‌طوری که در صورت وقوع رویداد خاصی، فایل صوتی مربوطه پخش و اطلاع‌رسانی انجام می‌گردد.



ارسال پیامک با محتوای دلخواه به شماره‌های تعریف شده: این کار با اضافه کردن یک یا چند دستگاه مودم GSM به سامانه انجام می‌شود که پیام‌های هشدار را به شماره‌های از پیش تعیین شده ارسال می‌کند.



ارسال پیام (دستور) به دستگاه‌های آدرس‌پذیر: سامانه آماداً قادر است پیام‌ها و دستورات لازم را به تمامی دستگاه‌های آدرس‌پذیر شبکه، از جمله سرورهای موجود در شبکه، محل ذخیره‌سازی داده‌ها، دستگاه‌های IoT و دیگر تجهیزات متصل، ارسال کند و آن‌ها را برای کنترل از راه دور آماده کند. این ویژگی، امکان درج هشدارها و اطلاعات تولید شده توسط سامانه آماداً (مانند کشف رخدادهای ترندها و ...) را به سایر برنامه‌های دیگر اجرا شده در سرورها و یا ابزارهای مختلف می‌دهد. این قابلیت همچنین می‌تواند اطلاعات مربوط به رخدادهای سامانه‌های مدیریت اطلاعات امنیتی (SIEM¹)، سامانه‌های هشدار، سامانه‌های اطفای حریق خودکار، سامانه‌های شلیک خودکار، سامانه‌های ارسال پیامک و پیجینگ، و سامانه‌های مدیریت منابع انسانی ارسال نماید.



۱-۱۴) آمار و گزارش‌گیری

بخش «آمار و گزارش‌گیری» به‌عنوان یکی از اصلی‌ترین و کلیدی‌ترین بخش‌های سامانه آماداً تلقی می‌شود و نقش مهمی در تحلیل و مدیریت داده‌ها ایفا می‌کند. این بخش با ارائه امکانات متنوع برای گزارش‌گیری، به کاربران این امکان را می‌دهد تا اطلاعات مورد نیاز خود را به صورت دقیق و جامع استخراج و تحلیل کنند. طراحی این بخش به گونه‌ای است که پاسخگوی نیازهای مختلف کاربران بوده و ابزارهای کاربردی متعددی برای تسهیل فرآیند گزارش‌گیری فراهم کرده است.

۱-۱۵) ایجاد کیوسک‌های متعدد برای ثبت ورود-خروج

سامانه آماداً قابلیت راه‌اندازی و مدیریت کیوسک‌های متعدد برای تشخیص چهره را داراست و اطلاعات تمامی کیوسک‌ها به صورت متمرکز و یکپارچه در سامانه تجمیع می‌شود. این ویژگی امکان ایجاد کیوسک‌های تشخیص چهره را برای مقاصد مختلف فراهم می‌کند، از جمله

¹ Security Information and Event Management

کیوسک‌های اختصاصی برای **فقط ورود، فقط خروج، یا ورود و خروج همزمان**، که می‌توانند بر اساس زمان‌بندی‌های دلخواه پیکربندی شوند. این انعطاف‌پذیری به کاربران اجازه می‌دهد تا با توجه به نیازهای خاص خود، انواع مختلفی از کیوسک‌ها را برای کاربردهای گوناگون راه‌اندازی کرده و اطلاعات ورود-خروج تمامی نقاط را به صورت جامع در اختیار داشته باشند.

۱-۱۶ ویژگی‌های فنی سامانه

ویژگی‌های فنی منحصر بفرد سامانه آماندا این امکان را می‌دهد که در شرایط و نیازهای مختلف عملکردی بسیار قابل قبول و بهینه از خود ارائه دهد و به کاربران اجازه می‌دهد تا در تمامی محیط‌ها و با انواع دستگاه‌ها از آن بهره‌برداری کنند.

کاربری بسیار ساده به زبان فارسی: سامانه آماندا با طراحی کاربرپسند و زبان فارسی، استفاده از آن را برای کاربران مختلف، حتی کسانی که تجربه فنی کمی دارند، راحت و بدون پیچیدگی کرده است.



نصب و راه‌اندازی سریع: سامانه آماندا به گونه‌ای طراحی شده که نصب و راه‌اندازی آن به سرعت و به راحتی انجام می‌شود. فرآیند راه‌اندازی بدون نیاز به تنظیمات پیچیده، امکان استقرار سریع و کم هزینه را فراهم می‌آورد.



قابل استفاده در سیستم‌عامل‌های ویندوز و لینوکس: سامانه آماندا به‌طور کامل با سیستم‌عامل‌های ویندوز و لینوکس سازگار بوده و امکان اجرای بی‌دردسر در محیط‌های نرم‌افزاری متنوع را فراهم می‌کند. این سطح از سازگاری و انعطاف‌پذیری، سامانه آماندا را به گزینه‌ای ایده‌آل برای سازمان‌ها، کسب‌وکارها، و پروژه‌های چندپلتفرمی تبدیل کرده و امکان استفاده در محیط‌های مختلف نرم‌افزاری و سخت‌افزاری را بدون محدودیت فراهم می‌کند.



قابل اجرا روی کامپیوترهای کوچک و تک‌بردی: سامانه آماندا به گونه‌ای بهینه‌سازی شده است که حتی روی سیستم‌های کم مصرف و دستگاه‌های تک‌بردی مانند رزبری پای^۱، عملکردی روان و دقیق ارائه می‌دهد. طراحی سبک و کارآمد آن، این سیستم را به یک گزینه عالی برای پردازش روی لبه تبدیل^۲ کرده است، به‌ویژه در کاربردهایی که نیاز به پردازش در محل، کاهش تأخیر، و عدم وابستگی به زیرساخت‌های سنگین سروری وجود دارد. قابلیت اجرای سامانه روی دستگاه‌های کوچک، امکان استفاده در محیط‌هایی با محدودیت منابع را فراهم کرده و به دلیل کاهش نیاز به ارسال داده‌ها به سرورهای مرکزی، امنیت و حریم خصوصی را نیز افزایش می‌دهد. این ویژگی‌ها سامانه را برای مواردی همچون نظارت تصویری هوشمند، اینترنت اشیاء^۳، و سیستم‌های خودکار در محیط‌های صنعتی و خانگی ایده‌آل می‌سازد.



^۱ Raspberry Pi

^۲ Edge Computing

^۳ IoT



سازگاری با شرایط مختلف جوی و روشنائی: سامانه آماندا قادر است به طور خودکار با شرایط مختلف محیطی، از جمله تغییرات در دما، رطوبت، و روشنائی تطبیق پیدا کند و عملکرد مطلوبی را در هر شرایطی ارائه دهد.



انعطاف پذیری بی نظیر در اتصال به انواع دوربین ها: سامانه آماندا با پشتیبانی از اتصال به انواع دوربین ها، بدون توجه به برند، مدل، یا پروتکل ارتباطی، یکی از انعطاف پذیرترین راه حل ها در مدیریت و نظارت تصویری به شمار می رود. این سامانه قابلیت یکپارچه سازی با دوربین های تحت شبکه، دوربین های آنالوگ با مبدل های مناسب، و حتی دوربین های خارج از مدار مانند وب کم ها یا سایر دستگاه های ضبط تصویر را داراست. این ویژگی به کارفرمایان امکان می دهد تا بدون محدودیت در انتخاب تجهیزات، از زیرساخت ها و دوربین های موجود حداکثر بهره وری را داشته باشند یا دوربین های متناسب با نیازها و بودجه خود را آزادانه انتخاب کنند. علاوه بر این، سازگاری گسترده آماندا با انواع تجهیزات، کاهش هزینه های پیاده سازی و به روزرسانی سیستم ها را ممکن ساخته و از هدررفت منابع ناشی از عدم سازگاری جلوگیری می کند. این انعطاف پذیری، سامانه را برای کاربردهای گوناگون، از نظارت صنعتی و شهری گرفته تا پروژه های خانگی و کوچک، به یک راه حل جامع و کارآمد تبدیل کرده است.



استفاده از توان پردازشی GPU ها: سامانه آماندا از قابلیت پردازش موازی GPU ها بهره برداری می کند تا سرعت پردازش تصاویر و ویدئوها را افزایش دهد. این امکان به ویژه در پردازش های سنگین و بلادرنگ برای پردازش تصویر و ویدئوهای با کیفیت بالا نکته حیاتی بشمار می رود.



توسعه داده شده با زبان C++: سامانه آماندا با استفاده از زبان برنامه نویسی C++ توسعه داده شده است که به طور طبیعی به خاطر ویژگی های خود مانند پردازش سریع، بهره وری بالا از منابع، و دسترسی مستقیم به سخت افزار، عملکرد عالی را فراهم می کند. این انتخاب موجب شده تا سامانه بتواند در پردازش های پیچیده و زمان بری که به منابع بالایی نیاز دارند، با استفاده بهینه از قدرت پردازشی سیستم، به طور چشمگیری مصرف منابع سخت افزاری را کاهش دهد. این ویژگی بطور خاص در محیط هایی که تعداد زیادی دوربین باید بطور همزمان تحت پوشش قرار بگیرند، مزیت بزرگ و کلیدی به شمار می آید. در نتیجه، این سامانه نه تنها کارایی بالایی را ارائه می دهد بلکه برای کاربران به صرفه تر و کارآمدتر خواهد بود.

۱۷-۱) ویژگی های کاربردی سامانه

سیستم های نظارتی هوشمند امروزی نقش کلیدی را در حفظ امنیت و مدیریت بهینه ایفا می کنند. این سیستم ها نه تنها قادر به شناسایی دقیق و لحظه ای تهدیدات مختلف هستند، بلکه به کمک الگوریتم های پیشرفته، می توانند داده ها را تحلیل کرده و تصمیمات صحیح را در زمان مناسب اتخاذ کنند. با توجه به پیچیدگی و تنوع نیازهای نظارتی، این سیستم ها باید انعطاف پذیر و قابل تنظیم بوده تا قادر به پاسخ گویی به شرایط مختلف

و متنوع باشند. در این راستا، قابلیت‌های کاربردی متعددی برای افزایش کارایی و بهبود عملکرد سامانه آمادها طراحی شده است که در ادامه به معرفی برخی از مهم‌ترین آن‌ها پرداخته می‌شود.

۱) امکان اتصال به انواع دوربین‌های IP موجود با استفاده از استاندارد ONVIF: سامانه از پروتکل ONVIF پشتیبانی

می‌کند که امکان شناسایی، اتصال و کنترل انواع دوربین‌های IP سازگار با این استاندارد را فراهم می‌سازد.

۲) امکان دسترسی به پنل تنظیمات دوربین از داخل سامانه: کاربران می‌توانند بدون نیاز به مراجعه به پنل تحت وب دوربین،

مستقیماً از داخل سامانه به تنظیمات آن دسترسی داشته و تغییرات موردنیاز را اعمال کنند.

۳) امکان تعریف گروه‌های ذخیره‌سازی: تعریف گروه‌های متنوع ذخیره‌سازی با قابلیت تعیین آدرس ذخیره‌سازی، حداکثر فضای

ذخیره‌سازی و نوع جریان ضبط شونده.

۴) تعریف و زمان‌بندی فعالیت نظارت هوشمند برای هر دوربین به صورت مجزا: تنظیم زمان شروع و پایان فعالیت‌های

نظارتی برای هر دوربین به صورت مستقل و قابل تنظیم بر اساس نیازهای نظارتی و اولویت‌ها.

۵) تعریف کاربر و تعیین سطوح دسترسی به سامانه و دوربین‌ها: مدیریت دسترسی کاربران به سامانه با تعیین سطوح مختلف

دسترسی، برای افزایش امنیت و کنترل بر روی استفاده از منابع.

۶) مشاهده آمار و گزارش‌گیری و جستجو در ویدیوهای ضبط شده: امکان مشاهده و تحلیل داده‌های جمع‌آوری شده و

جستجوی آسان در میان ویدیوهای ضبط‌شده به منظور نظارت دقیق‌تر بر اتفاقات.

۷) تعریف زون-واحد برای هر دوربین: قابلیت تعریف نواحی خاص یا زون‌های نظارتی برای هر دوربین، تا مدیریت دوربین‌ها در

شرایط حساس راحت‌تر باشد.

۸) تعیین میزان حساسیت نسبت به نوع شیء شناسایی‌شده در حریم: تنظیم حساسیت سیستم در شناسایی اجسام مختلف،

به گونه‌ای که برای هر نوع شیء شناسایی‌شده، سیستم به‌طور خودکار واکنش‌های مناسبی نشان دهد.

۹) تعریف پرسنل و افراد شناس و آموزش هوش مصنوعی سیستم با تصاویر: شناسایی و تعریف پرسنل و افراد مجاز برای

استفاده از سیستم، به همراه آموزش و به‌کارگیری هوش مصنوعی برای شناسایی این افراد به صورت خودکار.

۱۰) برقراری محدودیت (زمانی و مکانی) حضور برای هر یک از افراد شناس: تعریف محدودیت‌های زمانی و مکانی دقیق

برای حضور هر فرد شناس در نواحی مختلف، به منظور جلوگیری از دسترسی غیرمجاز.



۱۱) اعلام هشدارهای لازم در صورت نقض محدودیت حضور افراد در نواحی غیرمجاز: سیستم قادر است در صورت نقض

محدودیت‌ها، هشدارهای فوری به مدیران و پرسنل امنیتی ارسال کند.

۱۲) برقراری کیوسک برای اظهار ورود یا خروج پرسنل (کنترل محسوس): ایجاد ایستگاه‌های کیوسک برای ثبت ورود و

خروج افراد و کنترل فیزیکی و محسوس برای امنیت بیشتر.

۱۳) تشخیص هویت چندین نفر بطور همزمان با هدف کنترل نامحسوس: قابلیت تشخیص و شناسایی همزمان هویت چندین

فرد در محیط، به‌منظور کنترل و نظارت نامحسوس و بهبود امنیت.

۱۴) شناسایی و ثبت افراد ناشناس و اعلام هشدارهای لازم: شناسایی و ثبت افرادی که به‌طور غیرمجاز وارد محیط می‌شوند

و ارسال هشدارهای فوری در این باره.

۱۵) پیدا کردن میزان شباهت یک چهره با چهره‌های ثبت‌شده: قابلیت مقایسه تصاویر صورت‌های جدید با داده‌های ثبت‌شده

و شناسایی شباهت‌های احتمالی به‌منظور افزایش دقت شناسایی.

۱۶) پیدا کردن چهره‌های مشابه در انبوهی از تصاویر چهره و دسته‌بندی آن‌ها: جستجوی تصاویر مشابه در پایگاه داده‌ها

برای دسته‌بندی و تجزیه و تحلیل بهتر اطلاعات.

۱۷) بازبسته کردن خودکار راهبند یا درب‌ها برای دسترسی محدود و امن: کنترل دقیق و اتوماتیک درب‌ها یا راهبندها برای

مدیریت دسترسی افراد به مناطق مختلف.

۱۸) گزارش‌گیری از حضور پرسنل در نواحی مختلف: سیستم به‌طور خودکار گزارش‌هایی از حضور پرسنل در مناطق مختلف

جمع‌آوری و ذخیره می‌کند.

۱۹) گزارش‌گیری از حضور افراد ناشناس در نواحی مختلف: نظارت دقیق بر حضور افراد ناشناس و ثبت تمامی فعالیت‌ها و

هشدارها برای افزایش امنیت.

۲۰) گزارش‌گیری از موارد رخ داده (مانند آتش‌سوزی، مشاهده پهلپاد و...): امکان گزارش‌گیری دقیق از حوادث مختلف مانند

آتش‌سوزی، ورود غیرمجاز یا مشاهده پهلپادها و دیگر رخداد‌های امنیتی.



(۲۱) برقراری ارتباط با سخت‌افزارهای متنوع جهت فعال‌سازی سامانه‌های امنیتی: برقراری ارتباط با تجهیزات سخت‌افزاری

مختلف مانند سامانه‌های اطفای حریق، سامانه‌های آتش‌بار و سایر تجهیزات خودکار جهت پاسخ‌گویی به حوادث به صورت سریع و مؤثر.

(۲۲) تعریف خودروهای شناس و اعمال محدودیت حضور: شناسایی خودروهای مجاز و تعریف محدودیت‌های مکانی و زمانی

برای ورود آن‌ها به مناطق خاص.

(۲۳) اعلام هشدارهای لازم در صورت نقض محدودیت حضور خودروها در نواحی غیرمجاز: هشدار به مدیران و مسئولین

در صورت ورود غیرمجاز خودروها به مناطق محدود.

(۲۴) گزارش‌گیری از ورود و خروج خودروهای شناس و ناشناس: جمع‌آوری و گزارش‌گیری از ورود و خروج خودروهای شناس

و ناشناس به سامانه و تعیین وضعیت حضور آن‌ها در مناطق مختلف.

(۲۵) امکان تعریف ابزارهای هشدار متنوع و قوانین امنیتی: تعریف انواع ابزارهای هشدار و قوانین امنیتی مجزا و یا گروهی برای

هر دوربین بصورت اختصاصی.

بخش دوم

راهنمای استفاده

نسخه سرور



۲) مقدمه

در این بخش، مراحل اصلی تنظیمات **نسخه‌ی سرور** سامانه آماندا به‌طور کامل شرح داده می‌شود. نسخه‌ی سرور سامانه آماندا به منظور انجام عملیات مدیریتی طراحی و توسعه داده شده است؛ این عملیات شامل راه‌اندازی سرویس‌ها، مدیریت دوربین‌ها، تنظیمات ضبط تصاویر، تعریف و ویرایش کاربران، ثبت اطلاعات اشخاص، کارکنان و پلاک خودروهای شناس، انجام تنظیمات مربوط به هوشمندسازی دوربین‌ها و غیره است. پس از اعمال این تنظیمات در نسخه‌ی سرور، کاربران می‌توانند از طریق نسخه‌ی ناظر سامانه (بخش سوم را مشاهده کنید) فرآیند نظارت و پایش را بصورت کامل انجام دهند.

با قرار دادن ماووس روی هر یک از آیتم‌های موجود در بخش‌ها و منوها، توضیحات مختصر و لازم‌نشان داده می‌شود.



مراحل اصلی و کلیدی راه‌اندازی و بهره‌برداری از سامانه آماندا به این ترتیب است: ۱) نصب و راه‌اندازی سرویس‌ها، ۲) تعریف و معرفی ناحیه‌ها و واحدها، ۳) اتصال و پیکربندی دوربین‌ها، ۴) ایجاد نقشه و جانمایی دوربین‌ها روی آن، ۵) مدیریت و ذخیره‌سازی ویدیوها و تصاویر، ۶) ثبت اطلاعات اشخاص و خودروها، ۷) ایجاد فنس مجازی و فعال‌سازی قابلیت‌های هوش مصنوعی دوربین‌ها. این مراحل بصورت گام‌به‌گام برای تضمین عملکرد بهینه سامانه باید اجرا شوند. توجه داشته باشید که در متن راهنمای پیش‌رو، بصورت مکرر به **منوی اصلی** و آیتم‌های مختلف آن اشاره شده است. در شکل ۲-۱، نمایی از این منو نشان داده شده است.



شکل ۲-۱: نمایی از منوی اصلی سامانه آماندا

۲-۱) راه اندازی سرویس ها

سامانه آمندا شامل چهار سرویس به شرح زیر است:

سرویس مرکزی: این سرویس عملیات اتصال به دوربین های تعریف شده را انجام داده و فرآیند ضبط و ذخیره سازی ویدیوها را در مسیرهای مشخص شده انجام می دهد.



سرویس ناظر فضای ذخیره سازی: این سرویس بصورت مداوم فضای ذخیره سازی اختصاص یافته به ویدیوها را پایش کرده و اطمینان حاصل می کند که همواره فضای کافی برای ذخیره سازی ویدیوهای جدید فراهم است.



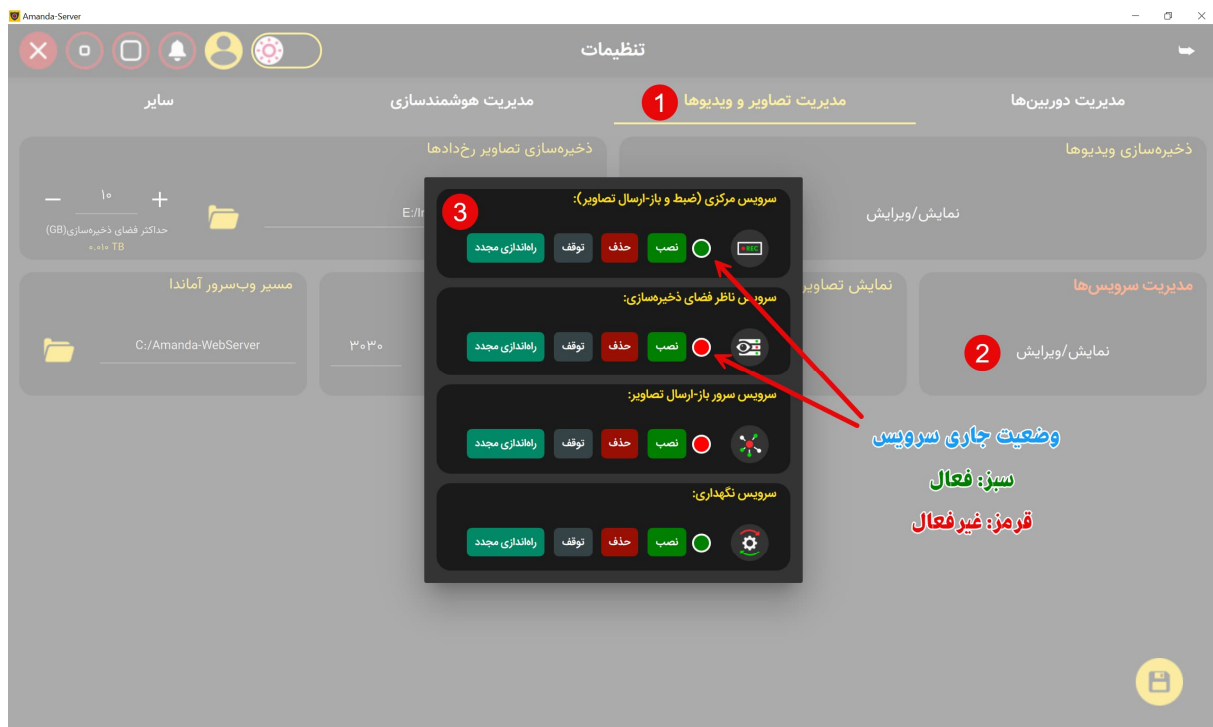
سرویس سرور باز-ارسال تصاویر: این سرویس نقش سرور باز-ارسال تصاویر دریافتی از دوربین ها را ایفا می کند. با اجرای این سرویس، تصاویر دریافتی از دوربین ها بصورت بلادرنگ در اختیار ناظران قرار می گیرد.



سرویس نگهداری: این سرویس با هدف حفظ عملکرد سایر سرویس ها، در بازه های زمانی مشخص آن ها را متوقف کرده و مجدداً اجرا می کند. با نگه داشتن کلید Ctrl و کلیک روی این آیکن، بازه ی زمانی و ساعتی را که می خواهید فرآیند نگهداری انجام شود، ظاهر می شود.



بنابراین، اولین و مهمترین کاری که باید انجام دهید، نصب و راه اندازی هر یک از این سرویس ها است. برای دسترسی به منوی سرویس ها، از **منوی اصلی** به برگه **مدیریت تصاویر و ویدیوها** رفته و دکمه نمایش/ویرایش مدیریت سرویس ها را فشار دهید. شکل ۲-۲ نمایشی از این منو را نشان می دهد.



شکل ۲-۲: نمایشی از منوی سرویس ها



پس از نصب هر یک از این سرویس‌ها، با فشردن دکمه‌ی **راه‌اندازی مجدد**، سرویس مورد نظر فعال و اجرا خواهد شد. شایان ذکر است که این سرویس‌ها به‌طور خودکار تمامی تغییرات مرتبط با دوربین‌ها و گروه‌های ذخیره‌سازی را رصد می‌کنند و نیازی به راه‌اندازی مجدد آنها وجود ندارد. به عبارت دیگر، هرگونه عملیات اضافه، حذف یا ویرایش دوربین‌ها و گروه‌های ذخیره‌سازی بصورت خودکار توسط این سرویس‌ها شناسایی و اعمال می‌شود.

