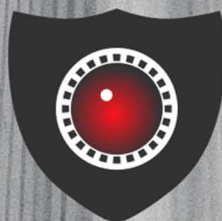


آماندا

سامانه پایش هوشمند تصویری



A M A N D A[®]

زمستان ۱۴۰۴



A M A N D A[®]

محصول دانش بنیان

قدرت گرفته از هوش مصنوعی



شماره: CBP-C1808-0301
تاریخ: ۱۴۰۳/۱۲/۲۰

گواهی ارزیابی امنیتی محصول

بدینوسیله تأیید می‌گردد محصول «سالمه مدیریت و نظارت هوشمند تصویری آمندا» نسخه 2.2.1 از شرکت «هوشمند پردازان فرانکرها» به شماره ثبت «۵۰۵۱۶» با سطح یک از نظام ارزیابی و اعتبار بخشی امنیتی محصولات منطبق و گواهی صادره تنها منحصر به این نسخه از محصول است.

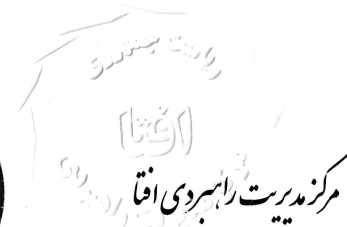
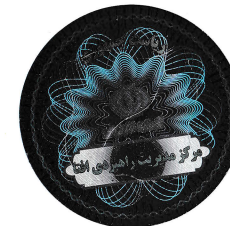
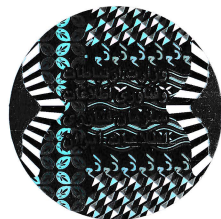
شماره گواهی	CBP-C1808-0301	تاریخ صدور	۱۴۰۳/۱۲/۲۰	مدت اعتبار	دو سال
نام آزمایشگاه	صنایع امنیت فضای تبادل اطلاعات (صافتا)	شماره آزمون	TRP-Amanda	شماره تعهدنامه	CBRP-C1808-0301

دارنده گواهی متعهد به رعایت تعهدنامه و تضمین کیفیت است.

حفظ اعتبار در طول دوره اعتبار گواهی منوط به تأیید آن در سایت سازمان فناوری اطلاعات ایران به آدرس sec.ito.gov.ir است.

گواهی بدون مهر برجسته و لوگوگرام و لوگوی سازمان فناوری اطلاعات ایران و مرکز مدیریت راهبردی اوراق اعتبار است.

شخصه های امنیتی ارزیابی شده، در سندهای امنیتی محصول بیان شده است.





قراگاه پدافند سایی کشور



جمهوری اسلامی ایران



سازمان پدافند غیر عامل کشور

کوپینامه صلاحیت بهره برداری از محصولات پدافند سایی

شماره: ۱۴۰۴/۱۰/۱/سی/۰۱

تاریخ: ۱۴۰۴/۱۱/۰۱

مدیر عامل محترم شرکت هوشمند پردازان فرانگر هما جناب آقای ناصر فرج زاده

با استناد به اساسنامه سازمان پدافند غیر عامل کشور و وظیفه ناشی از تبصره بند یکم از بخش ۴ مصوبه شماره ۱۲۷/۱۲۰/۴۰۰ مورخ ۱۳۹۲/۰۴/۰۵ کمیته دائمی پدافند غیر عامل کشور، صلاحیت بهره برداری از سامانه هوشمند مدیریت و نظارت تصویری با نام تجاری **آماندا** متعلق به آن شرکت به شماره ثبت ۵۰۵۱۶ مورد تایید می باشد.

لذا به آن شرکت اجازه داده می شود؛ از تاریخ صدور به مدت یک سال از محصول خود در راستای ارتقاء امنیت، ایمنی و پایداری در زیر ساخت های مهم کشور بهره برداری نماید.