۲-۲) معرفی ناحیه (زون^۱) و واحد (یونیت^۲)

در پروژه‌هایی که ناحیه تحت نظارت تصویری وسیع و تعداد دوربین‌ها زیاد است، تقسیم‌بندی دوربین‌ها در سطوح مختلف می‌تواند مدیریت و نظارت را بسیار ساده‌تر و کارآمدتر کند. در سامانه آماندا، ساختار سلسله مراتبی برای این منظور در نظر گرفته شده است:

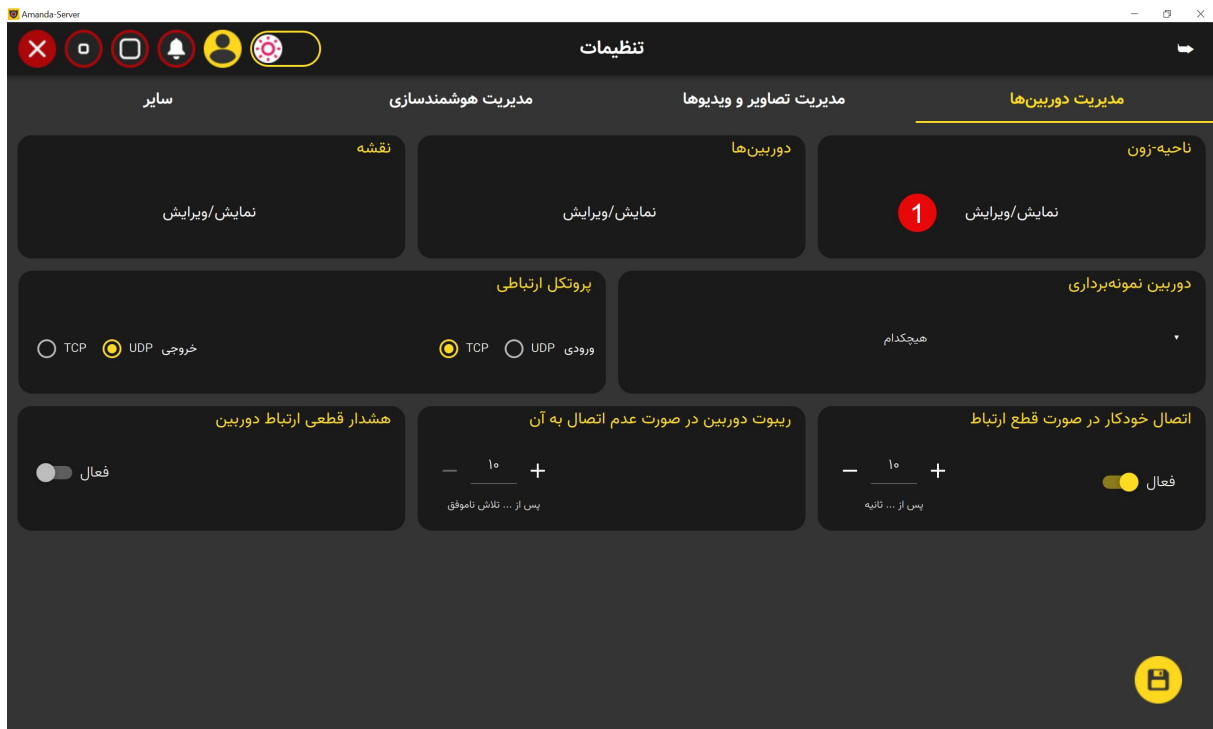
(۱) **زون:** نمایانگر یک ناحیه بزرگ مانند یک ساختمان یا محوطه

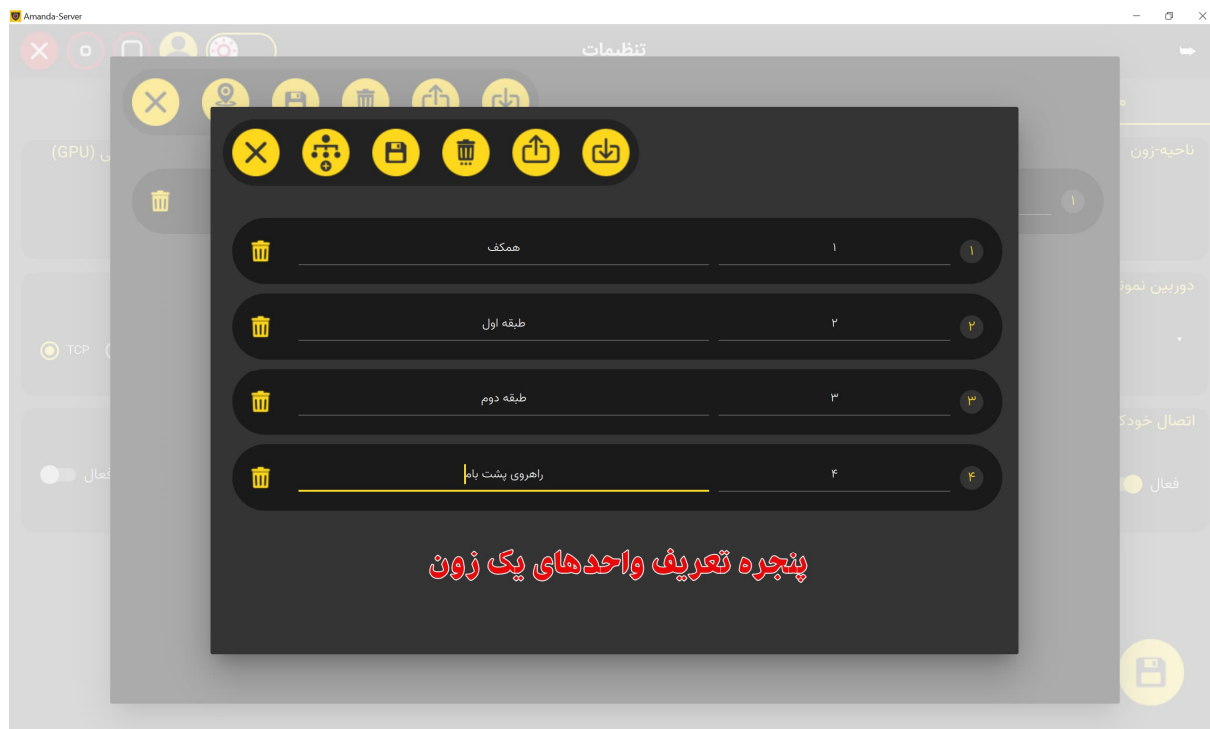
(۲) **واحد:** زیرمجموعه‌ای از یک زون، مانند طبقه یا بخش خاصی از ساختمان

هر دوربین باید به‌طور دقیق در یک زون-واحد مشخص طبقه‌بندی شود. پیش از تعریف و مدیریت دوربین‌ها، ضروری است که زون‌ها و واحدهای مرتبط به‌طور کامل معرفی شوند. این کار امکان اختصاص دقیق دوربین‌ها به نواحی مشخص را فراهم می‌کند. به‌عنوان مثال، در مجموعه‌ای شامل چندین ساختمان، می‌توان هر ساختمان را به‌عنوان یک زون و هر طبقه از آن را به‌عنوان یک واحد تعریف کرد. این روش نه تنها به سازماندهی بهتر کمک می‌کند، بلکه جستجو، نظارت و مدیریت را نیز کارآمدتر می‌سازد. برای تعریف زون و سپس واحد، از **منوی اصلی** به بخش **تنظیمات** رفته و مراحل نشان داده شده در شکل ۲-۳ را دنبال کنید.

¹ Zone

² Unit

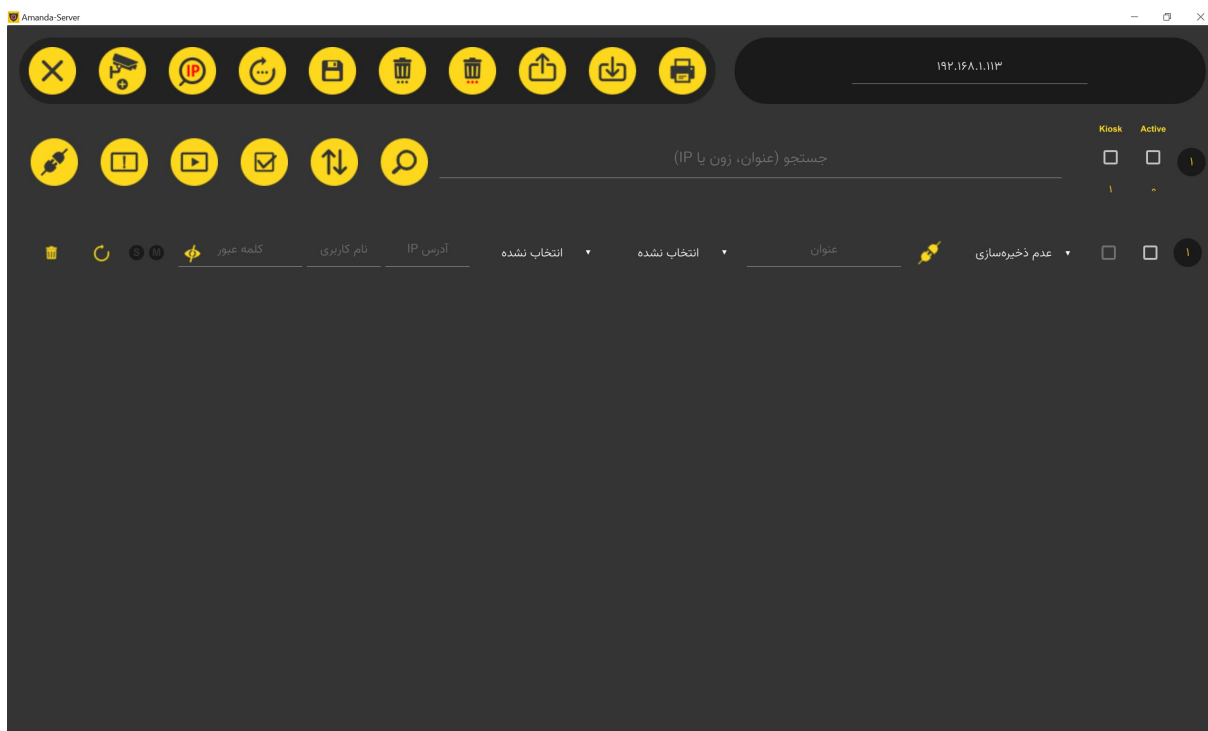
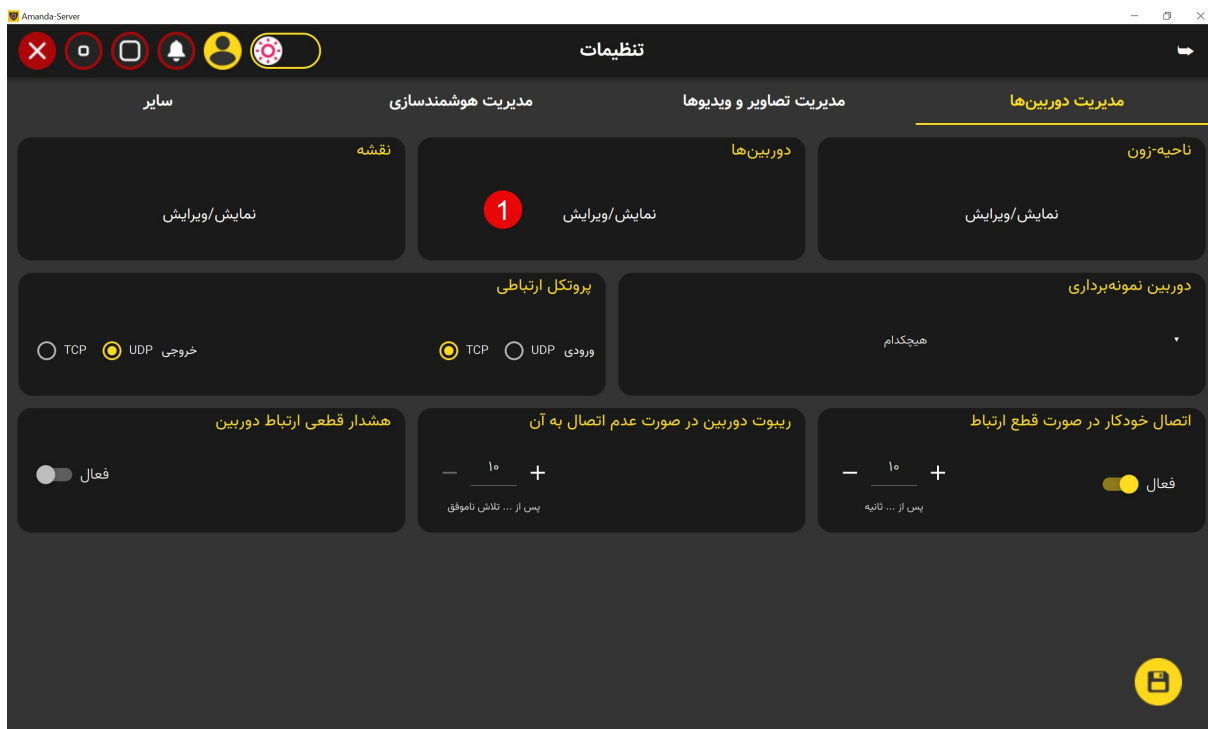




شکل ۳-۲: مراحل تعریف زون-واحد

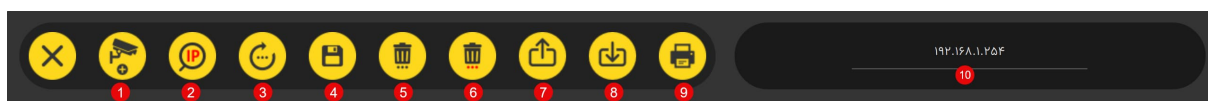
۳-۲) تعریف و اتصال به دوربین‌ها

برای تعریف اطلاعات دوربین‌ها و اتصال به آنها، از **منوی اصلی** به **تنظیمات** رفته و به ترتیب مراحل نشان داده شده در شکل ۳-۲ عمل کنید.



شکل ۲-۴: مراحل تعریف دوربین

با توجه به تعدد آیتم‌های منوی نمایش و ویرایش دوربین‌ها، آنها را به دو بخش آیتم‌های عمومی (شکل ۲-۵) و آیتم‌های خصوصی (شکل ۲-۶) تقسیم کرده‌ایم. در ادامه، توضیحات هر کدام از این آیتم‌ها ارائه می‌شود.



شکل ۲-۵: آیتم‌های عمومی منوی تعریف و ویرایش دوربین‌ها

توضیحات مربوط به آیتم‌های نشان داده شده در شکل ۲-۵:

۱) **دکمه افزودن دوربین جدید:** با فشردن این دکمه، یک ردیف خالی برای وارد کردن اطلاعات دوربین جدید به لیست دوربین‌ها اضافه می‌شود. اگر کلید Ctrl رو گرفته و این دکمه را فشار دهید، ردیف جدیدی با کپی اطلاعات آخرین دوربین افزوده شده و افزایش یک واحد به عدد IP آن، ایجاد می‌شود. مزیت اینکار، تسریع در فرآیند افزودن دوربین‌هایی با اطلاعات یکسان است.

۲) **دکمه جستجوی دوربین‌ها بصورت خودکار:** با فشردن این دکمه، منویی جهت جستجوی دامنه‌ای از آدرس‌های IP نشان داده می‌شود.

۳) **دکمه بروزرسانی همه دوربین‌های فعال:** با فشردن این دکمه، وضعیت اتصال همه دوربین‌های فعال نشان داده شده در لیست، بروزرسانی می‌شوند.

۴) **دکمه ذخیره تغییرات:** با فشردن این دکمه، آخرین تغییرات در دوربین‌ها ذخیره می‌شود.

۵) **دکمه حذف همه اطلاعات دوربین‌ها:** با فشردن این دکمه، اطلاعات همه دوربین‌ها حذف می‌شود.

۶) **دکمه حذف اطلاعات دوربین‌های انتخاب شده:** با فشردن این دکمه، فقط دوربین‌هایی که انتخاب شده‌اند، حذف می‌شوند. برای انتخاب (و عدم انتخاب) دوربین، کافی است روی شماره ردیف هر دوربین یک بار کلیک کنید.

۷) **دکمه ذخیره اطلاعات دوربین‌ها در فایل^۱:** با فشردن این دکمه، اطلاعات دوربین‌های وارد شده در فایلی ذخیره می‌شود.

۸) **دکمه بارگذاری اطلاعات دوربین‌ها از فایل^۲:** با فشردن این دکمه، امکان بارگذاری اطلاعات دوربین‌ها که قبلاً در فایلی ذخیره شده‌اند، فراهم می‌شود.

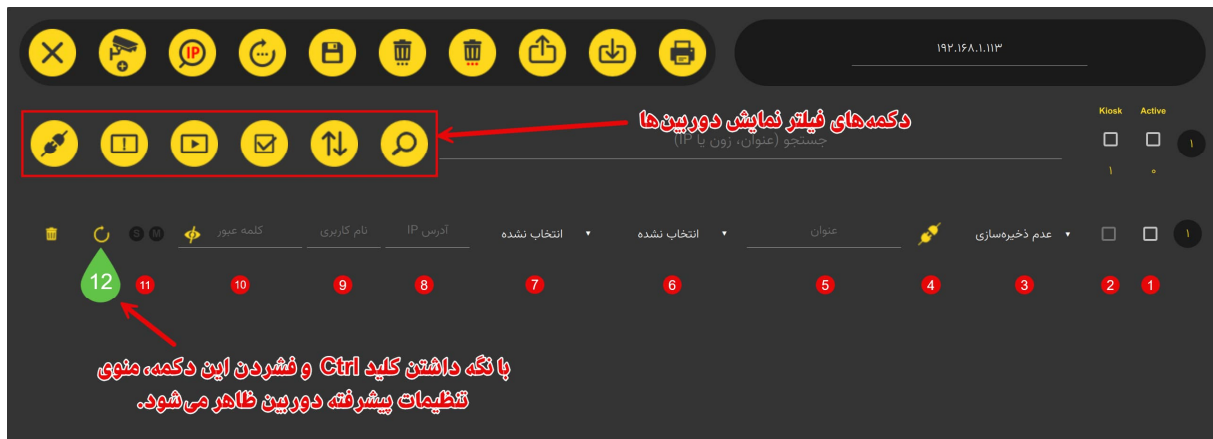
^۱ Export

^۲ Import



۹) **چاپ اطلاعات دوربین‌ها:** با فشردن این دکمه، اطلاعات تمامی دوربین‌های فعال در یک فایل PDF ذخیره خواهد شد.

۱۰) **آیتم نمایش آدرس IP ماشین-سرور:** در این قسمت آدرس IP ماشین یا سروری که سامانه آماندا در آن اجرا شده است، نشان داده می‌شود.



شکل ۲-۶: آیتم‌های خصوصی هر دوربین در منوی تعریف و ویرایش دوربین‌ها

توضیحات مربوط به آیتم‌های نشان داده شده در شکل ۲-۶:

۱) **چک‌باکس فعال یا غیرفعال کردن دوربین:** در صورتی که تیک این چک‌باکس زده شود، دوربین فعال فرض می‌شود و در

تمامی قسمت‌های سامانه از جمله قسمت اجرا، در دسترس قرار خواهد داشت. در صورتی که بخواهید دوربینی را از مدار خارج کرده ولی اطلاعات آنرا همچنان نگه دارید، می‌توانید تیک چک‌باکس آنرا بردارید.

۲) **چک‌باکس نشان‌گذاری دوربین برای استفاده از آن به عنوان کیوسک:** در صورتی که تیک این چک‌باکس برای دوربینی

فعال باشد، فرض بر این خواهد بود که این دوربین قابلیت بکارگیری در حالت کیوسک را (رجوع شود به ۲-۱۱) دارد.

۳) **انتخاب گروه ذخیره‌سازی:** با انتخاب گروه ذخیره‌سازی برای هر دوربین، محل ذخیره‌سازی و همچنین نوع ذخیره‌سازی ویدیو

(کیفیت اصلی یا فرعی) را مشخص می‌کنید (رجوع شود به بخش ۲-۵).

۴) **آیتم نشان‌دهنده وضعیت اتصال دوربین:** پس از اتمام بروزرسانی وضعیت اتصال به دوربین (آیتم شماره ۱۲)، وضعیت

اتصال سامانه به دوربین توسط این آیتم نشان داده می‌شود:

آدرس IP وارد شده برای دوربین در شبکه پیدا نشده است. به عبارتی، اصطلاحاً دوربین ping ندارد!





اطلاعات وارد شده برای دوربین (نام کاربری و یا کلمه عبور) صحیح نیست و یا پروتکل مناسب برای ارتباط با دوربین پیدا نشده است.



دوربین با موفقیت به سامانه متصل شده است. با کلیک روی این آیتم، اسنپ‌شاتی^۱ از آن دوربین نشان داده می‌شود. در این اسنپ‌شات، اطلاعات دوربین از جمله سازنده، مدل، رزولوشن و کدک^۲ مورد استفاده نیز نمایش داده می‌شود.



۵) آیتم محل درج نام-عنوان دوربین: نام-عنوان دوربین می‌تواند ترکیبی از حروف فارسی و انگلیسی با حداکثر طول ۵۰ حرف باشد.

۶) آیتم انتخاب زون قرارگیری دوربین: از لیست نمایش داده شده، زونی که دوربین در آن قرار دارد، انتخاب می‌شود.

۷) آیتم انتخاب واحد دوربین: از لیست نمایش داده شده، زون-واحد که دوربین در آن قرار دارد، انتخاب می‌شود.

۸) آیتم محل درج آدرس IP دوربین

۹) آیتم محل درج «نام کاربری» دوربین: معمولاً و در اکثر دوربین‌ها، نام کاربری پیش‌فرض admin است.

۱۰) آیتم محل درج «کلمه عبور» دوربین

۱۱) آیتم نشانگر نوع جریان‌های قابل دریافت از دوربین: M جریان اصلی^۳ (کیفیت تصویر اصلی) و S جریان ثانوی^۴ (کیفیت متوسط). این جریان‌ها پس از اتصال به دوربین بصورت خودکار شناسایی و نمایش داده می‌شوند.

۱۲) دکمه بروزرسانی اتصال به دوربین: با فشردن این دکمه، سامانه سعی خواهد کرد به دوربین متصل شود. نتیجه اتصال توسط آیتم «نشان دهنده وضعیت اتصال دوربین» اعلام می‌شود.

پس از بروزرسانی دوربین، با نگه داشتن کلید Ctrl و فشردن دکمه بروزرسانی دوربین، منوی **تنظیمات پیشرفته دوربین** ظاهر می‌شود. شکل ۲-۷ نمایی از این منو را نشان می‌دهد.

^۱ Snapshot

^۲ Codec (H264 or H265)

^۳ Main-Stream

^۴ Sub-Stream





uri های مربوط به پروتکل rtsp واکنشی شده از دوربین برای جریان های اصلی و فرعی

ردیف: ۲، دوربین: ۱۹۲.۱۶۸.۱.۹۹

rtsp://admin:123456@192.168.1.99:554/mode=real&idc=1&ids=1

rtsp://admin:123456@192.168.1.99:554/mode=real&idc=1&ids=2

تنظیمات پورت ها

— ۸۰ + شماره پورت HTTP

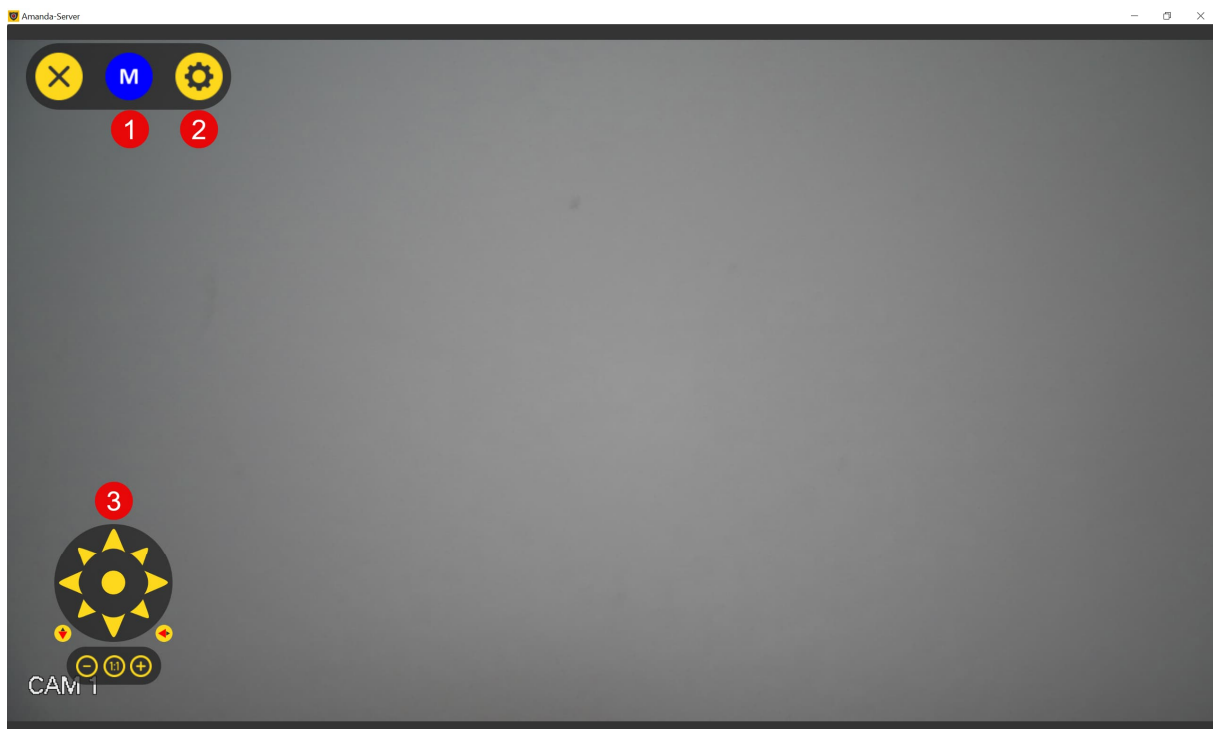
— ۵۵۴ + شماره پورت RTSP

توقف عملیات

پخش زنده

شکل ۲-۷: نمایی از منوی تنظیمات پیشرفته دوربین

در منوی تنظیمات پیشرفته دوربین، با فشردن دکمه **پخش زنده**، پخش زنده دوربین آغاز خواهد شد. شکل ۲-۸، نمایی از این پنجره را نشان می دهد.



شکل ۲-۸: نمایی از منوی پخش زنده دوربین



در منوی پخش زنده‌ی دوربین، با فشردن دکمه شماره ۱، نمایش تصاویر دوربین از جریان اصلی به جریان فرعی (و برعکس) تغییر پیدا می‌کند. با استفاده از کنترلر نشان داده شده در آیتیم شماره ۳، امکان جابجایی و تنظیم زاویه دید دوربین برای دوربین‌های چرخان، فراهم شده است.

با فشردن دکمه شماره ۲، **پنل تنظیمات دوربین** ظاهر می‌شود. این پنل در حال حاضر شامل تنظیمات مربوط به ویدیو، تنظیمات مربوط به تصویر و تنظیمات مربوط به شبکه دوربین است. شکل ۲-۹، نمایی از پنل تنظیمات دوربین را نشان می‌دهد.

با استفاده از این پنل داخلی، می‌توانید بدون نیاز به مراجعه به پنل تحت وب دوربین، تنظیمات پرکاربرد و روزمره آن را مستقیماً از داخل سامانه مدیریت کنید. این پنل از هر دو پروفایل ¹S و ²T استاندارد ONVIF ³ بصورت همزمان پشتیبانی می‌کند.



The screenshot shows a settings menu with three tabs: 'تنظیمات شبکه' (Network Settings), 'تنظیمات تصویر' (Image Settings), and 'تنظیمات ویدیو' (Video Settings), which is currently selected. The 'تنظیمات ویدیو' tab contains several settings:

- جریان (Stream):** Set to 'اصلی' (Main).
- فشرده‌سازی (Compression):** Set to 'H265'.
- اندازه تصویر (Resolution):** Set to '۱۹۲۰x۱۰۸۰'.
- نرخ فریم (FPS):** Set to '۱۲'.
- کیفیت (Quality):** Set to 'خیلی بالا' (Very High).
- نوع نرخ بیت (BitRate Type):** Set to 'CBR'.
- نرخ بیت (BitRate):** Set to '۴۵۸۲' (range ۱۲۸ ~ ۱۶۳۸۴).
- گروه تصاویر (iFrame):** Set to '۱۰' (range ۱ ~ ۱۰۰).

At the bottom of the interface, there are four buttons: 'بازگشت' (Back), 'حالت کارخانه (بدون تغییر IP)' (Factory Reset), 'راه‌اندازی مجدد' (Restart), and 'اعمال تغییرات' (Apply Changes).

(الف)

¹ ONVIF Profile S

² ONVIF Profile T

³ Open Network Video Interface Forum



تنظیمات شبکهتنظیمات تصویرتنظیمات ویدیو

روشنایی (Brightness)50

کنتراست (Contrast)50

اشباع رنگ (Saturation)50

وضوح (Sharpness)50

تراز سفیدی (White Balance)خودکار

تقویت رنگ قرمز (Red Gain)0

تقویت رنگ آبی (Blue Gain)0

WDR

سطح WDR0

حالت نوردهی (Exposure Mode)خودکار

سرعت شاتر (Shutter Speed)1/5

تقویت نوردهی (Gain)1

بازگشتحالت کارخانه (بدون تغییر IP)راه اندازی مجدداعمال تغییرات

(ب)

تنظیمات شبکهتنظیمات تصویرتنظیمات ویدیو

DHCP

آدرس IP192.168.1.99

آدرس MAC00:46:b8:07:f0:1a

ماسک زیر شبکه (Subnet-mask)255.255.255.0

آدرس دروازه (Gateway)192.168.1.1

DNS مرجع (Preferred-DNS)192.168.1.1

پورت HTTP80

پورت RTSP554

بازگشتحالت کارخانه (بدون تغییر IP)راه اندازی مجدداعمال تغییرات

(پ)

شکل ۲-۹: نمایی از پنل تنظیمات دوربین. (الف): تنظیمات ویدیو، (ب): تنظیمات تصویر، (پ) تنظیمات شبکه

۲-۳-۱) بارگذاری فایل ویدیویی به جای دوربین

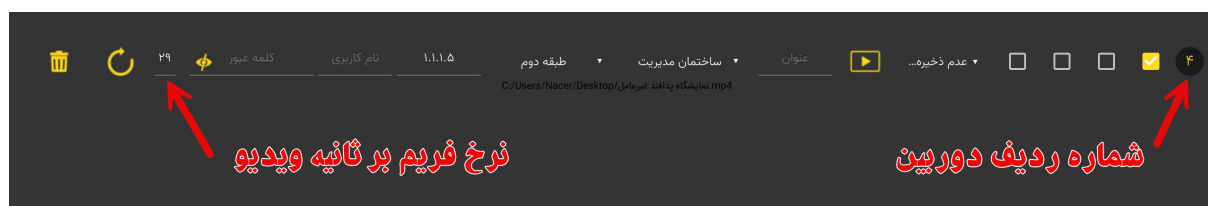
در شرایطی که نیاز باشد ویدیوهای ضبط شده از سایر دوربین‌ها را بازیابی کرده و تشخیص‌های هوش مصنوعی را بر روی آن‌ها اعمال کنید (برای مثال، استخراج خودکار پلاک خودروهای عبوری از یک مسیر)، می‌توانید بجای تعریف یک دوربین فیزیکی، از قابلیت **دوربین مجازی** استفاده کنید. در این حالت، محتوای دوربین مجازی، یک فایل ویدیویی انتخاب شده خواهد بود. برای انجام این کار:

۱) ابتدا یک دوربین خالی ایجاد کنید.

۲) کلید Ctrl را نگه داشته و روی شماره ردیف دوربین کلیک کنید.

۳) از منوی بازشده، فایل ویدیویی موردنظر را انتخاب کنید.

توجه داشته باشید که IP فایل ویدیویی باید در قالب *۱.۱.۱ باشد؛ به‌جای ستاره، می‌توانید از هر عددی بین ۱ تا ۲۵۵ استفاده کنید. پس از انتخاب فایل ویدیویی، با فشردن دکمه **بروزرسانی اتصال به دوربین**، فایل مورد نظر به‌جای دوربین بارگذاری خواهد شد. بعد از بارگذاری فایل، نرخ فریم بر ثانیه (FPS^۱) ویدیو نمایش داده می‌شود که می‌توانید این مقدار را تغییر داده تا سرعت پخش ویدیو را مطابق نیازتان تنظیم کنید. شکل ۲-۱۰ نمونه‌ای از فرآیند تعریف دوربین مجازی را نشان می‌دهد.

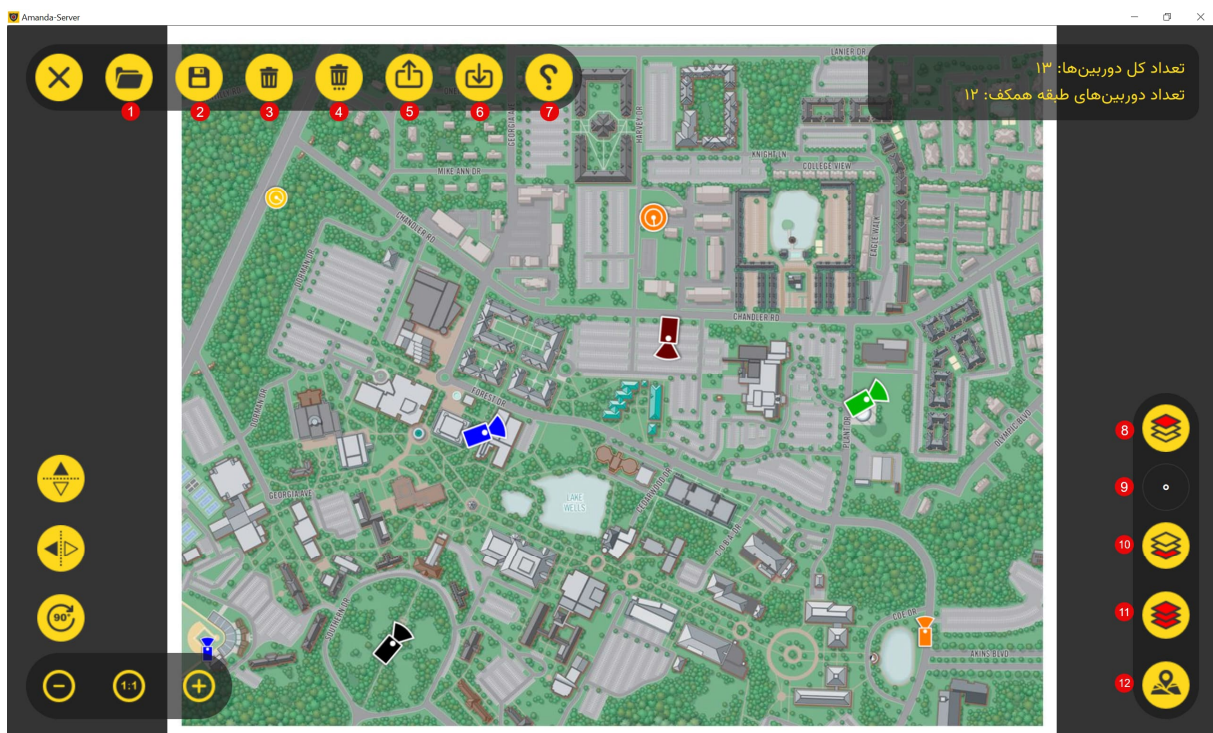
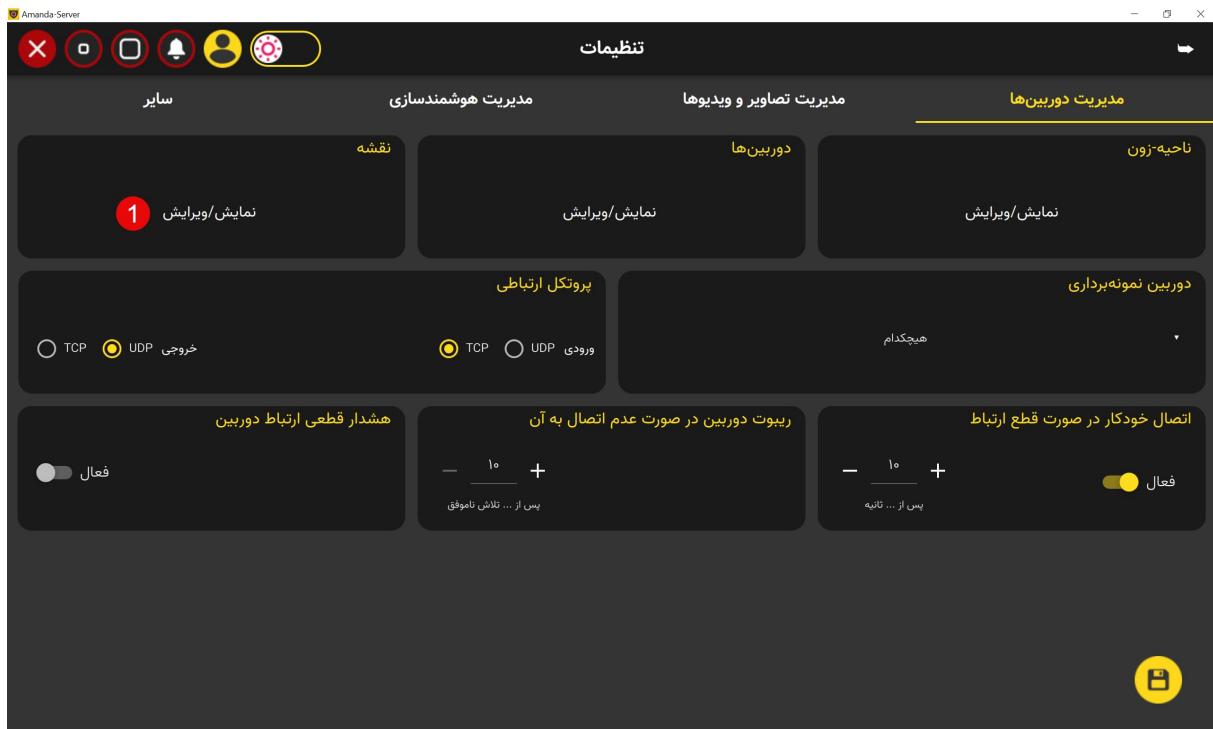


شکل ۲-۱۰: تعریف و ایجاد دوربین مجازی با استفاده از فایل ویدیویی

۲-۴) ایجاد نقشه و چیدن دوربین‌ها روی نقشه

برای ایجاد نقشه و چیدن دوربین‌ها روی آن، از **منوی اصلی** به **تنظیمات** رفته و به ترتیب مراحل نشان داده شده در شکل ۲-۱۱ عمل کنید.

¹ Frame Per Second



شکل ۲-۱۱: مراحل ایجاد نقشه

در ادامه، توضیحات مربوط به آیتم‌های این منو بر اساس شماره‌گذاری موجود در شکل ۲-۱۱ ارائه می‌شود. لازم به ذکر است که نقشه بارگذاری شده یک تصویر دوبعدی (پلان) از فضای تحت پوشش دوربین‌ها است. این تصویر می‌تواند در یکی از فرمت‌های متداول تصویری ذخیره شده باشد. همچنین، امکان اختصاص هر دوربین به یک طبقه مشخص فراهم شده است، به این ترتیب می‌توانید چیدمان دوربین‌ها را در



طبقات مختلف مدیریت کنید. به عبارت دیگر، با اختصاص شماره طبقه به هر دوربین، ساماندهی و شناسایی دوربین‌ها در سطوح مختلف امکان‌پذیر می‌شود.

(۱) **دکمه انتخاب فایل نقشه:** با فشردن این دکمه شما قادر خواهید بود نقشه دوبعدی را که یک فایل تصویری است، بارگذاری کنید.

(۲) **دکمه ذخیره اطلاعات جاری نقشه**

(۳) **دکمه حذف دوربین انتخاب شده**

(۴) **دکمه حذف همه دوربین‌ها (در همه طبقات)**

(۵) **دکمه ذخیره اطلاعات جاری نقشه در فایل**

(۶) **دکمه بازبینی اطلاعات ذخیره شده نقشه از فایل**

(۷) **راهنمای ویرایش دوربین‌ها:** در شکل ۲-۱۳، راهنمای ویرایش دوربین‌ها روی نقشه نشان داده شده است.

(۸) **دکمه جابجایی به طبقه بالاتر:** با فشردن این دکمه، دوربین‌های یک طبقه بالاتر نشان داده می‌شوند.

(۹) **آیتم شماره طبقه جاری:** این آیتم، شماره طبقه جاری را نشان می‌دهد. همچنین، با چرخاندن چرخ ماووس روی این آیتم، می‌توانید به راحتی بین طبقات جابجا شوید.

(۱۰) **دکمه جابجایی به طبقه پایین‌تر:** با فشردن این دکمه، دوربین‌های یک طبقه پایین‌تر نشان داده می‌شود.

(۱۱) **دکمه نمایش دوربین‌های قرار گرفته در تمامی طبقات:** با زدن این دکمه، تمامی دوربین‌هایی که در طبقات مختلف قرار داده شده‌اند، نشان داده می‌شود.

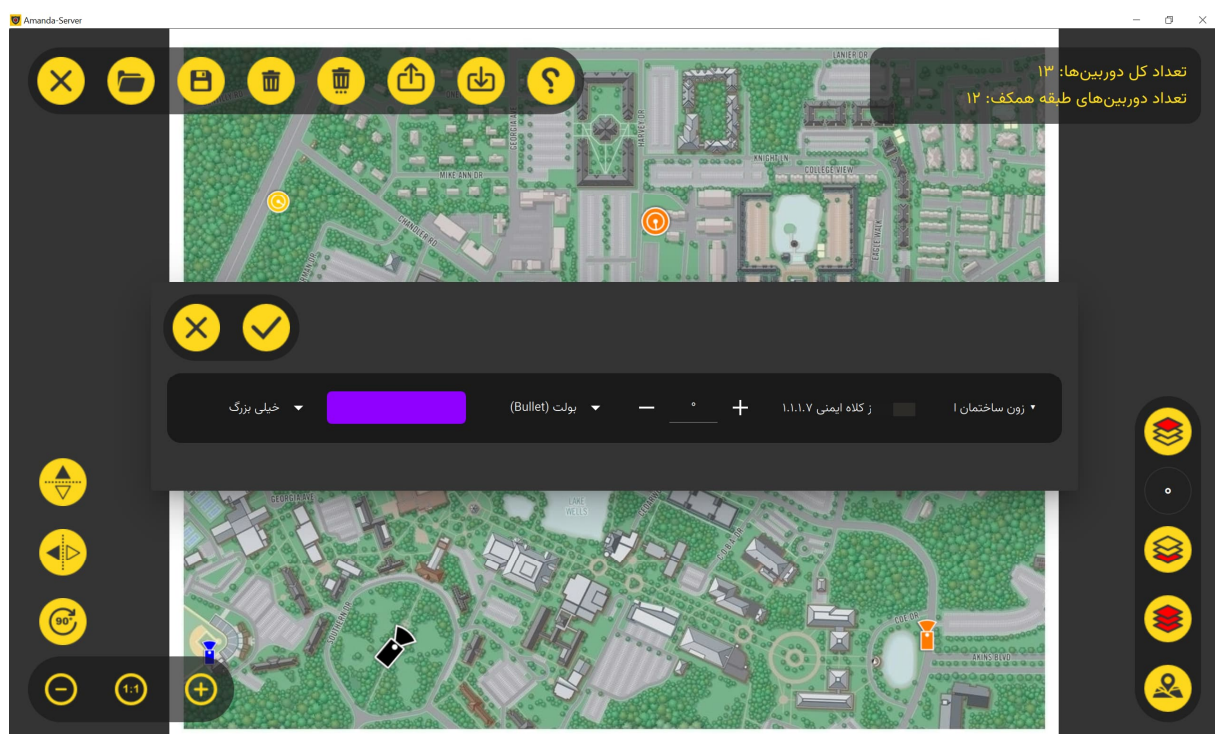
(۱۲) **دکمه برجسته کردن دوربین‌های قرار گرفته در طبقه جاری:** در مواقعی که پیدا کردن محل قرارگیری دوربین‌ها به دلیل شلوغی نقشه کار سختی باشد، با زدن این دکمه می‌توانید دوربین‌های روی نقشه را شناسایی کنید.



- (۱) اضافه کردن دوربین: ماوس را به نقطه مورد نظر برده و سپس Ctrl+Left-Click را فشار دهید.
- (۲) حذف دوربین: دوربین مورد نظر را انتخاب کرده و سپس Ctrl+Right-Click را فشار دهید.
- (۳) جابجا کردن دوربین: دوربین مورد نظر را انتخاب کرده و سپس Shift+Left-Click را فشار داده و دوربین را جابجا کنید.
- (۴) تغییر زاویه دوربین: دوربین مورد نظر را انتخاب کرده و سپس با نگه داشتن دکمه Shift و بالا-پایین کردن چرخ ماوس، زاویه دوربین را تغییر دهید.
- (۵) ویرایش اطلاعات دوربین: دوربین مورد نظر را انتخاب کرده و سپس روی آن دوبار کلیک کنید.
- (۶) بزرگ-کوچک نمایی نقشه: کلید Ctrl را گرفته و با بالا-پایین کردن چرخ ماوس، نقشه را بزرگ یا کوچک کنید.

شکل ۲-۱۲: راهنمای ویرایش دوربین‌ها روی نقشه

همچنان که در راهنما نیز ذکر شده است، با استفاده از دکمه‌های ترکیبی Ctrl+Left-Click می‌توانید در محلی که اشاره‌گر ماوس قرار دارد، دوربینی اضافه کرده و سپس با دابل-کلیک^۱ کردن روی آن، مشخصات و جزئیات مربوط به دوربین را وارد کنید (شکل ۲-۱۳).



شکل ۲-۱۳: نمایی از منوی ویرایش اطلاعات دوربین جانمایی شده در روی نقشه

¹ Double-Click

۵-۲) تنظیمات مربوط به مدیریت ویدیوها و تصاویر

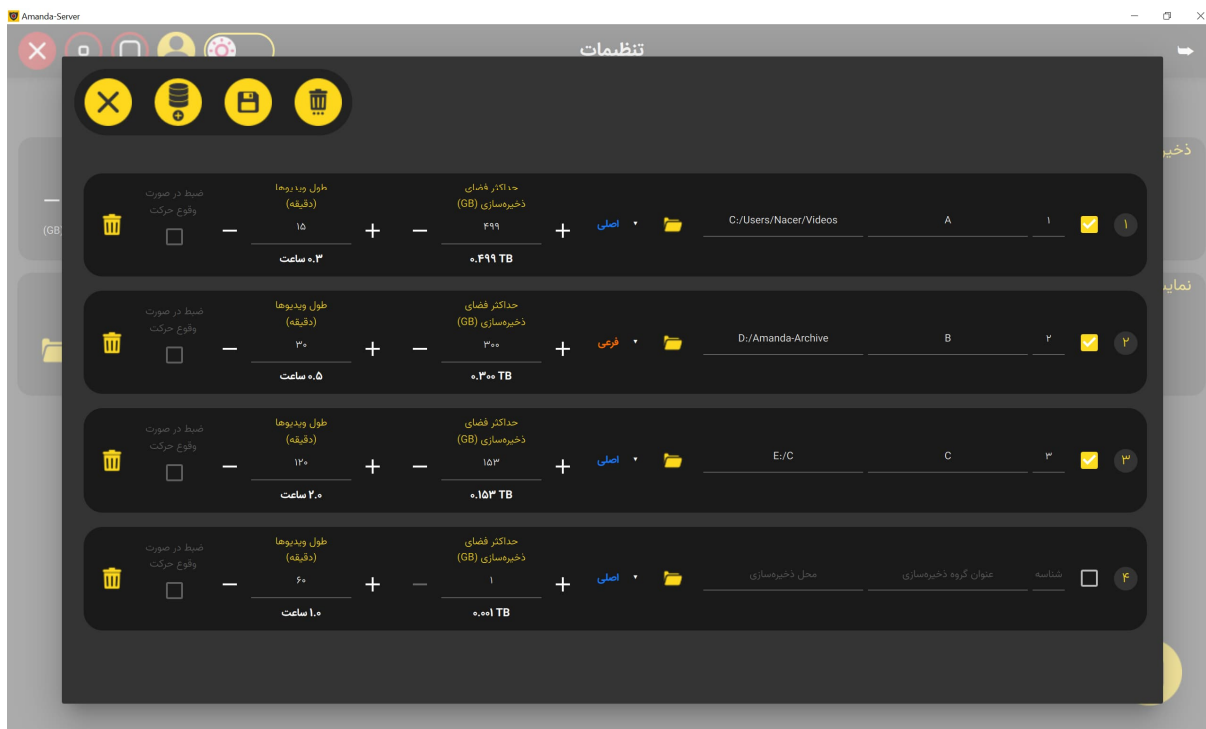
برای انجام تنظیمات مربوط به ذخیره‌سازی ویدیوهای دریافتی از دوربین‌ها، ذخیره‌سازی تصاویر ایجاد شده در فرآیند اعمال هوش مصنوعی و سایر تنظیمات مرتبط، از **منوی اصلی** به بخش **تنظیمات** رفته و برگه ^۱ **مدیریت تصاویر و ویدیوها** را انتخاب کنید. در شکل ۱۴-۲، بخش‌های مختلف این برگه نشان داده شده است.



شکل ۱۴-۲: نمایی از برگه «مدیریت تصاویر و ویدیوها»

با فشردن دکمه شماره ۱، منوی گروه‌های ذخیره‌سازی ویدیوها نمایش داده می‌شود. در این منو شما قادر خواهید بود گروه‌های ذخیره‌سازی تصاویر را تعریف کنید. شکل ۱۵-۲ نمایی از این منو را نشان می‌دهد. در آیتم شماره ۲، محل ذخیره‌سازی تصاویر ثبت‌شده از رخدادهایی که توسط هوش مصنوعی شناسایی شده‌اند، به سامانه اعلام می‌شود. با فعال کردن آیتم شماره ۴، می‌توانید به کاربرانی که از نسخه ناظر سامانه آماندا استفاده می‌کنند، اجازه نمایش تصاویر دوربین‌ها را بدهید. در آیتم شماره ۵، می‌توانید شماره پورت وب‌سرور آماندا را مشخص کنید، و در آیتم شماره ۶، آدرس محل قرارگیری وب‌سرور تعیین می‌شود. توجه داشته باشید که در پایان، با کلیک روی دکمه ذخیره‌سازی (آیتم شماره ۷)، تمامی تغییرات اعمال‌شده را ذخیره کنید.

^۱ Tab



شکل ۲-۱۵: نمایش از منوی تعریف گروه‌های ذخیره‌سازی

۲-۶) بازپخش^۱ ویدیوهای ضبط شده

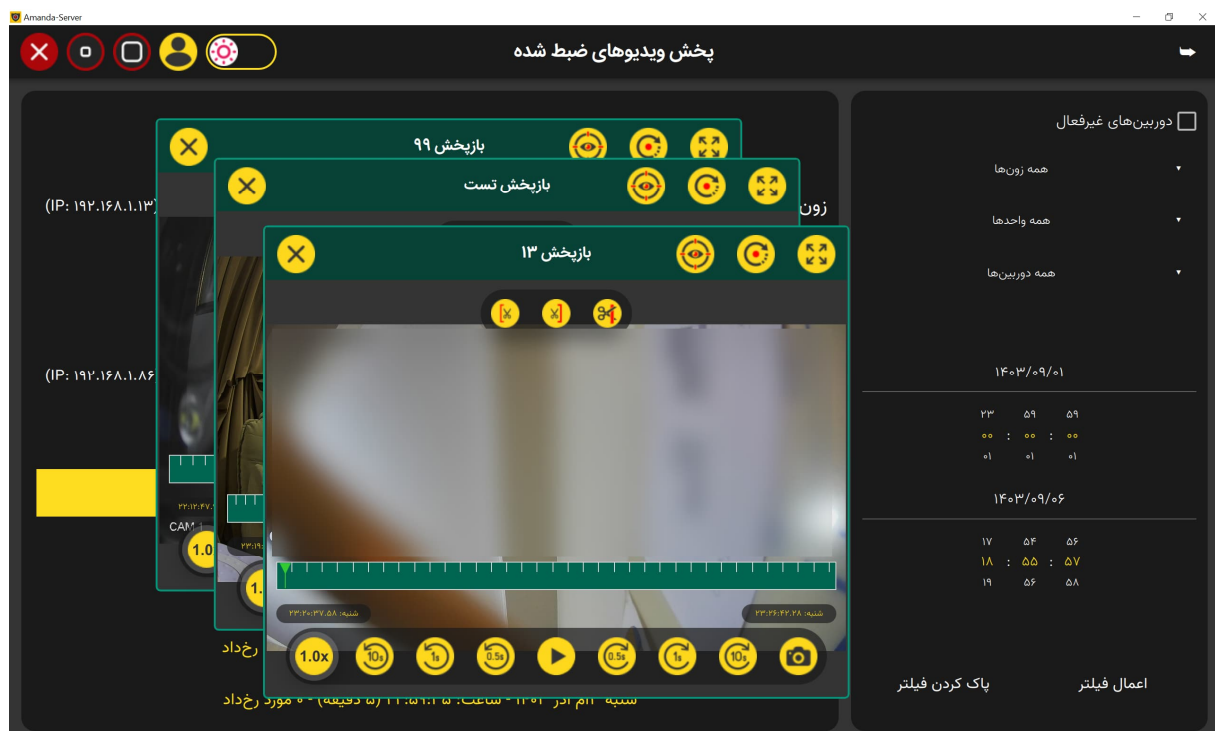
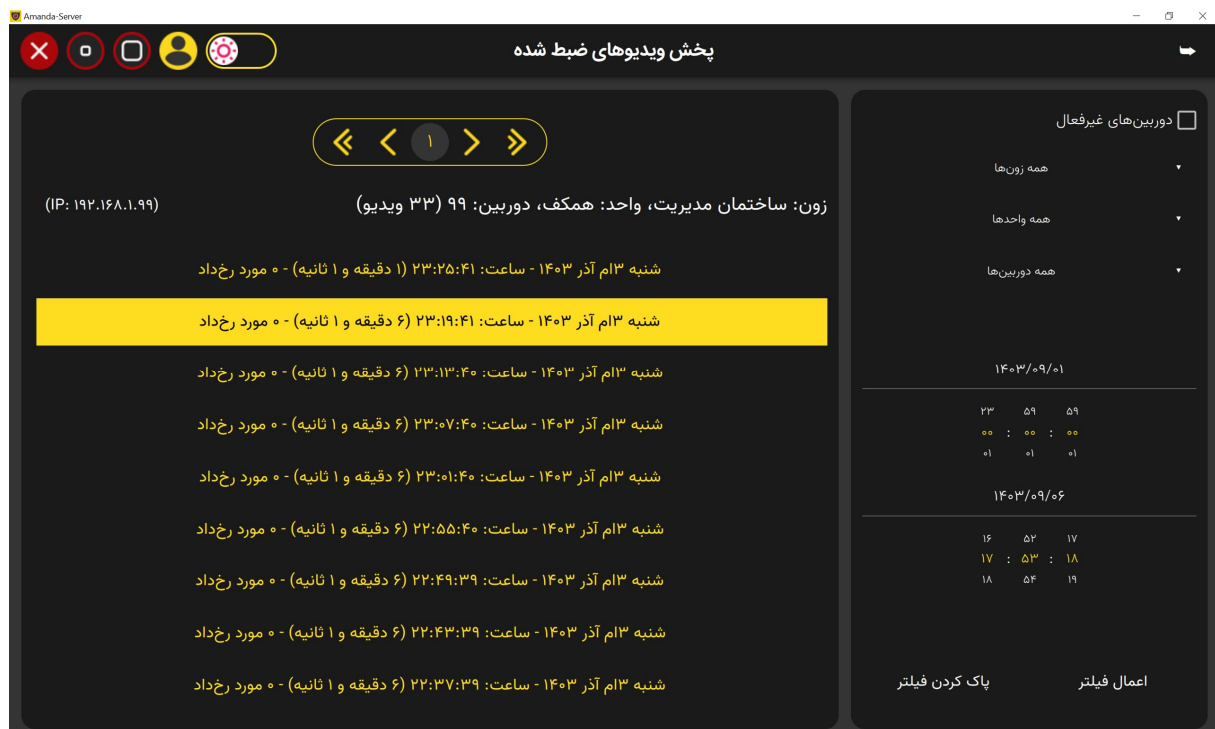
برای دسترسی به ویدیوهای ضبط شده و بازپخش آنها، از **منوی اصلی** به بخش **بازپخش ویدیوهای ضبط شده** رفته و با اعمال فیلترهای زون، واحد، دوربین، بازه تاریخی و ساعت، لیست ویدیوهای ذخیره شده را بارگذاری کنید. با دابل-کلیک کردن روی آیتم‌های (فایل‌های) نشان داده شده در پنل سمت چپ، می‌توانید ویدیوی مربوطه را مشاهده کنید. شکل ۲-۱۶ نمایش از این قسمت را نشان می‌دهد. همچنان که در این تصویر نشان داده شده است، شما می‌توانید همزمان چند ویدیو را تماشا کنید.

در هر بخش از سامانه که امکان انتخاب تاریخ وجود دارد، می‌توانید تاریخ مورد نظر را به یکی از دو روش زیر وارد کنید: تایپ مستقیم تاریخ (برای مثال: ۱۴۰۳/۰۹/۰۱) و یا فشردن دکمه Ctrl که با انجام این کار، منویی^۲ برای انتخاب تاریخ ظاهر خواهد شد.



¹ Playback

² Date Picker



شکل ۲-۱۶: نمایی از بخش «بازپخش ویدیوهای ضبط شده»

۷-۲) برپایی فنس مجازی و فعال سازی هوش مصنوعی

برای برپایی فنس مجازی (حریم) و فعال کردن هوش مصنوعی هر یک از دوربین‌ها، از **منوی اصلی** به **تنظیمات** رفته و برگه **مدیریت**

نظارت هوشمند را انتخاب کنید و مراحل نشان داده شده در شکل ۲-۱۷ را دنبال کنید.



شکل ۲-۱۷: مراحل فعال‌سازی هوش مصنوعی

با فشردن دکمه شماره ۲، آخرین اسنپ‌شات‌های^۱ دوربین‌های فعال بارگذاری و در پنل نشان داده می‌شود. پس از بارگذاری اسنپ‌شات‌ها، با کلیک روی هر کدام از آنها منوی تنظیمات هوش مصنوعی آن دوربین باز می‌شود. شکل ۲-۱۸، نمونه‌ای از این منو را نشان می‌دهد.

همانطور که گفته شد، دکمه شماره ۲ در شکل ۲-۱۷، آخرین اسنپ‌شات‌های دوربین‌ها را بارگذاری می‌کند (بدون اتصال مجدد به دوربین). برای اتصال مجدد به دوربین و بروزرسانی اسنپ‌شات آن، کلید Ctrl را نگه داشته و روی اسنپ‌شات مورد نظر کلیک کنید. با استفاده از دکمه شماره ۳، می‌توانید تعداد اسنپ‌شات‌های نشان داده شده در هر سطر را (حداکثر ۲۰ اسنپ‌شات) تغییر دهید.

در ادامه، توضیح کارکرد هر یک از آیتم‌های نشان داده شده در منوی شکل ۲-۱۸، ارائه می‌شود.



(الف)

^۱ Snapshot



(ب)

شکل ۲-۱۸: پنجره تنظیمات هوش مصنوعی دوربین

در ابتدای ورود به منوی تنظیمات هوش مصنوعی دوربین، تعداد و حالت دکمه‌های نوار ابزار به شکل ۲-۱۸ (الف) خواهد بود که نشان دهنده‌ی این است که برای این دوربین، هوش مصنوعی هنوز فعال نشده است. با فشردن دکمه مشخص شده در این شکل، دکمه‌های جدیدی (شکل ۲-۱۸ ب) نمایان خواهند شد. هر یک از این دکمه‌ها وظایفی به شرح زیر دارند:

۱) دکمه ذخیره تغییرات

۲) دکمه غیرفعال کردن نظارت هوشمند در دوربین جاری

۳) دکمه نمایش راهنمای ایجاد فنس مجازی (شکل ۲-۱۹)

۴) دکمه نمایش منوی تنظیمات مربوط به هوش مصنوعی (شکل ۲-۲۰): این منو **هسته اصلی هوشمندسازی** سامانه به شمار می‌رود و به همین دلیل، بخش جداگانه‌ای تحت عنوان **راهنمای تنظیمات تشخیص** (بخش ۲-۱۲-۶) برای توضیح آیتم‌های این منو در نظر گرفته شده است.

۵) **دکمه نمایش منوی زمانبندی نظارت هوشمند (شکل ۲-۲۱):** در این منو، قادر خواهید بود زمان فعال بودن نظارت هوشمند

را برای دوربین مورد نظر تعریف کنید. به عبارتی، فعالیت تشخیص هوش مصنوعی دوربین در بازه‌هایی که در این منو تعریف می‌کنید، انجام خواهد شد.

۶) **دکمه تار کردن حریم:** با فعال کردن این آیتم، محدوده فنس در زمان اجرا به منظور حفظ حریم خصوصی افراد به صورت تار

نمایش داده می‌شود.

۷) **دکمه برعکس کردن فنس مجازی:** در برخی از شرایط لازم است تا اطراف یک حریم خاص (و نه خود حریم) تحت نظارت

هوشمند قرار گیرد. به همین منظور، می‌توانید فنس را حول حریم مورد نظر ایجاد کرده و سپس آنرا برعکس نمایید. نمونه‌ای از فنس برعکس شده در شکل ۲-۲۲ نشان داده شده است.

۸) **دکمه ایجاد فنس مجازی در کل محدوده دید دوربین:** با فشار دادن این دکمه، کل محدوده دید دوربین تحت پوشش

فنس قرار می‌گیرد.

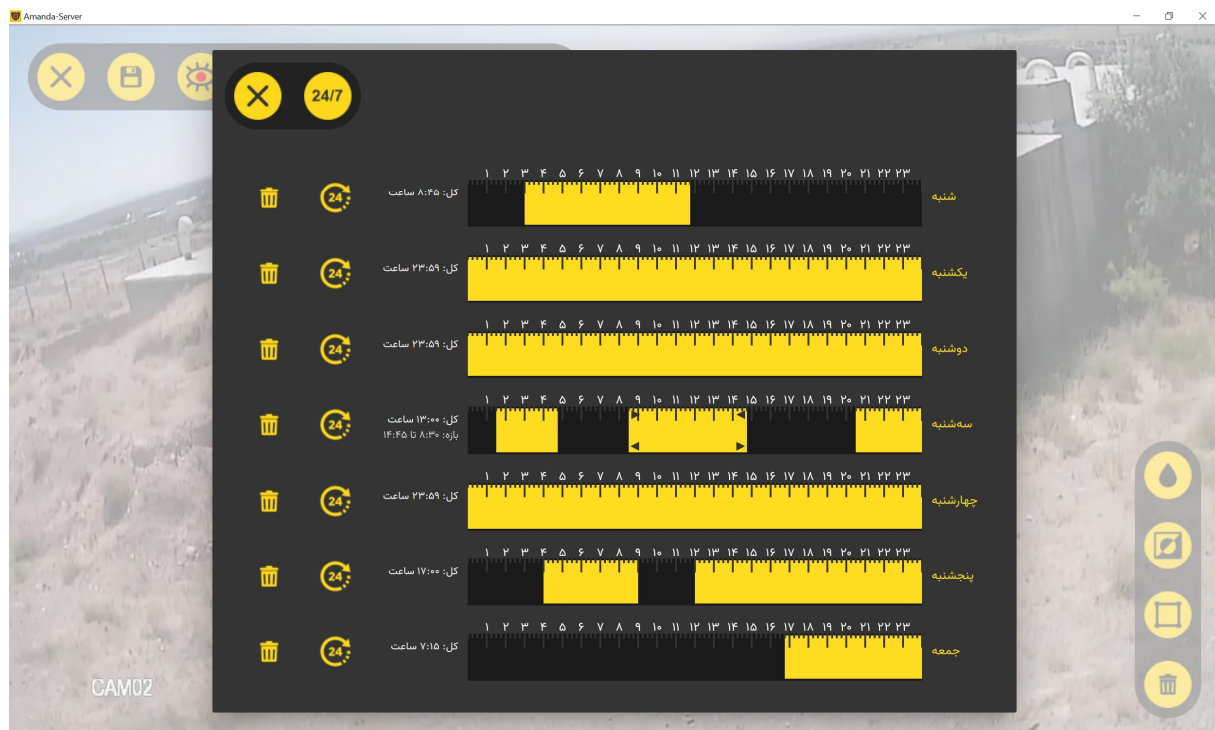
۹) **دکمه حذف فنس مجازی:** ابتدا روی فنس ایجاد شده کلیک کرده تا به رنگ آبی در بیایید. سپس اقدام به حذف آن نمایید.



شکل ۲-۱۹: نمایشی از منوی راهنمای ایجاد فنس مجازی



شکل ۲-۲۰: نمایی از منوی تنظیمات هوش مصنوعی



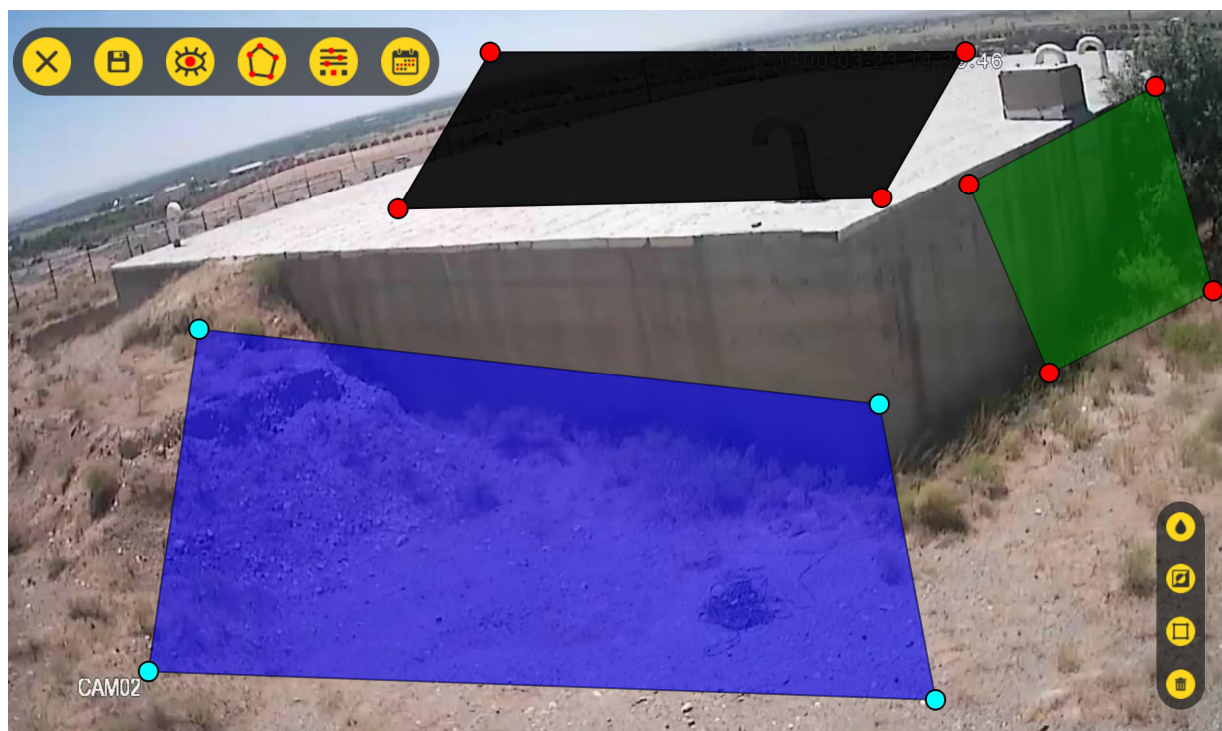
شکل ۲-۲۱: منوی تنظیمات زمانبندی فعال یا غیرفعال بودن نظارت هوشمند: با کلیک و کشیدن^۱ ماوس رو نوار ساعت هر روز، می‌توانید یک یا چند بازه زمانی ایجاد کنید. فلش‌های سیاه کوچک در انتهای بازه‌های زمانی، امکان تنظیم جزیی‌تر با دقت ۱۵ دقیقه را فراهم می‌کنند.

^۱ Drag



شکل ۲-۲۳: نمونه‌ای از فنس مجازی برعکس

کاربر می‌تواند در محدوده‌های موردنظر خود چندین فنس مجازی ایجاد کند و در صورت نیاز، هر یک را تار نماید. برای تار کردن، حذف یا ویرایش هر فنس، کافی است روی آن کلیک کنید تا فعال شود (با تغییر رنگ به آبی). در شکل ۲-۲۳، نمونه‌ای از ایجاد چندین فنس مجازی و تار کردن برخی از آنها نمایش داده شده است.



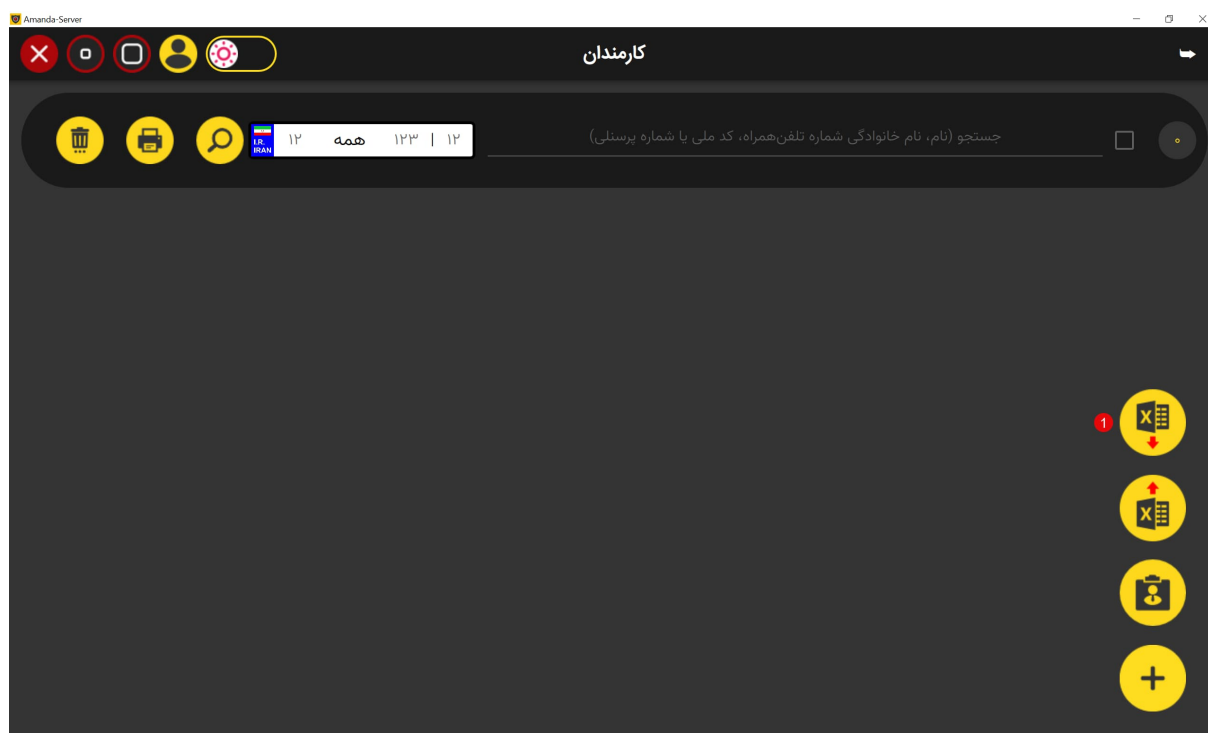
شکل ۲-۲۳: نمونه‌ای از رسم سه عدد فنس مجازی که یکی از آنها تار شده است (به رنگ سیاه) و یکی دیگر انتخاب شده است (به رنگ آبی).

۸-۲ راهنمای ثبت نام اشخاص شناسی (کارمندان-پرسنل)

در سامانه آماداسه روش برای ثبت نام اشخاص پیش بینی شده است: ۱) ثبت نام گروهی اشخاص با استفاده از فایل اکسل، ۲) ثبت نام مجزای اشخاص و ۳) ثبت نام در زمان اجرا و بصورت برخط^۱. در ادامه، راهنمای بکارگیری ثبت نام گروهی و ثبت نام مجزا توضیح داده می شود و راهنمای ثبت نام برخط، در بخش ۳-۵ ارائه شده است.

۸-۲-۱ راهنمای ثبت نام گروهی اشخاص با استفاده از فایل اکسل

در این روش می توانید با استفاده از اطلاعات تجمیعی کارمندان-پرسنل که در فایل اکسلی با فرمت CVS^۲ ذخیره شده اند، بصورت یکپارچه اقدام به ثبت نام کارمندان کنید. به همین منظور از **منوی اصلی** به بخش **کارمندان سازمان** رفته و مراحل نشان داده شده در شکل ۲-۲۴ را دنبال کنید.



¹ Online

² Comma Separated Value



شکل ۲-۲۴: مراحل ثبت نام گروهی کارمندان-پرسنل (اشخاص شناس)

با فشردن دکمه **دریافت فایل الگوی اکسل**، اقدام به دریافت فایل الگوی اکسل با فرمت CSV نمایید. سپس اطلاعات کارمندان را در این فایل اکسل وارد کنید. جهت سهولت کپی-پیست^۱ اطلاعاتی که ممکن است قبلاً گردآوری کرده باشید، می‌توانید ترتیب ستون‌ها را در فایل الگو براساس نیاز تغییر دهید.

از بین ستون‌های موجود در فایل الگو، تنها سه ستون: نام (فارسی)، نام خانوادگی (فارسی) و کد ملی جز ستون‌های ضروری هستند. بنابراین، وارد کردن یا نکردن بقیه ستون‌ها خللی در فرآیند ثبت اطلاعات ایجاد نمی‌کند.

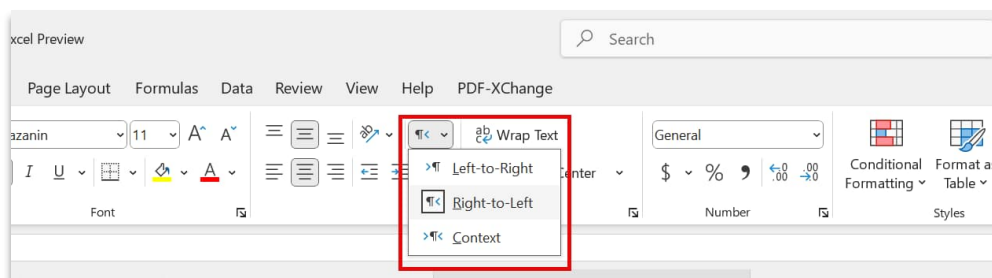


لازم به ذکر است که در حال حاضر برای هر کارمند امکان تعریف حداکثر ۲۰ دستگاه خودرو (پلاک) فراهم شده است. توجه داشته باشید به دلیل حساسیت سامانه به فرمت ورودی اطلاعات پلاک، ضروری است که اطلاعات پلاک‌ها طبق قالب تعیین شده وارد شوند تا سامانه بتواند آنها را به درستی پردازش کرده و در پایگاه داده خود ذخیره کند. وارد کردن اطلاعات پلاک‌ها در فایل اکسل باید براساس مراحل زیر انجام شود:

(۱) ستون پلاک‌ها را انتخاب کنید.

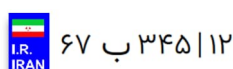
(۲) چیدمان آنرا راست-به-چپ کنید (شکل زیر).

^۱ Copy-Paste

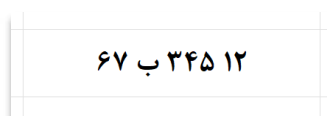


۳) صفحه کلید را فارسی کنید.

۴) فرض کنید که پلاک زیر را می‌خواهید وارد کنید:



ابتدا عدد ۱۲ را وارد کنید و سپس کلید **فاصله**^۱ را فشار دهید. عدد ۳۴۵ را وارد کرده و کلید **فاصله** را فشار دهید. در ادامه، حرف **ب** را وارد کنید و سپس کلید **فاصله** را فشار دهید و در انتها عدد ۶۷ را وارد کنید و کلید **اینتر**^۲ را برای خاتمه ورود اطلاعات فشار دهید. پس از اتمام کار، چیزی که در سلول مربوطه خواهید دید، باید دقیقاً بصورت شکل زیر باشد:

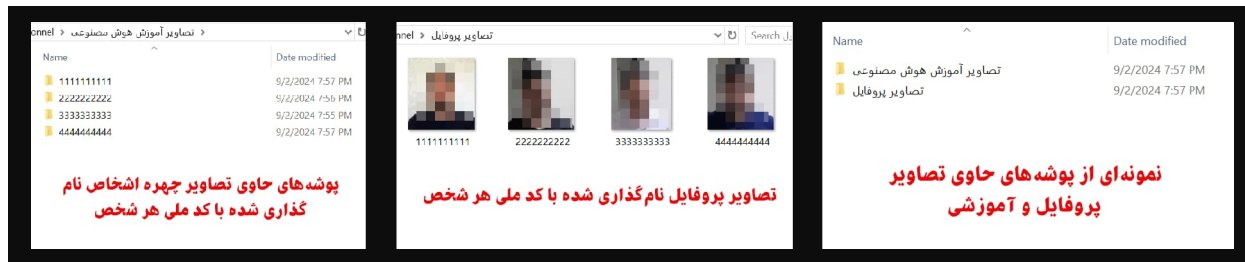


بارگذاری تصویر پروفایل و تصاویر آموزشی: در صورتی که تصاویر پروفایل و تصاویر آموزشی کارمندان را قبلاً جمع‌آوری کرده‌اید، می‌توانید به همراه با ورود اطلاعات کارمندان، آنها را نیز وارد سامانه کنید. به همین منظور، مسیر تصاویر پروفایل و همچنین مسیر تصاویر آموزشی کارمندان را بترتیب با استفاده از آیتم‌های شماره ۲ و ۳ نشان داده شده در شکل ۲-۲۴، به سامانه اعلام کنید.

فرمت تصاویر ورودی می‌تواند یکی از فرمت‌های رایج تصویری (JPG, JPEG, PNG, BMP, TIFF, ...) باشد ولی اندازه هر کدام از آنها نباید بیشتر از ۵ مگابایت باشد. دقت داشته باشید که تصویر پروفایل یک شخص و پوشه‌ی حاوی تصاویر آموزشی چهره آن شخص باید با کد ملی همان شخص نام‌گذاری شود. شکل ۲-۲۵ نمونه‌ای از این نام‌گذاری‌ها را نشان می‌دهد.

^۱ Space

^۲ Enter



شکل ۲-۲۵: نمونه‌ای از نام‌گذاری تصاویر پروفایل و پوشه حاوی تصاویر آموزشی با کد ملی

در صورتی که تمایل داشته باشید اطلاعات قبلی موجود در پایگاه داده سامانه با اطلاعات جدید بروزرسانی شوند، چک‌باکس **بروزرسانی اطلاعات قبلی** را فعال کنید. توجه داشته باشید بروزرسانی براساس کد ملی انجام می‌شود. در انتها با فشردن دکمه **بارگذاری از فایل اکسل**، فایل اکسلی که تهیه کرده‌اید را انتخاب کنید تا فرآیند ورود اطلاعات تکمیل شود.

اگر خطایی در مرحله خوانش اطلاعات فایل اکسل بارگذاری شده رخ دهد، سطر و ستون خطا به اطلاع کاربر رسانده می‌شود.



فرآیند وارد کردن اطلاعات از فایل اکسل بصورت اتمیک^۱ است؛ یا همه اطلاعات درج شده در فایل اکسل بدون ایراد خوانده شده و در پایگاه داده درج خواهند شد و یا اگر خطای رخ دهد، کل فرآیند لغو می‌شود. بنابراین اگر خطایی در حین ورود اطلاعات از فایل اکسل گزارش شود، ابتدا باید خطای گزارش شده را رفع نمایید و مجدداً اقدام به وارد کردن اطلاعات کنید.



تاکید می‌شود از نسخه آفیس ۲۰۱۹ به بالا برای ویرایش فایل اکسل استفاده کنید.



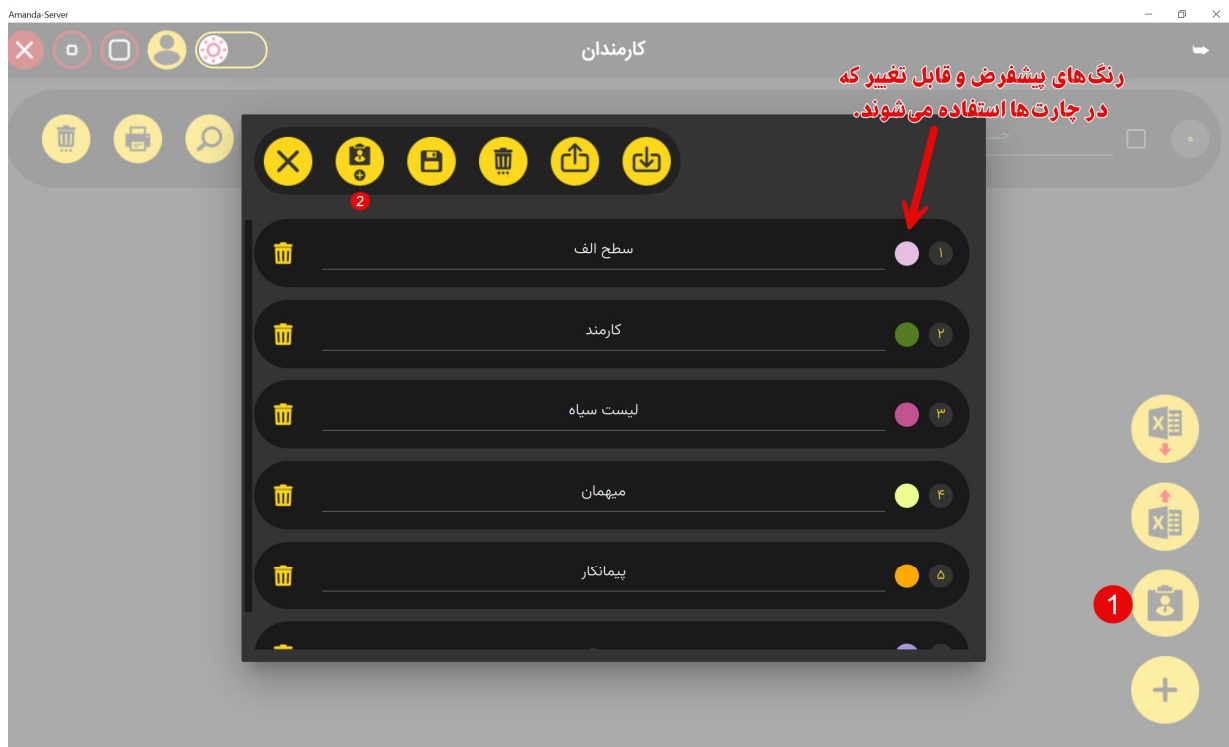
توجه داشته باشید که پس از وارد کردن اطلاعات به صورت تجمیعی از فایل اکسل و تصاویر آموزشی برای هر فرد، لازم است فرآیند آموزش تصاویر به صورت دستی انجام شود. این کار به شما امکان می‌دهد تا از صحت تصاویر آموزشی اختصاص یافته به هر شخص اطمینان حاصل کرده و تصاویر مناسب را از میان تصاویر موجود برای فرآیند آموزش انتخاب کنید. این اقدام **تأثیر مستقیمی** بر دقت و عملکرد سامانه خواهد داشت (رجوع شود به بخش ۲-۸-۲).



۲-۸-۲) ثبت نام مجزای اشخاص

برای ثبت نام افراد به صورت مجزا، پیشنهاد می‌شود ابتدا عناوین گروه‌های کارمندی (سمت) و یا شغلی مورد نظر را ایجاد کنید. این کار امکان اختصاص گروه کارمندی مشخص به هر فرد را هنگام وارد کردن اطلاعات، فراهم می‌کند. شکل ۲-۲۶ فرآیند اضافه و یا ویرایش گروه‌های کارمندی را نشان می‌دهد.

¹ Atomic



شکل ۲-۲۶: مراحل افزودن گروه‌های کارمندی

تعریف انواع گروه‌ها و یا سمت‌های شغلی و اختصاص آن به اشخاص، انعطاف‌پذیری بیشتری به شما در زمان گزارش‌گیری و یا تعریف قوانین امنیتی خواهد داد.



پس از تعریف گروه‌های کارمندی، مراحل نشان داده شده در شکل ۲-۲۷ را جهت ثبت‌نام شخص مورد نظر دنبال کنید.



شکل ۲-۲۷: مراحل ثبت نام یک شخص

پس درج اطلاعات شخص مورد نظر، آنرا ذخیره کرده و از منو خارج شوید. سپس آیتم شماره ۱ نشان داده شده در شکل ۲-۲۸ را انتخاب کنید تا منوی ویرایش اطلاعات شخص نمایش داده شود (شکل ۲-۲۹).

شکل ۲-۲۸: نمایش از لیست اشخاص (کارمندان) تعریف شده

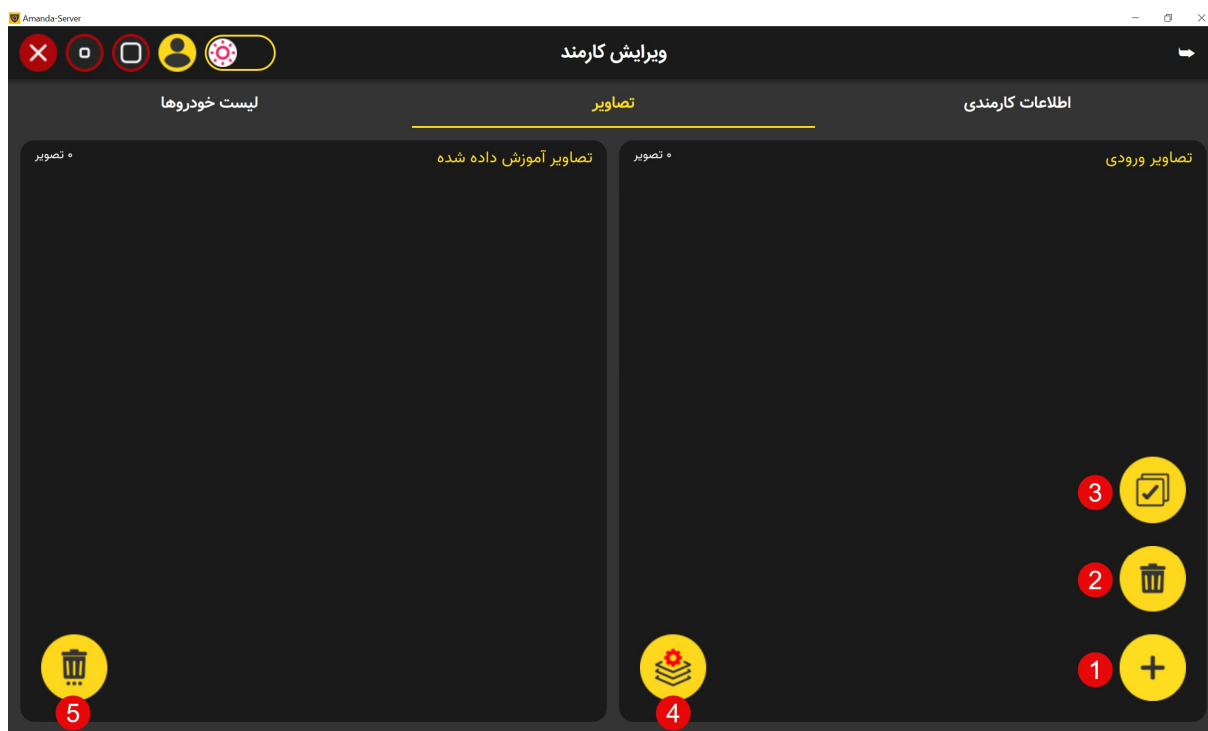
پس از ورود به منوی ویرایش اطلاعات کارمند، سه برگه با عناوین زیر در دسترس خواهد بود:

(۱) **اطلاعات کارمندی:** در این برگه، امکان مشاهده و ویرایش اطلاعات کارمند فراهم شده است.

(۲) **تصاویر:** این برگه برای افزودن، ویرایش و آموزش تصاویر چهره‌ی کارمند مورد نظر طراحی شده است.

(۳) **لیست خودروها:** در این برگه می‌توانید اطلاعات مربوط به خودروهای کارمند را ویرایش کنید.

در شکل ۲-۲۹، نمایی از برگه **تصاویر** نشان داده شده است. توضیحات مربوط به هر یک از گزینه‌های موجود در این برگه در ادامه شرح داده می‌شوند.



شکل ۲-۲۹: برگه ویرایش تصاویر آموزشی

(۱) **افزودن تصاویر آموزشی:** با کلیک بر روی این دکمه، می‌توانید تصاویر چهره‌ی کارمند مورد نظر را از میان فایل‌های موجود

انتخاب کنید یا به صورت زنده با استفاده از دوربین نمونه‌برداری، عکس‌برداری نمایید. توجه داشته باشید که دوربین نمونه‌برداری،

همان دوربینی است که از میان دوربین‌های تعریف شده در سامانه، به‌عنوان دوربین نمونه‌برداری انتخاب شده است. برای انتخاب یا

تغییر دوربین نمونه‌برداری از **منوی اصلی** به بخش **تنظیمات** رفته و وارد برگه **مدیریت دوربین‌ها** شوید و سپس بر روی گزینه

دوربین نمونه‌برداری کلیک کرده و دوربین مورد نظر خود را به‌عنوان دوربین نمونه‌برداری تعیین کنید.

(۲) **حذف تصاویر آموزشی انتخاب شده:** با فشردن این دکمه، تصاویر انتخاب شده از بین تصاویر آموزشی بارگذاری شده‌اند، حذف خواهند شد.

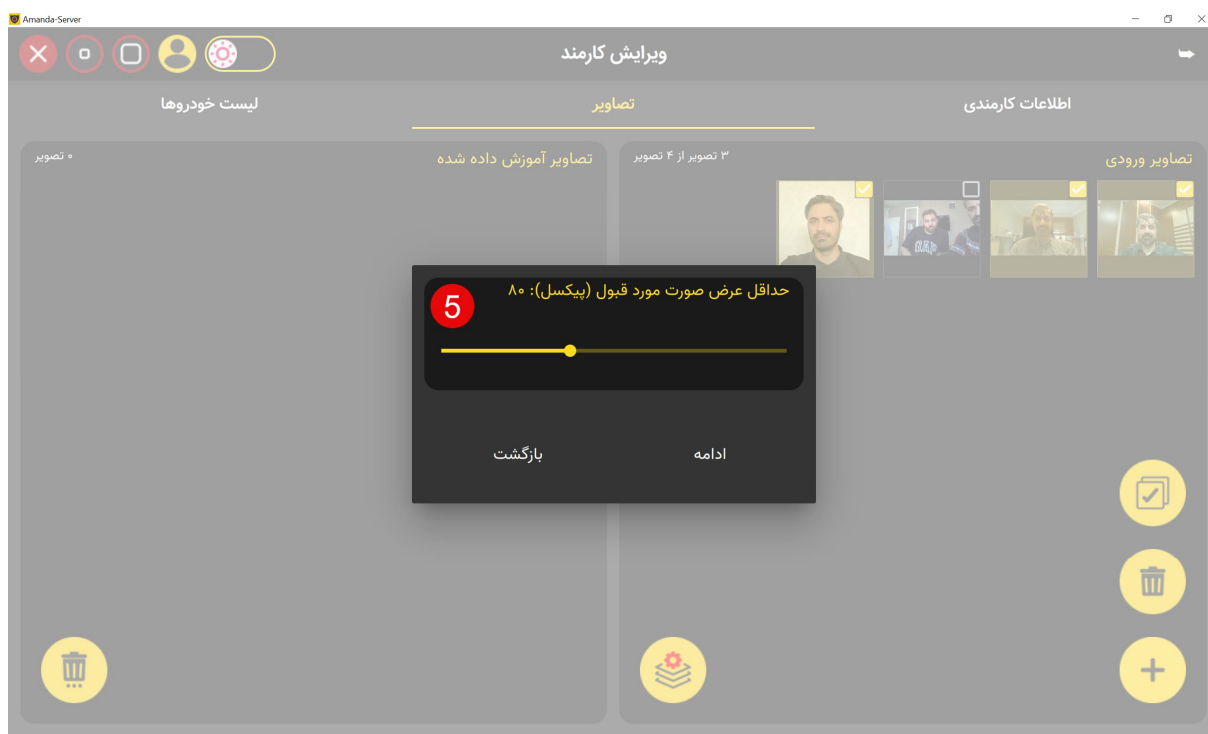
(۳) **انتخاب یا عدم انتخاب همه تصاویر آموزشی:** با فعال کردن تیک این چک‌باکس، همه تصاویر بارگذاری شده برای انجام عملیات مورد نظر انتخاب می‌شوند (یا نمی‌شوند).

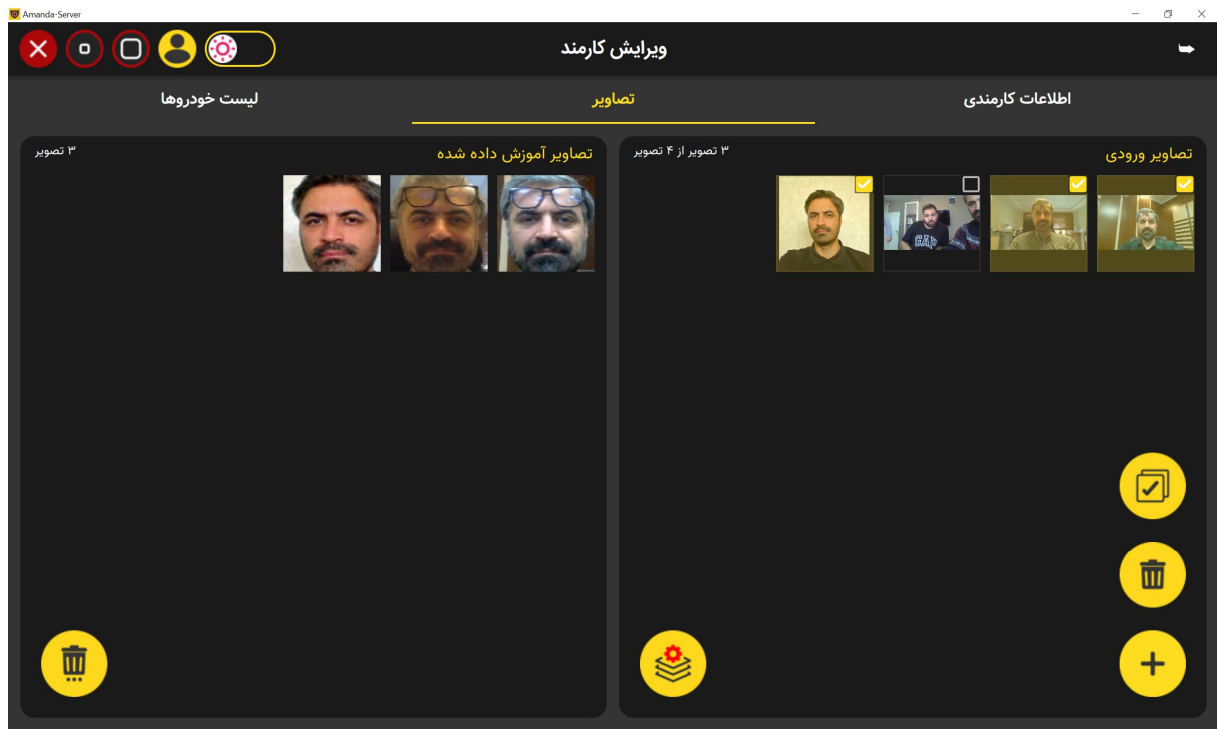
(۴) **آموزش تصاویر انتخاب شده:** با فشردن این دکمه، تصاویر چهره آموزشی انتخاب شده جهت آموزش به سامانه پردازش می‌شوند.

(۵) **حذف تصاویر آموزش داده شده:** با فشردن این دکمه، همه تصاویر چهره آموزش داده شده به سامانه، پاک می‌شوند. توجه داشته باشید که این کار موجب خواهد شد کارمند مربوطه دیگر **قابل شناسایی** در سامانه نباشد.

در شکل ۲-۳۰، نمونه‌ای از فرآیند بارگذاری تصاویر چهره آموزشی و آموزش آنها به سامانه نشان داده شده است.



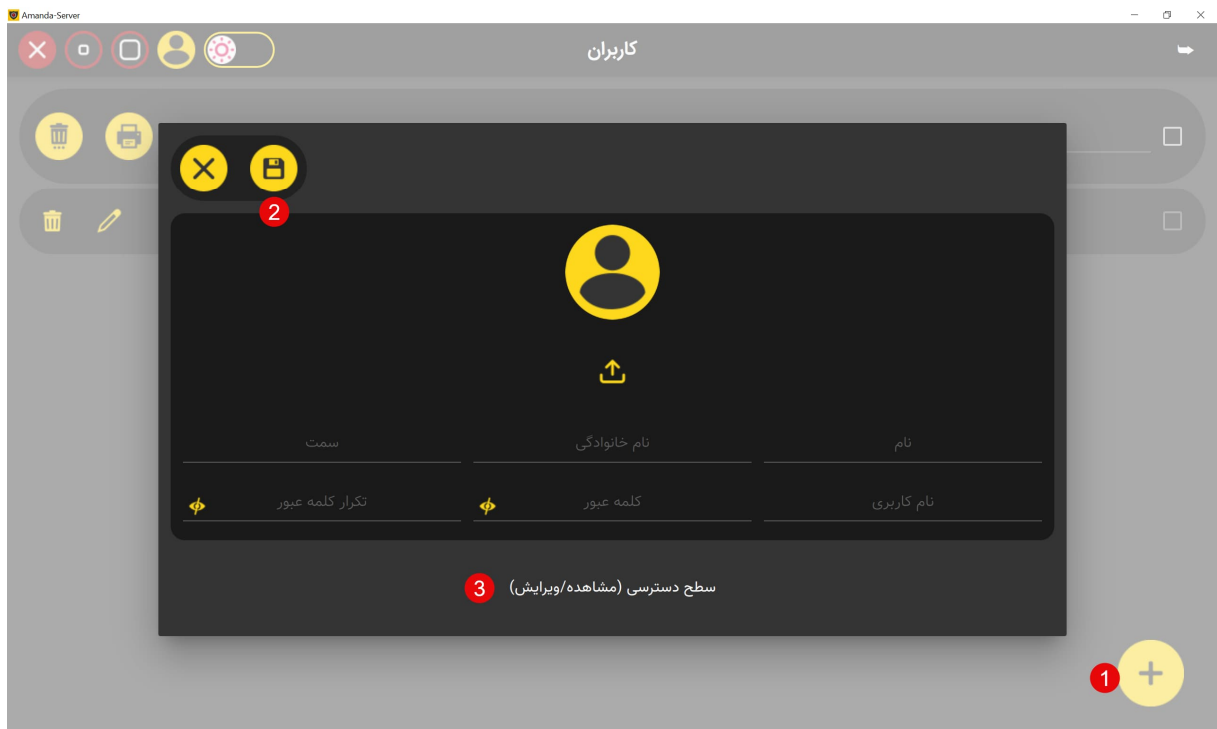




شکل ۲-۳۰: مراحل افزودن تصاویر چهره آموزشی و آموزش آن به سامانه

۲-۹) افزودن و ویرایش کاربر

برای افزودن و یا ویرایش اطلاعات کاربران سامانه، از **منوی اصلی** به بخش **کاربران سامانه** رفته و مراحل نشان داده شده در شکل ۲-۳۱ را دنبال کنید.



شکل ۲-۳۱: مراحل افزودن یا ویرایش کاربر جدید

پس از تعریف اطلاعات کاربری، لازم است سطح دسترسی کاربر را نیز مشخص کنید. برای این کار روی آیتم شماره ۳ نشان داده شده در شکل ۳۱-۲ کلیک کنید تا وارد منوی ویرایش سطح دسترسی کاربر شوید. شکل ۳۲-۲ نمونه‌ای از این منو را نشان می‌دهد.



شکل ۳۲-۲: نمایش از منوی تعیین سطح دسترسی کاربر

در ادامه توضیح هر یک از آیتم‌های موجود در شکل ۳۲-۲ به ترتیب ارائه می‌شود:

- **اجرا:** کاربر ناظر تعریف شده، پس از ورود به حساب کاری، اجازه اجرای سامانه (رجوع شود به ۳-۴) را خواهد داشت.
- **اعمال هوش مصنوعی:** اگر دوربین مجهز به هوش مصنوعی شده باشد، کاربر ناظر می‌تواند با فعال کردن این قابلیت در تنظیمات دوربین‌هایی که اجازه دسترسی به آنها را دارد (رجوع شود به ۳-۲)، از آن بهره‌برد.
- **امکان اتصال مستقیم به دوربین:** در حالت عادی، تصاویر دریافتی ناظرها از طریق باز-ارسال تصاویر توسط سرور، تامین می‌شود. در صورتی که این گزینه برای کاربری فعال باشد، آن کاربر می‌تواند بصورت مستقیم از خود دوربین نیز تصویر دریافت نماید. این گزینه به ویژه برای حالت‌هایی که ممکن است سرور به هر دلیلی از مدار خارج شود، پیش‌بینی شده است تا ناظرها تا برپایی سرور و بازگشت آن به مدار، بتوانند تصاویر دوربین‌ها را داشته باشند.



- **راه اندازی مجدد دوربین:** دوربین‌ها پس از مدتی کار مداوم، نیاز به راه اندازی خواهند داشت تا بصورت عادی به فعالیت خودشان ادامه دهند. با فعال سازی این گزینه، **کاربر ناظر** امکان راه اندازی (ریبوت^۱) مجدد دوربین‌ها را با هدف نگهداری^۲ خواهد داشت.
- **نظارت از راه دور:** با فعال سازی این گزینه، **کاربر ناظر** امکان مشاهده تصاویر باز-ارسال شده از سرور را خواهد داشت.
- **مشاهده رویدادها از راه دور:** با فعال سازی این گزینه، **کاربر ناظر** امکان دریافت تشخیص‌های هوشمندی که انجام می شود را خواهد داشت.
- **آمار و گزارش گیری:** اجازه ی دسترسی به منوی **آمار و گزارش گیری** در اختیار کاربر قرار داده می شود.
- **کارمندان سازمان:** اجازه ی دسترسی به منوی **کارمندان سازمان** در اختیار کاربر قرار داده می شود.
- **کاربران سامانه:** اجازه دسترسی به منوی **کاربران سامانه** در اختیار کاربر قرار داده می شود.
- **عملیات اخیر:** اجازه دسترسی به منوی **عملیات اخیر** در اختیار کاربر قرار داده می شود.
- **تنظیمات:** اجازه دسترسی به منوی **تنظیمات** در اختیار کاربر قرار داده می شود.
- **گزارش خطا:** اجازه دسترسی به منوی **گزارش خطا** در اختیار کاربر قرار داده می شود.
- **مشاهده نقشه:** امکان مشاهده نقشه برای کاربر ناظر فراهم می شود.
- **مشاهده IP دوربین:** امکان مشاهده IP دوربین های مجوز داده شده برای کاربر ناظر فراهم می شود.
- **دریافت تشخیص های هوش مصنوعی سایر کلاینت ها:** در صورتی که از معماری توزیع شده استفاده شود، کاربر ناظر امکان دریافت تشخیص های هوشمند انجام گرفته توسط سایر کلاینت ها را خواهد داشت. توضیح اینکه، این گزینه مناسب کاربر ناظر در اتاق مانیتورینگ است.
- **افزون پرسنل در اجرا:** در صورتی که این گزینه برای کاربری فعال باشد، امکان افزودن (ثبت نام) اشخاص شناس در زمان اجرا برای آن کاربر فراهم می شود (رجوع شود به ۳-۵).

¹ Reboot

² Maintenance



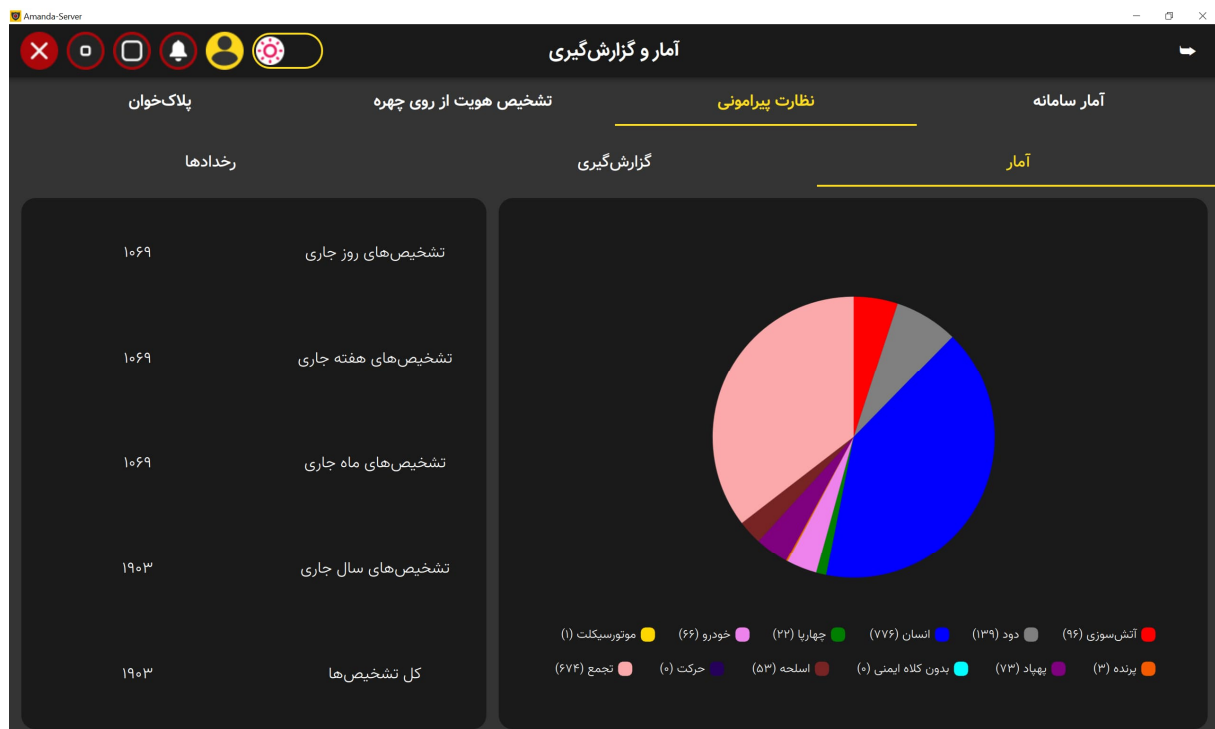
- **افزودن پلاک در اجرا:** در صورتی که این گزینه برای کاربری فعال باشد، امکان افزودن پلاک و انتساب آن به شخصی شناس در زمان اجرا برای آن کاربر فراهم می‌شود (رجوع شود به ۳-۵).
- **امکان تعریف و استفاده از قوانین امنیتی:** در صورتی که این گزینه برای کاربری فعال باشد، آن کاربر می‌تواند ابزارهای هشدار و قوانین امنیتی مورد نظر خود را تعریف کند (رجوع شود به ۳-۳).
- **باز پخش ویدیوهای ضبط شده:** با فعال کردن این گزینه، کاربر امکان بازپخش ویدیوهای ضبط شده دوربین‌هایی که اجازه دسترسی به آنها را دارد، خواهد داشت. با محدود کردن محدوده‌ی بازپخش، صرفاً امکان مشاهده آن محدود برای کاربر فراهم خواهد شد. توجه داشته باشید اگر آیت **تا تاریخ** پر نشود، کاربر امکان مشاهده ویدیوهای ضبط شده **از تاریخ** را تا تاریخ جاری خواهد داشت.
- **دسترسی دوربین‌ها:** در این بخش، اجازه دسترسی کاربر به دوربین‌ها تعیین می‌شود. توجه داشته باشید که با ویرایش زون‌ها، واحدها و یا دوربین‌ها، این قسمت (در صورت نیاز) باید برای کاربر مورد نظر بروزرسانی شود.
- **انتخاب دوربین کیوسک:** در این قسمت، امکان استفاده از یک دوربین از دوربین‌های مجاز به عنوان دوربین کیوسک به کاربر داده می‌شود (مراجع شود به ۲-۱۱).

۲-۱۰) آمار و گزارش‌گیری

برای تهیه آمار و گزارش‌گیری از **منوی اصلی** وارد بخش **آمار و گزارش‌گیری** شوید. این بخش از چهار برگه تشکیل شده است:

- (۱) **آمار سامانه:** در این برگه آمار کلی سامانه در معرض نمایش قرار می‌گیرد.
- (۲) **نظارت پیرامونی:** در این برگه آمار مرتبط با تشخیص‌های پیرامونی و امکانات گزارش‌گیری مرتبط ارائه شده است.
- (۳) **تشخیص هویت از روی چهره:** در این برگه آمار تشخیص اشخاص شناس و ناشناس از روی چهره و همچنین امکانات گزارش‌گیری از شخص یا گروه‌های کارمندی فراهم شده است.
- (۴) **پلاک‌خوان:** در این برگه نیز همانند سایر برگه‌ها امکانات مشاهده آمار و گزارش‌گیری از تردد خودروهای شناس و ناشناس فراهم شده است.

در شکل ۲-۳۳، نمایی از این بخش نشان داده شده است.



شکل ۲-۳۳: نمایی از بخش آمار و گزارش گیری سامانه

۱۱-۲) راه اندازی کیوسک

برای راه اندازی یک یا چند کیوسک، لازم است به ازای هر کیوسک، یک کاربر با سطح دسترسی ویژه ایجاد شود. برای این منظور، ابتدا به بخش مدیریت کاربران سامانه مراجعه کرده و اقدام به تعریف کاربر یا کاربران مرتبط با کیوسک کنید. سپس در منوی تنظیمات سطح دسترسی، گزینه ی کیوسک را فعال کنید. در ادامه، دوربین مربوط به کیوسک را انتخاب کرده و نوع کیوسک (ورود، خروج، یا ورود-خروج) را مشخص کنید. همچنین می توانید محدوده زمانی را روی کیوسک ورودی-خروجی اعمال کنید تا در ساعت مشخصی ثبت ورود و ثبت خروج فعال باشد. شکل ۲-۳۴

نمایی از این قسمت را نشان می دهد.

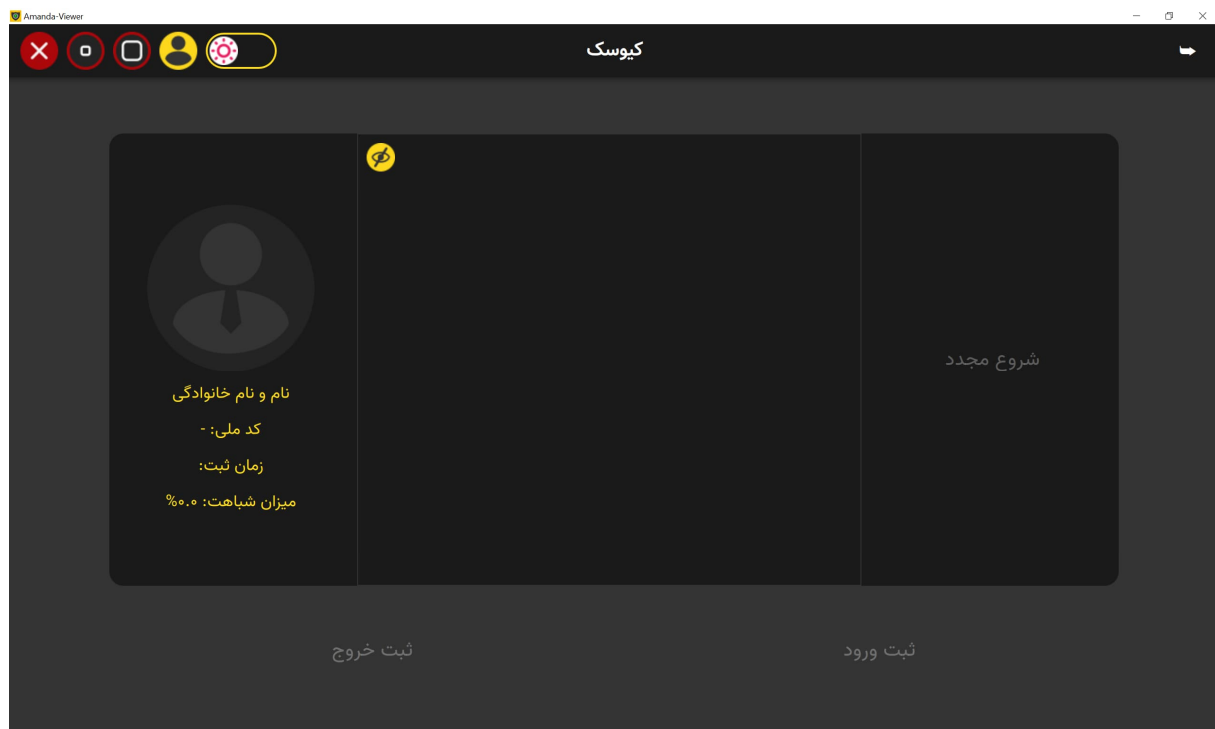


شکل ۲-۳۴: نمایشی از بخش تعیین سطح دسترسی کاربر به دوربین کیوسک

برای اینکه بتوانید دوربینی را به عنوان کیوسک انتخاب کنید، باید در قسمت تعریف و ویرایش دوربین‌ها، تیک چک‌باکس کیوسک آن دوربین را فعال کرده باشید. در غیر اینصورت امکان انتخاب دوربین به عنوان کیوسک امکانپذیر نخواهد بود.



پس از تعریف کاربر کیوسک، نسخه **ناظر** سامانه آمندا را بر روی کامپیوتر کیوسک نصب کرده و با استفاده از حساب کاربری تعریف شده وارد شوید. سپس از **منوی اصلی**، به بخش **کیوسک** بروید. شکل ۲-۳۵ نمای قبل از شروع این بخش را نشان می‌دهد.



شکل ۲-۳۵: نمای قبل از شروع بخش کیوسک

دوربین کیوسک به صورت پیش فرض غیرفعال است. برای فعال سازی آن، کافی است کلید ترکیبی Ctrl+S را فشار داده و منتظر بمانید تا اتصال به دوربین تعریف شده برقرار شود. به همین ترتیب، برای توقف اجرای کیوسک، می توانید از کلید ترکیبی Shift+S استفاده کنید. این کلیدهای ترکیبی جهت جلوگیری از راه اندازی یا توقف غیرمجاز و سهوی کیوسک توسط مراجعه کنندگان تعریف شده اند.

ثبت (اظهار) ورود-خروج: افرادی که قصد ثبت ورود یا خروج از طریق کیوسک را دارند، ابتدا باید دکمه **شروع مجدد** را فشار داده و مقابل دوربین کیوسک قرار گیرند. پس از انجام فرآیند تشخیص چهره، متناسب با نوع کیوسک و قصد ورود یا خروج، لازم است شخص یکی از دکمه های **ثبت ورود** یا **ثبت خروج** را انتخاب کند تا ثبت ورود یا خروج انجام شود.

۱۲-۲) ملاحظات کلیدی برای افزایش دقت و کارایی سامانه آمندا

در طراحی و بهره برداری از سامانه های پیشرفته ای مانند آمندا، دقت و کارایی از عوامل حیاتی برای موفقیت و دستیابی به اهداف تعیین شده به شمار می روند. در این بخش، مجموعه ای از ملاحظات و الزامات فنی و اجرایی ارائه می شود که رعایت آنها **تأثیر مستقیمی** بر بهبود عملکرد سامانه خواهد داشت. این ملاحظات شامل تنظیمات دقیق سخت افزاری و نرم افزاری، بهینه سازی فرآیندها، استفاده صحیح از منابع پردازشی و ذخیره سازی، و همچنین رعایت اصول استاندارد در تعریف و مدیریت داده ها است. برخی از نکات مهم که در این بخش بررسی خواهند شد عبارتند از:



(۱) **مدیریت بهینه منابع سخت‌افزاری و نرم‌افزاری:** تنظیم و بهینه‌سازی پردازش‌ها و اطمینان از تخصیص مناسب منابع به هر بخش از سامانه.

(۲) **تعریف دقیق و صحیح داده‌ها:** توجه ویژه به کیفیت داده‌های ورودی نظیر تصاویر آموزشی و اطلاعات مرتبط با اشخاص و خودروها برای بهبود نتایج تشخیص هوش مصنوعی.

(۳) **بهره‌گیری از الگوریتم‌های پیشرفته:** اطمینان از به‌روز بودن الگوریتم‌های هوش مصنوعی و تطبیق آنها با شرایط عملیاتی سامانه.

(۴) **نگهداری و پایش مستمر:** ارزیابی مداوم عملکرد سامانه و اعمال تغییرات لازم برای برطرف کردن هرگونه کاستی یا افت کیفیت.

(۵) **آموزش کاربران سامانه:** تضمین استفاده بهینه از قابلیت‌ها و امکانات سامانه از طریق آموزش کامل اپراتورها و کاربران نهایی. رعایت این ملاحظات نه تنها موجب ارتقای دقت و کارایی سامانه می‌شود، بلکه با کاهش خطاها و افزایش سرعت پردازش، بهره‌وری کلی سیستم را نیز به میزان قابل توجهی بهبود می‌بخشد. در ادامه، هر یک از این عوامل به تفصیل بررسی خواهند شد.

۲-۱۲-۱) بکارگیری توان پردازشی GPU

تمامی عملیات و فرآیندهای مرتبط با بخش هوشمند سیستم به صورت پیش‌فرض از توان پردازشی CPU استفاده می‌کنند. با این حال، به منظور افزایش بهره‌وری، تشخیص بلادرنگ و کاهش بار محاسباتی CPU، **اکیداً** توصیه می‌شود این فرآیندها با استفاده از GPU انجام شوند. استفاده از GPU علاوه بر کاهش تأخیر، کارایی سیستم را به‌ویژه در محیط‌هایی که تعداد دوربین‌های نظارتی زیاد است، بهبود می‌بخشد.

۲-۱۲-۲) الزامات دوربین‌های نظارت محیطی

برای اجرای فرآیندهای هوشمند نظارت پیرامونی، نظیر تشخیص ورود انسان یا حیوان، تشخیص دود و آتش، یا شناسایی عدم استفاده از کلاه ایمنی در محدوده‌های تعریف شده، استفاده از دوربین‌هایی با حداقل رزولوشن ۲ مگاپیکسل الزامی است. دوربین‌ها باید توانایی ارائه تصاویر با کیفیت و شفافیت مناسب در شرایط مختلف نوری را داشته باشند.

۲-۱۲-۳) الزامات دوربین‌های پلاک‌خوان

برای تشخیص و پلاک‌خوانی، استفاده از دوربین‌هایی با حداقل رزولوشن ۲ مگاپیکسل با سرعت شاتر ۱/۲۰۰ ثانیه و جانمایی مناسب (شامل زاویه دید و فاصله) در محل‌های تردد ضروری است. تنظیم صحیح مکان و زاویه دوربین تأثیر قابل توجهی بر دقت فرآیند پلاک‌خوانی دارد.



۲-۱۲-۴) الزامات دوربین‌های تشخیص و شناسایی چهره

برای دستیابی به دقت مطلوب در تشخیص چهره، رعایت الزامات زیر ضروری است:

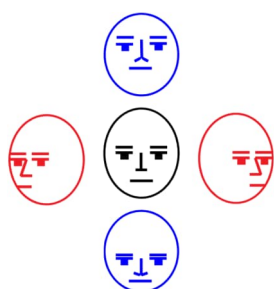
- ارتفاع دوربین از سطح زمین نباید بیش از ۲ متر باشد؛ زاویه دوربین نسبت به سطح افق برای ثبت چهره نباید از ۲۰ درجه تجاوز کند.
- زاویه انحراف افقی دوربین نیز نباید بیشتر از ۳۰ درجه باشد.
- حداقل تراکم پیکسلی مورد نیاز برای شناسایی چهره ۵۰۰ پیکسل بر متر است، به‌طوری که عرض چهره ثبت شده باید حداقل ۸۰ پیکسل باشد.
- فاصله کانونی دوربین باید به صورت دستی یا خودکار قابل تنظیم باشد تا امکان زوم و تمرکز دقیق روی محل ورود-خروج مورد نظر فراهم شود.
- در صورت استفاده از دوربین‌های با لنز ثابت، قطر لنز حداقل باید ۴ میلی‌متر باشد.
- رزولوشن دوربین تشخیص چهره باید حداقل ۴ مگاپیکسل باشد.
- سرعت شاتر دوربین باید حداقل ۱/۲۵۰ ثانیه باشد. برای تحقق این امر، محیط باید از نور کافی برخوردار باشد. وجود نور ناکافی یا نور از پشت^۱ می‌تواند باعث کاهش دقت تشخیص چهره و شناسایی هویت شود.

۲-۱۲-۵) شرایط نمونه‌برداری از چهره اشخاص

برای نمونه‌برداری صحیح از چهره و اطمینان از دقت در فرآیند شناسایی، توجه به نکات زیر الزامی است. رعایت این نکات موجب بهبود دقت و عملکرد سیستم در شناسایی و تطبیق چهره خواهد شد.

- **وضوح کامل چهره:** هر دو چشم باید در تصویر به‌طور کامل مشخص باشند و چهره فرد به صورت مستقیم در مقابل دوربین قرار گیرد.
- **زاویه‌های مختلف:** برای ثبت نمونه‌های متنوع و افزایش دقت شناسایی، لازم است چهره فرد در پنج حالت زیر تصویربرداری شود:

¹ Backlight

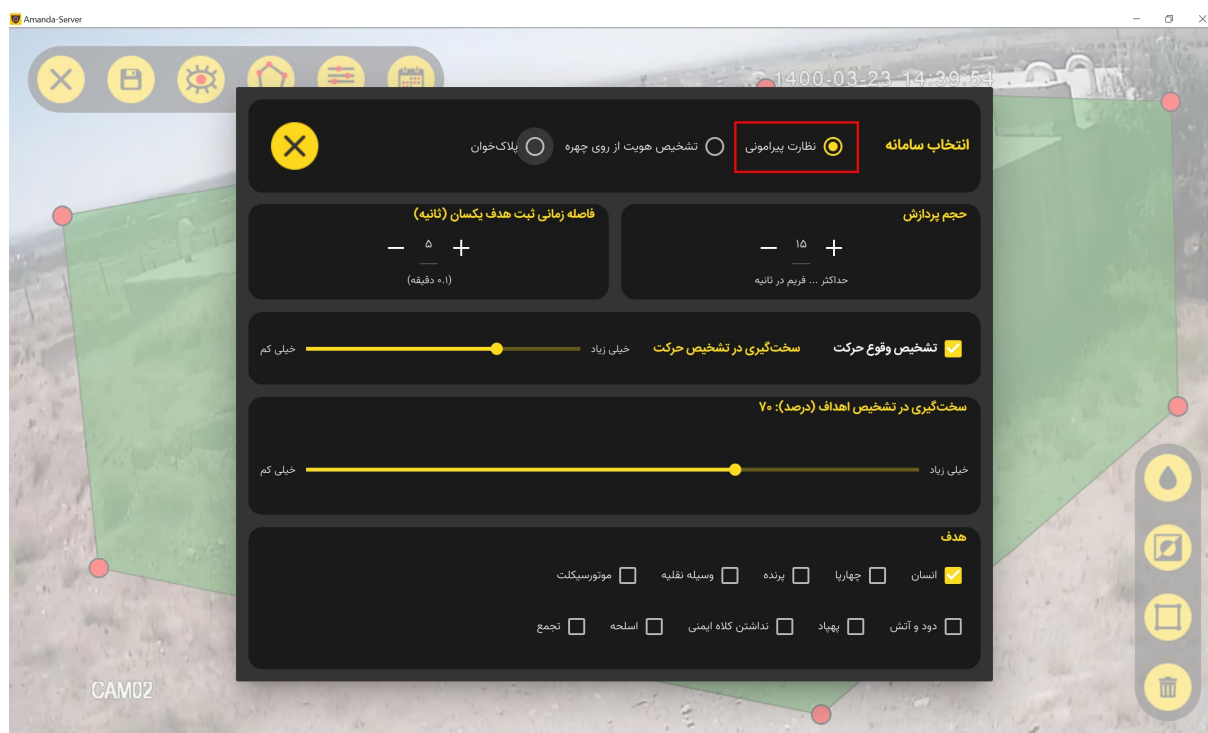


- مستقیم (چهره کاملاً روبروی دوربین)
- ۳۰ درجه به سمت بالا
- ۳۰ درجه به سمت پایین
- ۳۰ درجه به سمت چپ
- ۳۰ درجه به سمت راست

- **تعداد تصاویر:** مجموعاً پنج تصویر با زوایای ذکر شده برای نمونه برداری کافی است.

۲-۱۲-۶ راهنمای تنظیمات مربوط به نوع تشخیص

در شکل ۲-۳۶، سه نما از منوی تنظیمات مربوط به تشخیص هوش مصنوعی دوربین نشان داده شده است. در این منو، امکان تعیین نوع تشخیص دوربین به همراه تنظیمات پارامترهای بسیار مهم فراهم شده است. در ادامه، توضیحات کارکردی هر کدام از آیتم‌ها-پارامترهای موجود در این منو براساس نوع تشخیص و نام هر آیتم-پارامتر ارائه می‌شود.



(الف)



(ب)



(پ)

شکل ۲-۳۶: نمایی از منوی تنظیمات هوش مصنوعی. (الف) نظارت پیرامونی، (ب) تشخیص هویت از روی چهره، (پ) پلاک خوانی

(۱) نظارت پیرامونی

- **حجم پردازش:** این پارامتر مشخص کننده حداکثر تعداد فریم‌هایی است که در هر ثانیه برای انجام عمل تشخیص پردازش می‌شوند. افزایش مقدار این عدد منجر به پردازش تعداد بیشتری از فریم‌های دریافتی از دوربین شده و در نتیجه احتمال افزایش دقت تشخیص را به همراه دارد. با این حال، افزایش حجم پردازش مستلزم مصرف توان پردازشی بیشتری خواهد بود.
- در شرایطی که سرعت حرکت هدف در میدان دید دوربین معمولی است (مانند سرعت حرکت انسان)، تنظیم این مقدار روی مقادیر کمتر از ۵ مناسب و بهینه خواهد بود. اما اگر اهداف مورد نظر سرعت بالایی داشته باشند (مانند پهپادها یا سایر اشیای پرنده)، توصیه می‌شود این مقدار به عددی بالاتر از ۱۲ تنظیم شود تا دقت شناسایی بهبود یابد.
- **فاصله زمانی ثبت هدف یکسان (ثانیه):** این پارامتر تعیین می‌کند که اگر یک هدف مشابه در بازه زمانی مشخص شده شناسایی شود، تنها یکبار ثبت و اطلاع رسانی شود. با استفاده از این تنظیم، از ثبت مکرر یا تکراری یک هدف در طول این بازه زمانی جلوگیری می‌شود و در نتیجه داده‌های تولید شده منسجم‌تر و بهینه‌تر خواهند بود.
- **تشخیص وقوع حرکت:** با فعال‌سازی این گزینه، سامانه نسبت به وقوع حرکت در میدان دید دوربین مورد نظر حساس می‌شود. اگر گزینه تشخیص حرکت و یکی از اهداف **بصورت همزمان** فعال باشند، سامانه تنها در صورت وقوع حرکت در میدان دید دوربین اقدام به شناسایی هدف خواهد کرد. به عبارت دیگر، سامانه ابتدا منتظر ثبت حرکت می‌ماند و سپس بر اساس نوع هدف تعیین‌شده، به شناسایی ماهیت و منشأ آن حرکت می‌پردازد.

پیشنهاد می‌شود در صورت استفاده ترکیبی از تشخیص حرکت و تشخیص هدف، نرخ پردازش را به عددی بالاتر از ۲۰ تنظیم کنید. افزایش این مقدار موجب بهبود دقت تشخیص حرکت شده و به‌طور چشمگیری از هشدارهای کاذب می‌کاهد. شایان ذکر است که در حالت ترکیبی، افزایش این پارامتر تاثیر ناچیزی بر میزان توان مصرفی پردازش خواهد داشت.



- **سخت‌گیری در تشخیص اهداف (درصد):** این پارامتر میزان سخت‌گیری در فرآیند ثبت و اعلام حضور هدف را تعیین می‌کند. به عبارتی، شباهتی که سامانه برای هدف مورد نظر کشف و ثبت می‌کند باید بزرگتر-مساوی این پارامتر باشد تا هشدار صادر شود. انتخاب مقادیر پایین‌تر ممکن است منجر به بروز هشدارهای کاذب^۱ شود و انتخاب مقادیر بالاتر ممکن است باعث نادیده گرفتن اهداف شود. بنابراین، تنظیم صحیح این مقدار می‌تواند به تعادل بین دقت تشخیص و کاهش هشدارهای

¹ False Alarm

اشتباه کمک کند. انتخاب مقدار مناسب برای این پارامتر توسط اوپراتور انجام می‌شود و وابسته به شرایطی محیطی-جغرافیایی و فاصله دوربین از اهداف است.

۲) تشخیص هویت از روی چهره

- **حجم پردازش:** این پارامتر مشخص‌کننده حداکثر تعداد فریم‌هایی است که در هر ثانیه برای انجام فرآیند تشخیص هویت از چهره پردازش می‌شوند. برای شرایط عادی عبور و مرور، پیشنهاد می‌شود عددی بین ۵ الی ۱۰ انتخاب شود.
- **فاصله زمانی ثبت شخص یکسان (ثانیه):** این پارامتر تعیین می‌کند که اگر یک شخص در بازه زمانی مشخص شده شناسایی شود، تنها یکبار حضور آن شخص ثبت شود. با استفاده از این پارامتر، از ثبت مکرر یا تکراری حضور یک شخص در طول این بازه زمانی جلوگیری می‌شود. بعنوان مثال، اگر مدت زمان عبور و مرور از گیت بازرسی بطور میانگین یک دقیقه طول بکشد، پیشنهاد می‌شود این پارامتر روی عدد ۶۰ (ثانیه) تنظیم شود.
- **ثبت و نمایش اشخاص ناشناس:** در صورتی که این آیتم فعال باشد، علاوه بر شناسایی و ثبت چهره‌های شناس، چهره‌های ناشناس نیز ثبت و گزارش خواهند شد.
- **سخت‌گیری در مکان‌یابی صورت (درصد):** این پارامتر میزان سخت‌گیری در فرآیند مکان‌یابی صورت افراد در تصاویر دریافتی از دوربین را تعیین می‌کند. انتخاب مقادیر بالا (مثلاً ۹۰ درصد) موجب کاهش احتمال شناسایی نادرست صورت‌ها می‌شود، در حالی که مقادیر پایین‌تر ممکن است باعث شود که سامانه به اشتباه اشیاء گرد شبیه به صورت و یا الگوهای پیچیده مانند طرح لباس یا طرح روی دیوارها و کاشی‌ها را شبیه صورت انسان ببیند و آنها را به اشتباه صورت شناسایی کند. در شرایطی که محیط از المان‌های پیچیده‌ای برخوردار نباشد، مقدار ۸۰ می‌تواند گزینه مناسبی برای این پارامتر باشد.
- **حداقل عرض صورت مورد قبول (پیکسل):** این پارامتر حداقل عرض صورت (به پیکسل) مورد قبول در تصویر را مشخص می‌کند. به عبارت دیگر، اگر عرض صورت در تصویر کمتر از مقدار تعیین شده باشد، سیستم از احراز هویت آن صرف‌نظر خواهد کرد. این مقدار می‌تواند به دقت سیستم در شناسایی صورت‌های کوچک یا دور از دوربین کمک کند و از شناسایی صورت‌های نامشخص یا مبهم جلوگیری کند.
- حداقل مقدار استاندارد این پارامتر، ۸۰ پیکسل است. با اینحال، در شرایط خاصی که فاصله افراد از دوربین زیاد باشد و ثبت موفق چهره‌ها اولویت بالاتری نسبت به دقت احراز هویت داشته باشد، می‌توان این پارامتر را تا عدد ۱۰ پایین آورد.



- **حداقل میزان شباهت (درصد):** این پارامتر میزان شباهت بین چهره شناسایی شده و پایگاه داده موجود را تعیین می‌کند. به عبارت دیگر، سیستم تنها زمانی یک چهره را شناسایی شده می‌داند که میزان شباهت آن به یکی از داده‌های موجود بزرگتر- مساوی از حد مشخص شده توسط این پارامتر باشد. انتخاب مقادیر بالا برای این پارامتر باعث افزایش دقت در شناسایی و کاهش احتمال احراز هویت اشتباه می‌شود، اما ممکن است منجر به از دست دادن برخی از صورت‌های شناس شود.

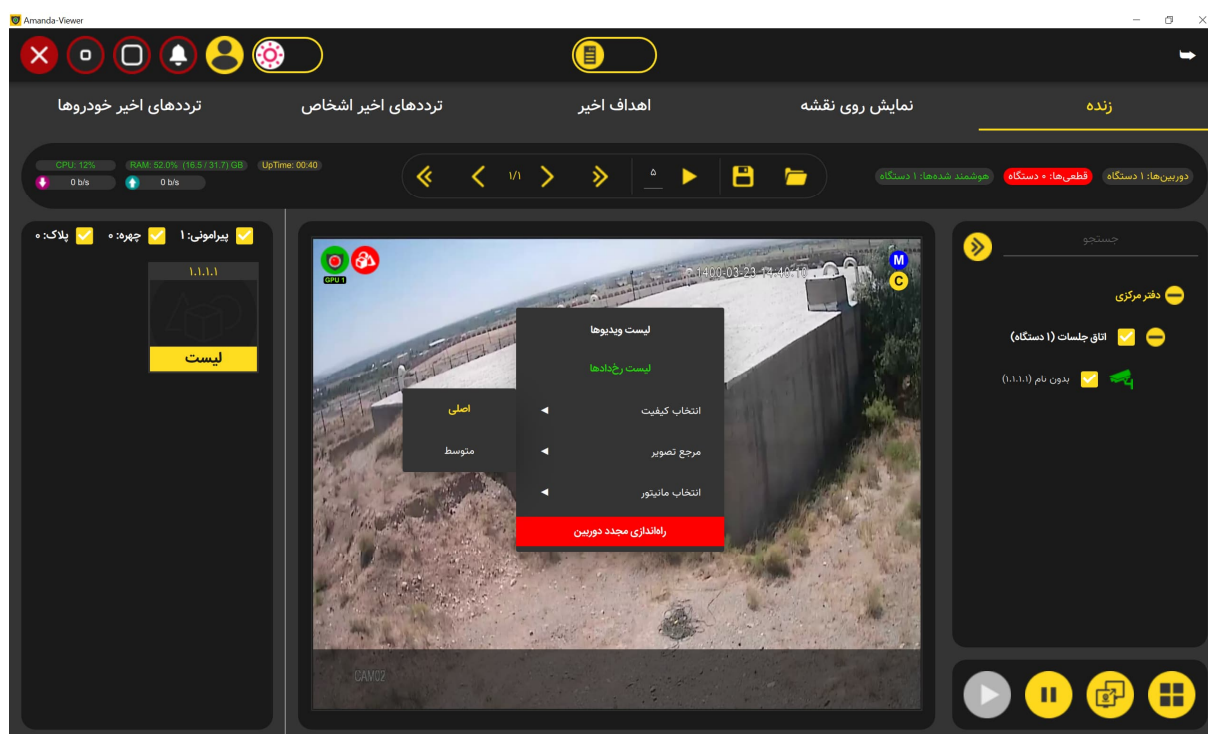
(۳) پلاک‌خوان

- **حجم پردازش:** این پارامتر مشخص‌کننده حداکثر تعداد فریم‌هایی است که در هر ثانیه برای پلاک‌خوانی پردازش می‌شوند. در شرایط عادی عبور و مرور از گیت‌ها، انتخاب عددی بین ۱۲ الی ۱۶ پیشنهاد می‌شود. اما در مواقعی که سرعت عبور و مرور بالا باشد (خیابان‌ها یا معابر اصلی)، پیشنهاد می‌شود مقدار این پارامتر بالای ۲۰ انتخاب شود.
- **فاصله زمانی ثبت پلاک یکسان (ثانیه):** این پارامتر تعیین می‌کند که اگر یک خودرو در بازه زمانی مشخص شده چندین بار شناسایی شود، تنها یک‌بار حضورش ثبت و اعلام شود.
- **ثبت و نمایش پلاک‌های ناشناس، نیمه‌خوانا و ناخوانا:** با فعال کردن هر کدام از این آیتم‌ها، سامانه علاوه بر ثبت پلاک‌های شناس، اقدام به ثبت و نمایش پلاک‌های ناشناس، نیمه‌خوانا و ناخوانا خواهد کرد. در مواقعی که ثبت پلاک بدون خوانش صحیح آن مد نظر باشد، آیتم‌های نیمه‌خوانا و ناخوانا باید فعال باشند.
- پلاک نیمه‌خوانا پلاکی است که یک یا چند عدد از اعداد پلاک غیرقابل شناسایی باشد.
- پلاک ناخوانا، پلاکی است که هیچ یک از اعداد و حروف درج شده روی آن قابل خواندن نباشد.
- **سخت‌گیری در مکان‌یابی پلاک (درصد):** این پارامتر میزان سخت‌گیری در فرآیند مکان‌یابی پلاک خودرو در تصاویر دریافتی را تعیین می‌کند. انتخاب مقادیر بالا (مثلاً ۹۰ درصد) موجب کاهش احتمال شناسایی نادرست پلاک‌ها می‌شود، در حالی که مقادیر پایین‌تر ممکن است منجر به شناسایی نوشته‌ها و یا امان‌های مستطیل شکل بجای پلاک شود. انتخاب مقدار ۸۰ می‌تواند گزینه مناسبی برای اکثر شرایط باشد.
- **سخت‌گیری در تشخیص حروف پلاک (درصد):** این پارامتر میزان شباهت اعداد و حروف به مقدار واقعی آنها را مشخص می‌کند. انتخاب مقداری بین ۲۰ الی ۳۰ می‌تواند گزینه مناسبی برای این پارامتر باشد.

۷-۱۲-۲) انتخاب نوع جریان

برای دوربینی که به هوش مصنوعی مجهز شده است، توصیه اکید می‌شود که **جریان اصلی** برای نمایش تصاویر آن دوربین توسط اپراتور انتخاب شود تا تصاویر اصلی دوربین که کیفیت بالاتری دارند به فرآیند پردازش ارسال شوند. در صورتی که **جریان فرعی** انتخاب شود، به دلیل پایین بودن کیفیت تصاویر در این جریان نسبت به کیفیت تصاویر اصلی، کارایی سامانه در تشخیص اهداف کاهش خواهد یافت. اما در مواقعی که منابع سخت‌افزاری محدودی در اختیار داشته باشید، استفاده از جریان فرعی پیشنهاد می‌شود چراکه به توان پردازشی بسیار کمتری نسبت به تصاویر اصلی نیاز دارند.

برای انتخاب جریان اصلی و یا فرعی، در زمان اجرا (رجوع شود به ۳-۴) روی دوربین مورد نظر کلیک-راست کرده و از گزینه **انتخاب کیفیت** اقدام به تغییر جریان نمایید. شکل ۲-۳۷ نمونه‌ای از این فرآیند را نشان می‌دهد.



شکل ۲-۳۷: نمایی از نحوه انتخاب جریان اصلی یا فرعی برای یک دوربین

۸-۱۲-۲) نکات تکمیلی

- تنظیم مناسب نور محیط، نظیر استفاده از روشنایی اضافی در نقاط سایه‌دار، بهبود قابل توجهی در دقت سیستم تشخیص فراهم می‌کند.
- استفاده از دوربین‌هایی با قابلیت WDR^۱ (دامنه دینامیکی بالا) برای محیط‌های با تضاد نور شدید توصیه می‌شود.
- انتخاب تجهیزات با استانداردهای مقاومتی نظیر IP66 یا IP67 برای محیط‌های بیرونی ضروری است.

¹ Wide Dynamic Range

بخش سوم

راهنمای استفاده

نسخه ناظر



۳) مقدمه

در این بخش، مراحل راه‌اندازی و استفاده از نسخه **ناظر^۱** سامانه آمادها توضیح داده می‌شود. همانطور که در مقدمه بخش دوم هم ذکر گردید، نسخه ناظر سامانه با هدف نظارت و اعمال پردازش‌های مرتبط با هوشمندسازی طراحی و توسعه داده شده است. کاربران-اوپراتورها می‌توانند با نصب این نسخه روی کامپیوترهای خود، به سامانه اصلی (نسخه سرور) وصل شده و براساس سطح دسترسی که توسط کاربر **ادمین^۲** برای‌شان تعریف شده است، فرآیند نظارت را انجام دهند.

۳-۱) ورود به حساب کاربری

پس از اجرای نسخه ناظر، کاربر با صفحه ورود نشان داده شده در شکل ۳-۱ مواجه خواهد شد. آدرس وب سرور نشان داده شده در شکل، آدرس همان ماشینی است که نسخه سرور آمادها روی آن نصب شده است. توجه داشته باشید که پس از وارد کردن آدرس، شماره پورت اتصال (بصورت پیش‌فرض ۳۰۳۰ است) را هم باید طبق شکل درج کنید.



شکل ۳-۱: نمایی از منوی ورود به حساب کاربری در نسخه ناظر آمادها

^۱ Viewer-Client

^۲ Admin



اگر نسخه ناظر روی همان ماشین که نسخه سرور نصب شده اجرا شود، باید در بخش آدرس وب سرور، مقدار 127.0.0.1^۱ را همراه با شماره پورتی که برای وب سرور تعیین شده است، وارد کنید. به عنوان مثال، اگر شماره پورت وب سرور 3030 باشد، مقدار این فیلد باید بصورت 127.0.0.1:3030 وارد شود.



۳-۲) تنظیمات

در نسخه ناظر، نیاز به اعمال تنظیمات پیچیده برای کاربر-اپراتور نیست. تنها نکته مهم، انتخاب پروتکل مناسب ارتباطی و مدیریت فعال سازی یا غیرفعال سازی هوش مصنوعی دوربین ها است.

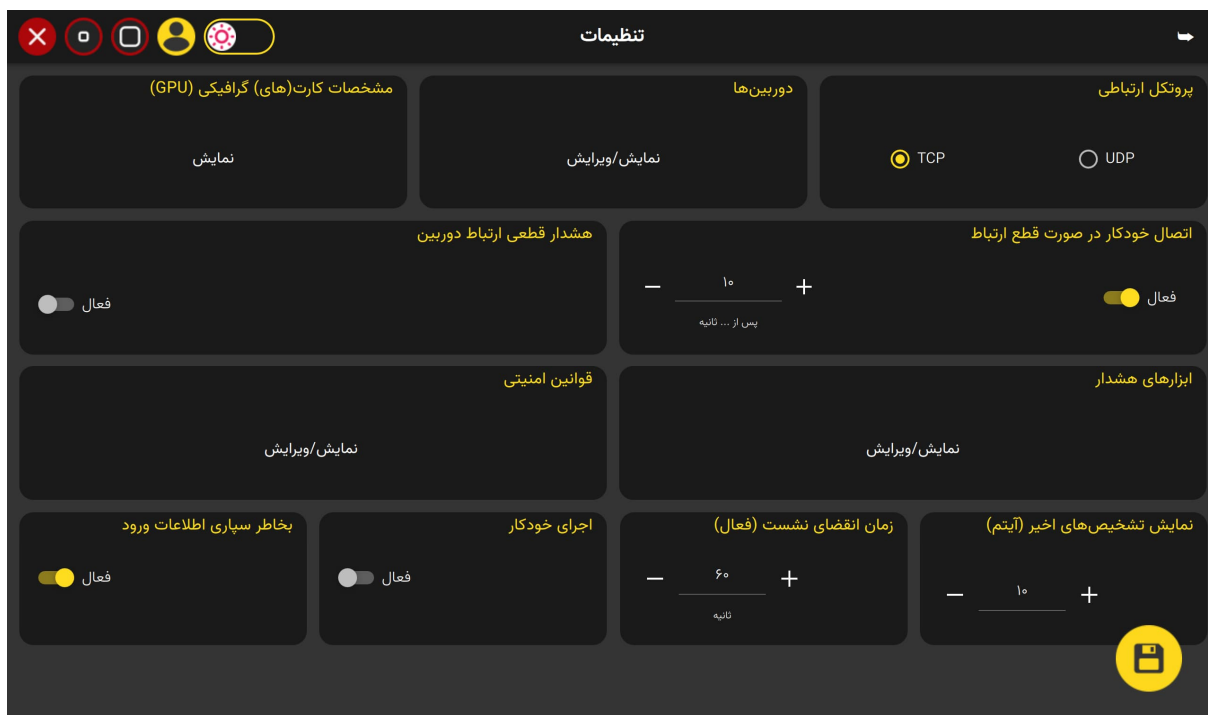
اگر شبکه دوربین ها به درستی پیکربندی شده و از پایداری مناسبی برخوردار است (بدون از دست رفتن بسته های داده)^۲ توصیه می شود از پروتکل ارتباطی UDP برای دریافت تصاویر استفاده کنید، زیرا این پروتکل تأخیر کمتری دارد و عملکرد بهتری در انتقال ویدئو ارائه می دهد. با این حال، اگر در هنگام استفاده از UDP متوجه شدید که تصاویر بصورت شطرنجی یا خاکستری نمایش داده می شوند، احتمالاً بسته های داده در مسیر انتقال از بین می روند. در این صورت، توصیه می شود پروتکل ارتباطی را به TCP تغییر دهید تا انتقال داده ها با اطمینان بیشتری انجام شود.



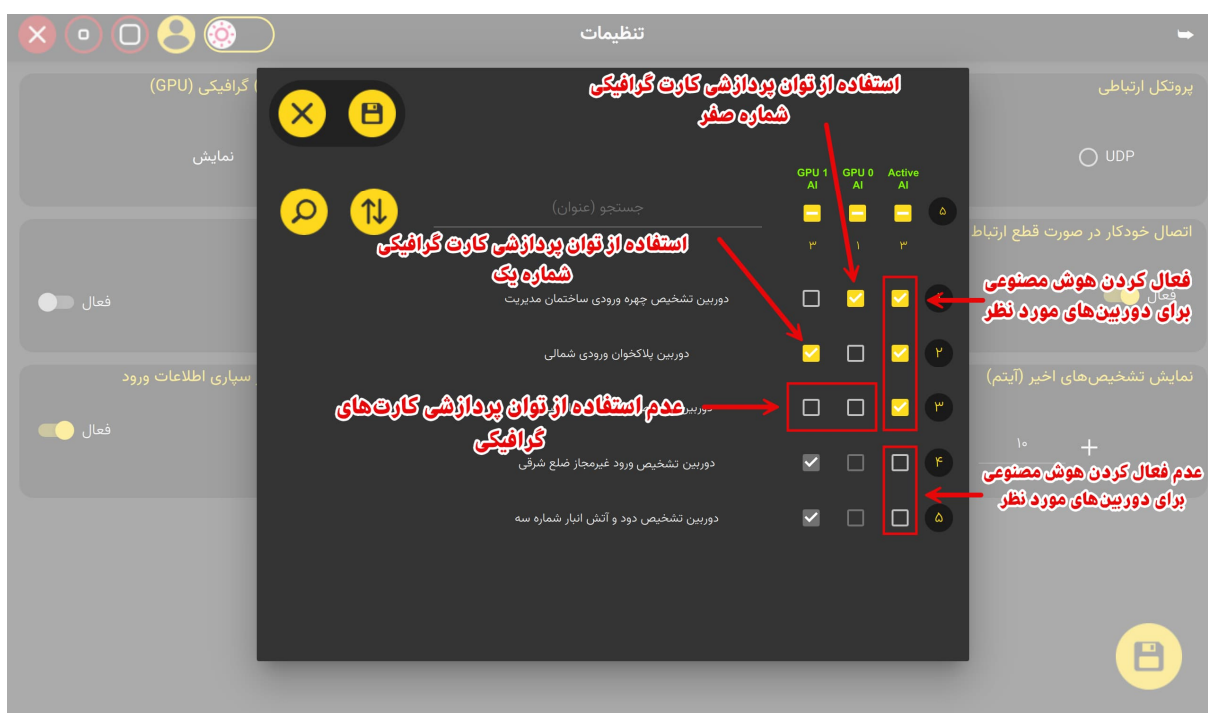
اگر امکان پردازش هوش مصنوعی به کاربری داده شده باشد، کاربر می تواند از طریق بخش **تنظیمات** و ورود به **منوی ویرایش/نمایش دوربین ها**، قابلیت هوش مصنوعی هر دوربین را فعال یا غیرفعال کرده و تعیین کند که هر دوربین از توان پردازشی کدام کارت گرافیکی (GPU0 یا GPU1) استفاده کند. شکل ۳-۲ نمایی از منوی **تنظیمات** و شکل ۳-۳ نمایی از منوی **ویرایش/نمایش دوربین ها** در نسخه ناظر را نشان می دهد.

^۱ 127.0.0.1 که به آن localhost نیز گفته می شود، یک آدرس لوپبک (Loopback) است که برای ارتباط با همان دستگاهی که درخواست از آن ارسال شده، استفاده می شود. این آدرس امکان برقراری ارتباط با سرویس های محلی بدون نیاز به اتصال به شبکه را فراهم می کند.

^۲ Packet Loss



شکل ۳-۲: نمایی از منوی تنظیمات نسخه ناظر آماندا



شکل ۳-۳: نمایی از منوی ویرایش/نمایش دوربین‌ها در نسخه ناظر آماندا

برای آگاهی از تعداد GPUهای موجود در سیستم و ترتیب شناسایی آنها توسط سامانه، می‌توانید از بخش **تنظیمات** منوی **مشخصات کارت(های) گرافیکی**، اقدام به مشاهده آنها نمایید. شکل ۳-۴ نمونه‌ای از این منو را نشان می‌دهد.



شکل ۳-۴: نمایی از منوی نمایش کارت‌های گرافیکی شناسایی شده توسط نسخه ناظر

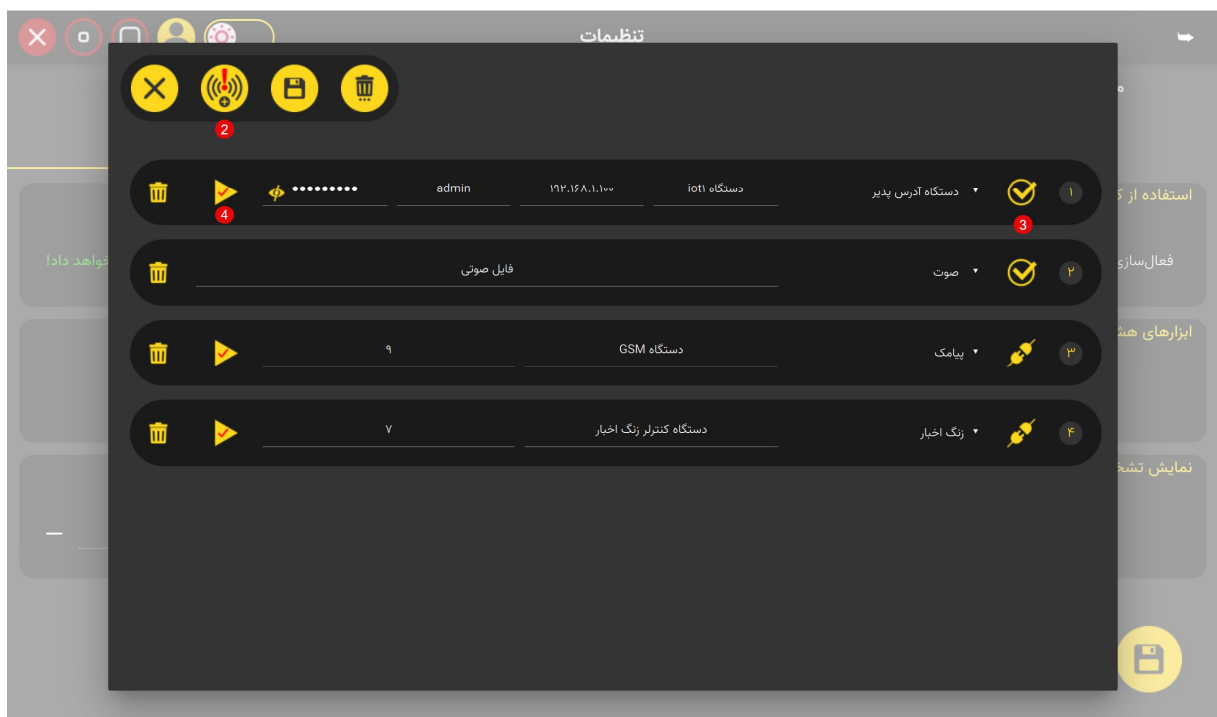
انتخاب صحیح کارت گرافیکی و یا عدم انتخاب آن برای هر دوربین، **تأثیر مستقیمی** در عملکرد سامانه در تشخیص‌های هوشمند خواهد داشت.



۳-۳) تعریف ابزارهای هشدار و قوانین امنیتی

سامانه آماداً در حال حاضر از پنج روش متنوع برای اعلام هشدار استفاده می‌کند: ۱) قرمز کردن پنجره‌ی نمایش دوربین، ۲) به صدا درآوردن آژیر خطر، ۳) پخش صدا، ۴) ارسال پیامک و از همه مهمتر ۵) اتصال به دستگاه آدرس‌پذیر و ارسال سیگنال به آن.

برای استفاده از این ابزارهای هشدار (بجز قرمز کردن پنجره نمایش دوربین)، نخست باید آنها را تعریف کرد؛ از **منوی اصلی** به **تنظیمات** رفته و با فشار دادن دکمه **نمایش/ویرایش ابزارهای هشدار**، اقدام به تعریف ابزارهای هشدار مورد نظر خود نمایید. شکل ۳-۵ مراحل انجام کار را نشان می‌دهد.



شکل ۳-۵: مراحل تعریف ابزارهای هشدار

توجه داشته باشید که به ازای هر دستگاه (پیامک، مازول زنگ اخبار و دستگاه آدرس پذیر) لازم است که ابزار هشدار جداگانه‌ای برای آن تعریف شود. به‌عنوان مثال، اگر دو دستگاه ارسال پیامک دارید، باید برای هر دستگاه بطور مجزا یک ابزار هشدار با شماره پورت^۱ مربوطه تعریف کنید.

^۱ شماره‌ی پورت USB که دستگاه از طریق آن به سیستم متصل است.

یا اگر سه دستگاه آدرس‌پذیر در اختیار دارید، لازم است برای هر دستگاه یک رکورد جداگانه ایجاد شود. اما برای ابزار هشدار صوتی، نیازی به تعریف چندین رکورد نیست و تنها تعریف یک رکورد کافی است.

پس از تعریف هر ابزار هوشمند، باید از اتصال صحیح آن به سیستم اطمینان حاصل کنید. البته این موضوع برای ابزار هشدار صوتی انجام نمی‌شود. برای این منظور، دکمه شماره ۴ را فشار دهید. پس از اتمام بررسی اتصال، وضعیت اتصال در آیتم شماره ۳ به یکی از سه حالت زیر تغییر خواهد کرد:

این آیکون در دستگاه‌های ارسال پیامک و ماژول‌های زنگ اخبار نشان می‌دهد که دستگاه از طریق پورت USB به ماشین میزبان متصل نیست. همچنین، در مورد دستگاه‌های آدرس‌پذیر، این وضعیت به معنای عدم شناسایی دستگاه در شبکه (عدم پاسخ به ping) است که احتمالاً به دلیل وارد نشدن صحیح آدرس IP آن می‌باشد.



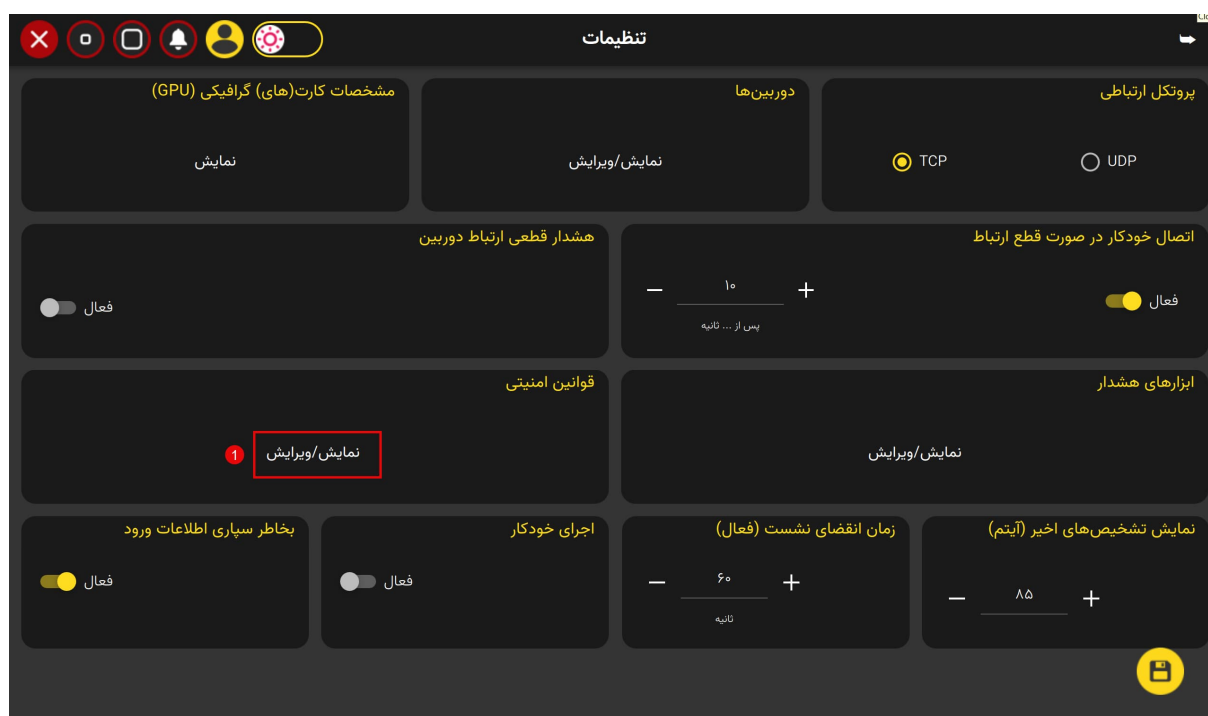
نام کاربری و یا کلمه عبور صحیح نیست (برای دستگاه آدرس‌پذیر).

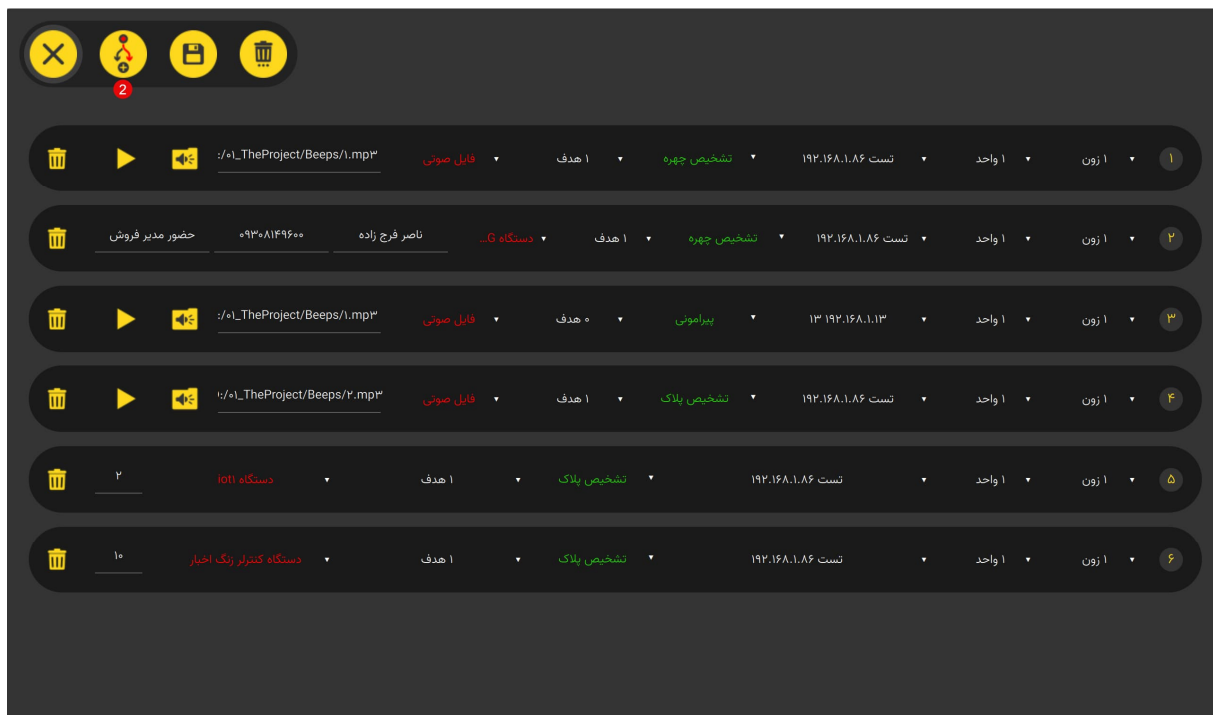


ابزار هشدار متصل است.



پس از اتمام تعریف ابزارهای هشدار، می‌توانید قوانین امنیتی مورد نظر خود را برای هر یک از دوربین‌ها تعریف کنید. برای این کار، دکمه **نمایش/ویرایش قوانین امنیتی** را فشار دهید و مراحل نشان داده شده در شکل ۳-۶ را دنبال کنید.





شکل ۳-۶: مراحل تعریف قوانین امنیتی

برای هر دوربین، می توان به **تعداد نامحدودی قانون امنیتی** تعریف کرد. بعنوان مثال، اگر دوربینی مجهز به هوش مصنوعی تشخیص چهره است، می توانید براساس گروه کارمندی، قوانین امنیتی متفاوتی تعریف کنید. بعنوان مثال دیگر، اگر دوربینی مجهز به هوش مصنوعی تشخیص پلاک است، می توانید برای پلاک های خاص، قوانین مجزایی تعریف کنید.



ابزارهای هشدار و قوانین امنیتی تعریف شده در هر ماشین (کامپیوتر) بصورت محلی ذخیره شده و مختص همان ماشین می باشند. به عبارت دیگر، ابزارها و قوانینی تعریف شده در یک کامپیوتر، تنها برای همان کامپیوتر قابل استفاده هستند. بنابراین، هر کاربری که قصد استفاده از نسخه ناظر را دارد، باید ابزارها و قوانین امنیتی مورد نیاز خود را بصورت محلی و جداگانه تعریف کند.

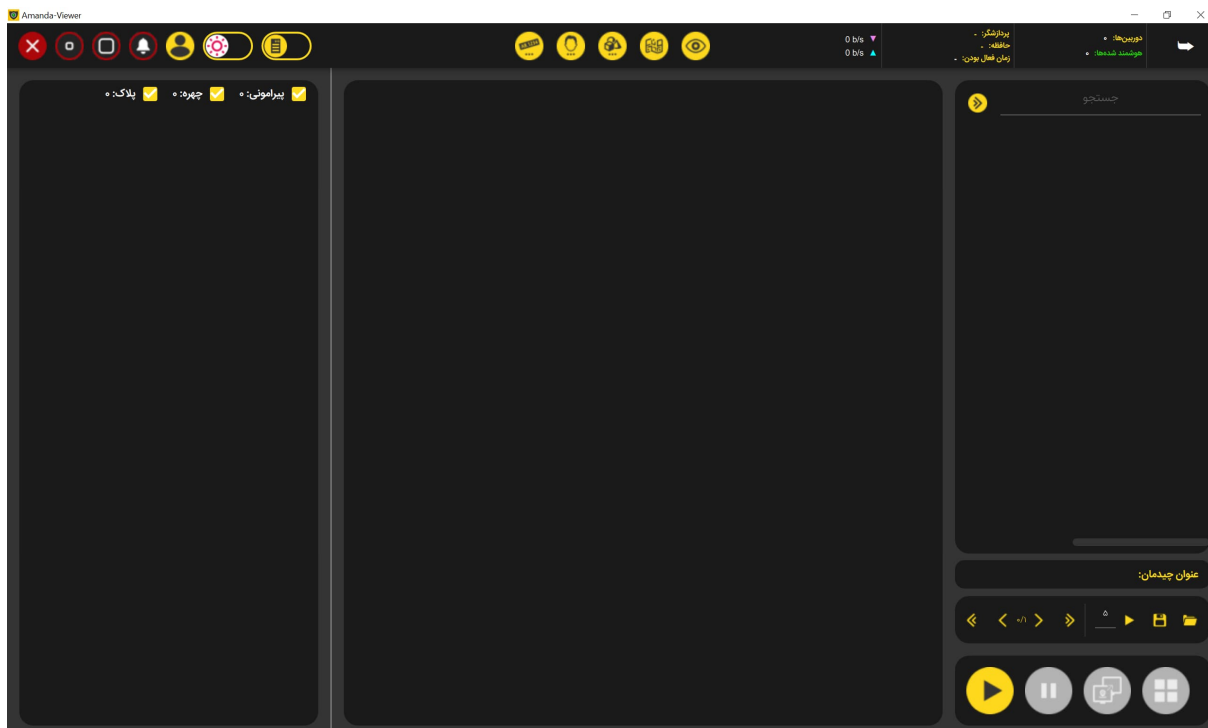


برای تسریع و سهولت تعریف قوانین مشابه، با نگه داشتن کلید Ctrl و فشردن دکمه افزودن **قانون امنیتی** جدید، می توانید کپی آخرین قانون تعریف شده را ایجاد کرده و تغییرات جزئی مورد نظر خود را روی آن اعمال کنید.

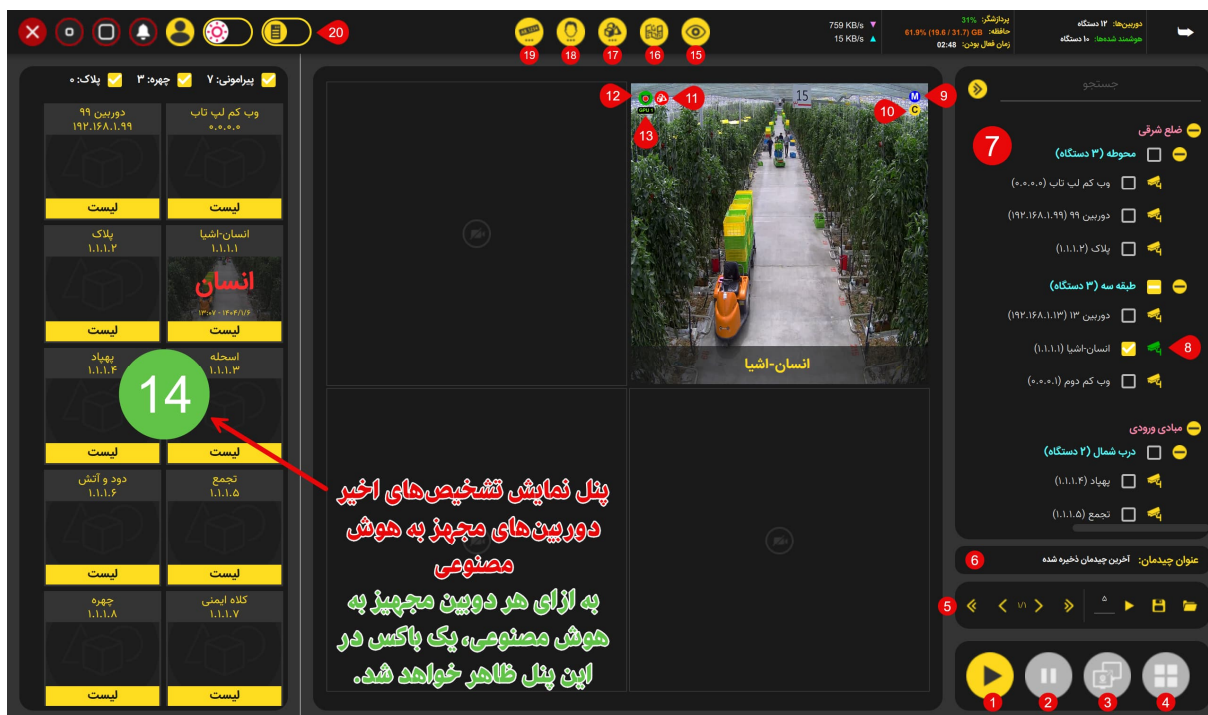


۳-۴) اجرا

پس از انجام تنظیمات مربوط به دوربین ها، زمان آن فرا رسیده است که سامانه را اجرا کرده و از آن بهره برداری کنید. برای اجرای سامانه، از **منوی اصلی** وارد بخش **اجرا** شوید. شکل ۳-۷ نمایی از بخش اجرا را قبل و بعد از شروع اجرا، نشان می دهد.



(الف)



(ب)

شکل ۷-۳: نمایی از حالت اجرای سامانه: (الف) قبل از اجرا، (ب) بعد از اجرا

در ادامه، کارکرد هر یک از آیتم‌های نشان داده شده در شکل ۷-۳ (ب)، توضیح داده می‌شود.



(۱) اجرا: با فشردن این دکمه، سامانه شروع به اتصال به دوربین‌ها و فعال‌سازی هوش مصنوعی هر یک از دوربین‌ها خواهد کرد. پس از بارگذاری کامل، از پنل درختی (آیتم شماره ۵)، دوربین‌های مورد نظر خود را می‌توانید برای نمایش تصویرش به ترتیب دلخواه انتخاب کنید.

(۲) توقف اجرا: فشردن این دکمه باعث توقف اجرا خواهد شد. بسته به حجم پردازش‌های انجام شونده، فرآیند توقف ممکن است چند ثانیه طول بکشد. لازم به ذکر است که تمامی تغییراتی که در زمان اجرا از جمله چیدمان^۱ دوربین‌ها و انتخاب جریان اصلی و یا فرعی برای هر یک از دوربین‌ها اعمال شده است، ذخیره شده و در اجرای بعدی اعمال خواهند شد.

(۳) منوی انتقال تصاویر یک زون-واحد بین مانیتورها: با فشردن این دکمه، منویی برای انتقال تصاویر یک زون-واحد از مانیتوری به مانیتور دیگری در ویدیووال ظاهر می‌شود. لازم به توضیح است که با کلیک-راست روی دوربین مورد نظر و با استفاده از گزینه **انتخاب مانیتور**، می‌توانید تصویر یک دوربین را به مانیتور دلخواه انتقال دهید.

(۴) منوی انتخاب چیدمان‌ها: با فشردن این دکمه، منویی که شامل مجموعه‌ای از چیدمان‌های پیش‌فرض برای دوربین‌ها در صفحه است، ظاهر می‌شود. لازم به ذکر است که با کشیدن تصویر یک دوربین و رها کردن آن روی دوربین دیگر، محل نمایش دو دوربین باهم عوض می‌شود.

(۵) نوار کنترل حرکت بین صفحات: با استفاده از ابزارهای موجود در این بخش، می‌توان بین صفحات نمایش دوربین‌ها جابجا شد. همچنین، کاربر می‌تواند با استفاده از دکمه‌ی **ذخیره** تعبیه‌شده در این نوار، چیدمان فعلی خود را با نام دلخواه ذخیره کرده و در صورت نیاز، مجدداً آنرا بارگذاری کند.

(۶) عنوان چیدمان فعلی: این آیتم عنوان چیدمان فعلی را که کاربر انتخاب کرده است، نمایش می‌دهد.

(۷) پنل نمایش درختی دوربین‌ها: این آیتم امکان دسترسی سریع به دوربین‌ها را براساس زون-واحدی که دوربین‌ها در آن قرار گرفته‌اند، میسر می‌سازد. لازم به ذکر است که ترتیب-محل نمایش هر دوربین در صفحه چیدمان دوربین‌ها، براساس ترتیب فعال کردن چک‌باکس آن دوربین خواهد بود.

(۸) وضعیت جاری دوربین: این آیتم وضعیت جاری دوربین را نشان می‌دهد:

اتصال به دوربین برقرار نیست.



¹ Layout



اتصال به دوربین برقرار است.



اتصال به دوربین برقرار است و هوش مصنوعی آن نیز فعال شده است.



اتصال به دوربین برقرار است ولی هوش مصنوعی آن فعال نشده است.



اتصال به دوربین برقرار نیست ولی هوش مصنوعی آن فعال شده است.



۹) نشانگر نوع جریان دوربین:

جریان اصلی در حال نمایش است. لازم به توضیح است که با کلیک-راست دوربین مورد نظر و با استفاده از گزینه **انتخاب کیفیت**، می‌توانید نوع جریان را مشخص کنید.



جریان فرعی در حال نمایش است.



۱۰) مرجع تصویر: این آیتم مرجع تصویر دوربین را نشان می‌دهد:

تصاویر از سرور (بصورت غیر مستقیم) دریافت می‌شوند.



تصاویر بصورت مستقیم از دوربین دریافت می‌شوند.



۱۱) نشانگر نوع تشخیص هوش مصنوعی دوربین:

تشخیص حرکت



تشخیص اشیا شامل انسان، چهارپا، پرنده، وسیله نقلیه، موتورسیکلت



تشخیص شی پرنده



تشخیص اسلحه



تشخیص دود و آتش





تشخیص به سرنداشتن کلاه ایمنی



شمارش و تشخیص تجمع



تشخیص هویت از روی چهره



تشخیص پلاک



۱۲) نشانگر وضعیت جاری هوشمندی دوربین:

هوش مصنوعی دوربین غیرفعال است.



هوش مصنوعی دوربین فعال است اما طبق زمانبندی، هنوز زمان فعالیت آن شروع نشده است.



هوش مصنوعی دوربین فعال است اما فنسی برای مراقبت تعریف نشده است.



هوش مصنوعی دوربین فعال است.



۱۳) نشانگر وضعیت جاری استفاده از توان پردازشی GPU: نمایش داده شدن این نشانگر به این معنی است که از GPU برای

پردازش‌های هوشمند این دوربین استفاده می‌شود.

۱۴) پل نمایش لیست تشخیص‌های دوربین‌ها: در این پل، به ازای هر دوربینی که به هوش مصنوعی مجهز شده است، آیتمی

نمایش داده می‌شود که تشخیص‌های اخیر همان دوربین را نمایش می‌دهد. این آیتم‌ها اطلاعات مربوط به شناسایی‌های انجام‌شده را

به صورت بلادرنگ از بافر بارگذاری می‌کنند. به همین دلیل، پس از توقف و اجرای مجدد سامانه، محتوای این آیتم‌ها خالی می‌شود

و با ورود داده‌های جدید از دوربین، به تدریج تکمیل خواهد شد.

۱۵) برگه نمایش اجرا: این برگه وضعیت اجرایی سامانه را نمایش می‌دهد.

۱۶) برگه نمایش نقشه: با انتخاب این برگه، نقشه دو بعدی تعریف شده به همراه دوربین‌هایی که روی آن چیده شده‌اند، نشان داده

می‌شود. با دابل-کلیک کردن روی هر کدام از دوربین‌ها، تصاویر دریافتی از آن دوربین نشان داده می‌شود.



(۱۷) برگه نمایش اهداف اخیر: با انتخاب این برگه، حداکثر ۱۰۰ هدف کشف‌شده‌ی اخیر توسط دوربین‌های پیرامونی قابل مشاهده

است. برخلاف آیتم‌های مربوط به نمایش تشخیص‌های اخیر هر دوربین که محتوای آن‌ها هنگام توقف و اجرای مجدد سامانه خالی می‌شود، این برگه و همچنین برگه‌ی نمایش تردهای اخیر اشخاص و خودروها از پایگاه داده بارگذاری می‌شوند. بنابراین، اطلاعات این بخش‌ها پایدار بوده و پس از راه‌اندازی مجدد سامانه نیز قابل دسترسی باقی می‌مانند.

(۱۸) برگه نمایش تردهای اخیر اشخاص: با انتخاب این برگه، حداکثر ۱۰۰ مورد تردد اخیر (شناس یا ناشناس) اشخاص که توسط

دوربین‌های تشخیص هویت ثبت شده‌اند، قابل مشاهده خواهد بود.

(۱۹) برگه نمایش تردهای اخیر خودروها: با انتخاب این برگه، حداکثر ۱۰۰ مورد تردد اخیر خودرویی (شناس یا ناشناس) ثبت شده

توسط دوربین‌های پلاک‌خوان قابل مشاهده خواهد بود.

(۲۰) آیتم تغییر مرجع تصاویر: با تغییر حالت این آیتم، مرجع تصاویر دریافتی همه دوربین‌ها بصورت یکپارچه از دوربین به سرور و یا

برعکس انجام می‌گیرد. لازم به توضیح است که با کلیک-راست روی هر دوربین، می‌توانید از منوی ظاهر شده مرجع تصویر را بصورت مجزا برای هر دوربین مشخص نمایید.

در حالت عادی، تصاویر دوربین‌ها از طریق سرور تامین می‌شود. در صورتی که سرور به هر دلیلی از مدار خارج شود، ناظرها می‌توانند تا برپایی مجدد سرور و بازگشت آن به مدار، تصاویر را با اتصال مستقیم به دوربین‌ها دریافت کنند.

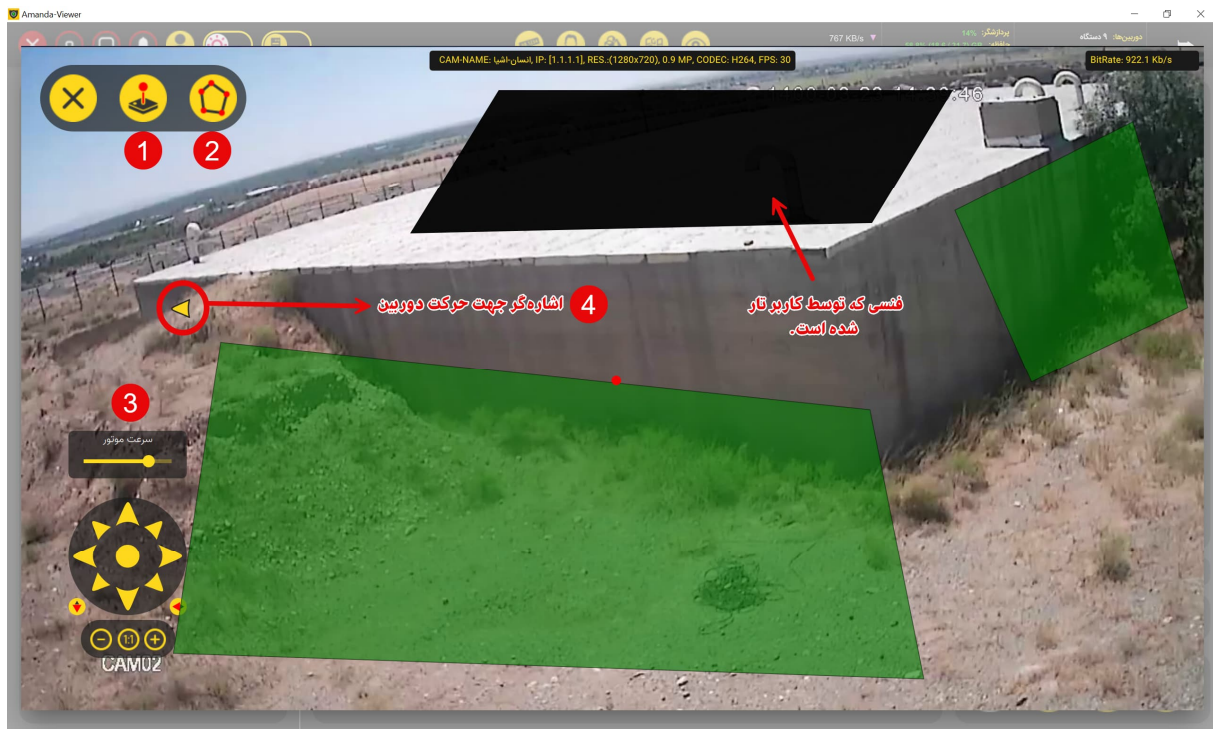


برای مشاهده جریان اصلی هریک از دوربین‌ها، کافی است روی دوربین مورد نظر کلیک کرده تا تصویر جریان اصلی آن به نمایش در آید. شکل ۳-۸، نمایی از منوی نمایش جریان اصلی دوربین را نشان می‌دهد.

با فشردن آیتم شماره ۱، کنترلر دوربین چرخشی نمایان می‌شود که به شما امکان تغییر زاویه دید دوربین را می‌دهد. علاوه بر این، با حرکت ماوس به سمت نقطه مورد نظر و نگه داشتن دکمه چپ آن (مطابق نشانگر مشخص شده در آیتم شماره ۴) می‌توانید زاویه دوربین را در همان جهت تنظیم کنید. همچنین، با چرخاندن چرخ^۱ ماوس به جلو یا عقب، امکان زوم روی نقطه مورد نظر فراهم می‌شود.

با فشردن آیتم شماره ۲، فنس‌های ایجاد شده روی میدان دوربین ظاهر می‌شوند. توجه داشته باشید آن دسته از فنس‌هایی که تار شده باشند، روی صفحه نمایش تصویر چه در حالت جریان اصلی و چه در حالت جریان فرعی، ظاهر خواهند شد.

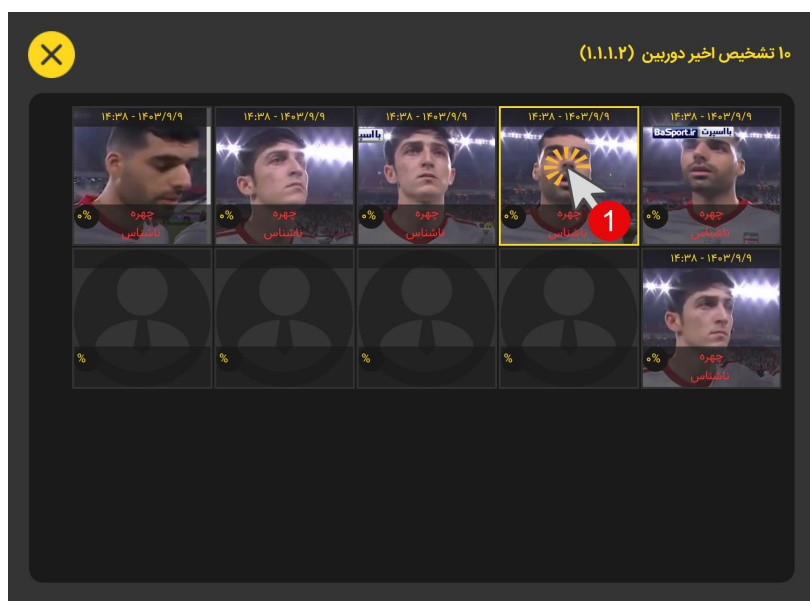
¹ Scroll

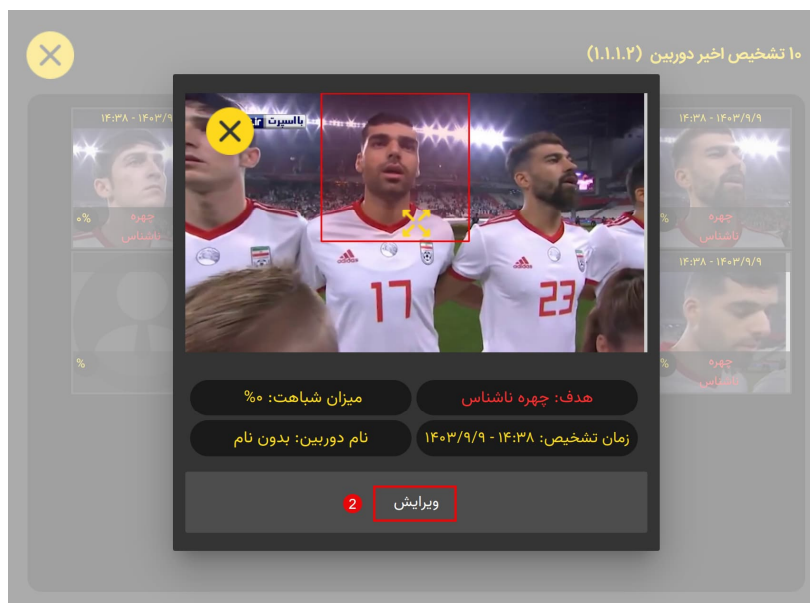


شکل ۳-۸: نمایی از نمایش جریان اصلی دوربین در زمان اجرا

۳-۵) ثبت نام برخط اشخاص

از این روش زمانی استفاده می شود که نیاز به ثبت نام برخط و آنی اشخاص باشد؛ در زمان اجرا، لیست تشخیص های اخیر دوربین مورد نظر را باز کرده و روی تصویر چهره ثبت شده کلیک نمایید تا منویی که شامل تصویر صورت شخص و جزئیات تشخیص است، ظاهر شود. سپس مراحل نشان داده شده در شکل ۳-۹ را برای ثبت نام برخط اشخاص دنبال کنید.





درج نام فارسی، نام خانوادگی فارسی و کد ملی ضروری است.

نام:	مهدی
نام خانوادگی:	طاهری
نام انگلیسی:	FirstName
نام خانوادگی انگلیسی:	LastName
کد ملی:	۱۳۳۴۵۶۷۸۹۱
سمت:	هیچکدام
شغل:	نامعلوم
تاریخ تولد:	۱۳۰۵/۰۵/۰۵
شماره همراه:	۰۹۰۰۰۰۰۰۰۰
شماره پرسنلی:	۰

4

شکل ۳-۸: مراحل ثبت نام برخط اشخاص

با فشار دادن دکمه شماره ۳ در شکل ۳-۹، فرآیند ثبت نام برخط به اتمام می‌رسد. پس از این مرحله، آیتم جدیدی تحت عنوان **آموزش تصویر چهره ثبت شده** در کنار آیتم شماره ۳ ظاهر خواهد شد (آیتم شماره ۱ در شکل ۳-۱۰). با فشردن این دکمه و تعیین حداقل عرض صورت مورد قبول، تصویر ثبت شده به عنوان تصویر چهره شخص مورد نظر به سیستم آموزش داده می‌شود. شکل ۳-۱۰ نمونه‌ای از فرآیند کار را نشان می‌دهد.

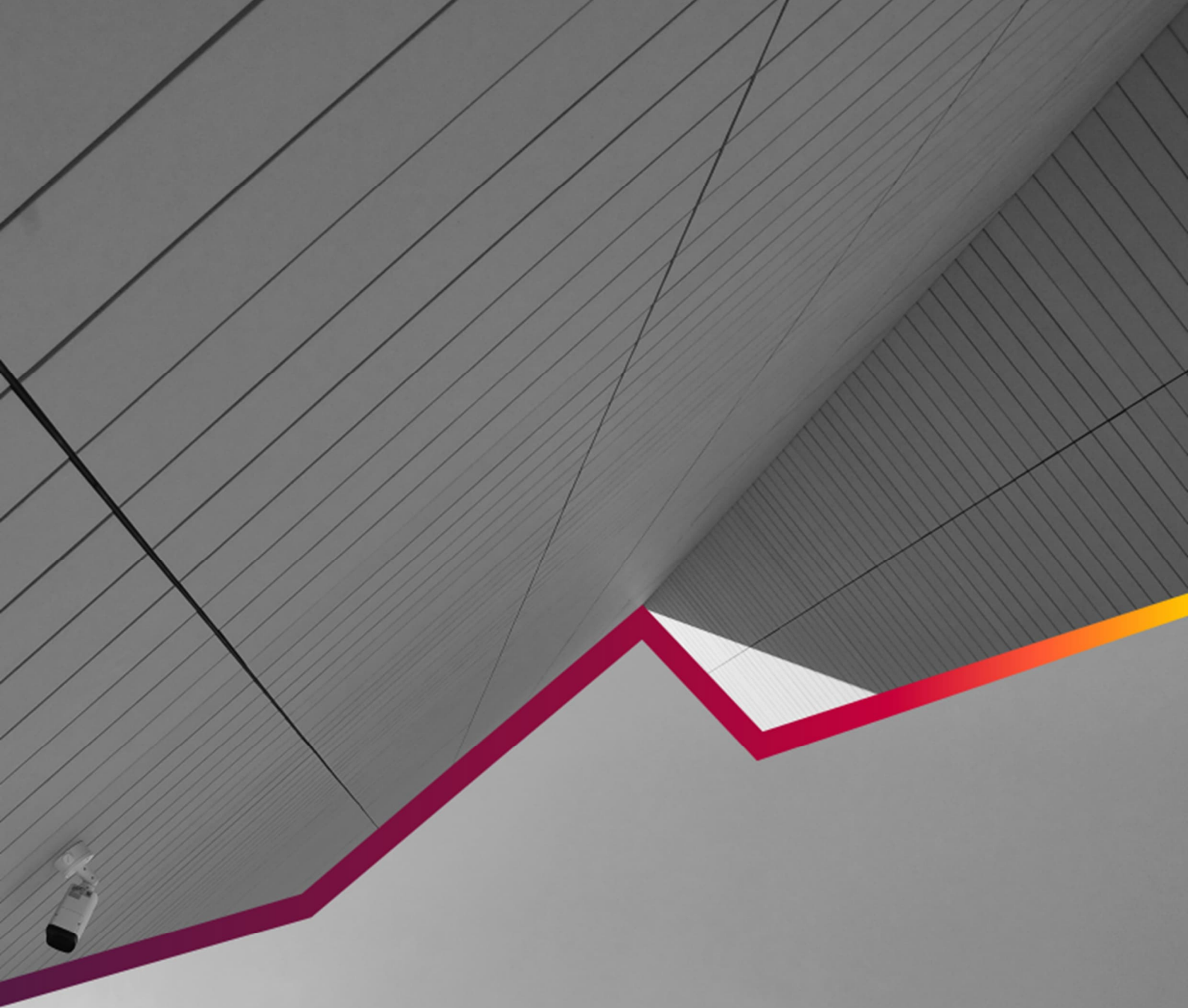
اگر تصویر چهره‌ی شخصی که قبلاً در سامانه ثبت‌نام شده است، تحت عنوان ناشناس گزارش شده باشد، می‌توانید با وارد کردن کد ملی آن شخص و فشردن دکمه شماره ۴ (نشان داده شده در شکل ۳-۹)، اطلاعات آن شخص را از پایگاه داده سامانه بارگذاری کنید و در صورت تمایل، تصویر چهره ثبت شده از وی را به سامانه آموزش دهید.



فرآیند ثبت خودرو به صورت برخط مشابه فرآیند ثبت‌نام برخط افراد انجام می‌شود، با این تفاوت که برای ثبت خودرو به نام یک شخص، لازم است ابتدا آن شخص در سامانه ثبت‌نام شده باشد.



شکل ۳-۱۰: مراحل آموزش برخط تصویر ثبت شده برای شخص مورد نظر



A M A N D A[®]

AI POWERED