رئیس سازمان پدافند غیر عامل کشور

س. ت. باسدار دکتر غلامرضا جلالی



الزامات:

- ✓ رعایت قوانین، مقررات و دستورالعمل های فنی و اجرایی کشور و سازمان پدافند غیر عامل الزامی می باشد.
- ✓ واگذاری حقوق متعلق به این گواهینامه به غیر ممنوع می باشد.
- ✓ ارائه گزارش مستمر (۳ ماهه) از انجام پروژه ها و اقدامات جهت تمدید و ارتقاء گواهینامه الزامی می باشد.
- ✓ در صورت ایجاد تغییرات در سامانه، تیم فنی یا مدیریتی شرکت، اطلاع رسانی به سازمان پدافند غیر عامل کشور الزامی می باشد.

آدرس: تهران، بزرگراه شهید قاسم سلیمانی، خیابان استاد حسن بنا (مجیدیه شمالی) روبروی بوستان امیدوار، سازمان پدافند غیر عامل کشور شماره: ۰۲۱-۲۵۹۳۵۶۱۰



دانشگاه صنعتی مالک اشتر

شماره گواهینامه: NEZARAT-01-1036

تاریخ صدور: ۱۴۰۱/۱۲/۱۶

مدت اعتبار: ۲ سال



جمهوری اسلامی ایران
وزارت دفاع و پشتیبانی نیروهای مسلح

شماره سند: MUT-QM-F-T-0801

گواهینامه امنیت محصول

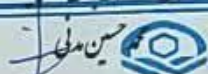
آزمایشگاه ارزیابی امنیتی محصولات و سامانه‌های فاوا

بدین وسیله گواهی می‌شود محصول با مشخصات زیر، مشروط به رعایت شرایط و الزامات اعتبار گواهی نامه، صرفاً جهت استفاده در «شبکه داخلی وزارت دفاع و پشتیبانی نیروهای مسلح (آرماد)» مورد تایید آزمایشگاه ارزیابی امنیتی محصولات و سامانه‌های فاوا (مساف) می‌باشد.

نام محصول	نسخه
سامانه هوشمند مدیریت و نظارت تصویری آماندا	۲.۲.۱



مجمع دانشکاهی برق و کامپیوتر



دانشگاه صنعتی مالک اشتر
مجمع دانشکاهی برق و کامپیوتر



فهرست

بخش اول معرفی ۴

(۱) مقدمه ۵

(۱-۱) مدیریت دوربین‌ها و تصاویر ضبط شده ۶

(۲-۱) برپایی فنس مجازی ۶

(۳-۱) تشخیص انواع اشیاء و اهداف ۷

(۴-۱) تشخیص و شناسایی هویت از روی چهره ۹

(۵-۱) تشخیص انواع اسحله ۱۰

(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) تشخیص ترک پُست نگهبانی-بازرسی یا محل کار ۱۷

(۱۲-۱) باز-ارسال تصاویر و ایجاد محدودیت در دسترسی مستقیم به دوربین‌ها ۱۷

(۱۳-۱) معماری، انعطاف‌پذیری و مقیاس‌پذیری ۱۸

(۱-۱۳-۱) ویژگی‌ها و مزایای استفاده از معماری توزیع شده ۱۸

(۱۴-۱) زیرسامانه‌های هشدار ۲۰

(۱۵-۱) آمار و گزارش‌گیری ۲۱

(۱۶-۱) ایجاد کیوسک‌های متعدد برای ثبت ورود-خروج ۲۱

(۱۷-۱) ویژگی‌های فنی سامانه ۲۱

(۱۸-۱) ویژگی‌های کاربردی سامانه ۲۳

بخش دوم: راهنمای نسخه سرور ۲۶

(۲) مقدمه ۲۷

(۱-۲) راه‌اندازی سرویس‌ها ۲۸

(۲-۲) معرفی ناحیه (زون) و واحد (یونیت) ۲۹

(۳-۲) تعریف و اتصال به دوربین‌ها ۳۱

(۱-۳-۲) پنل دوربین ۳۵



۳۹.....	۲-۳-۲) بارگذاری فایل ویدیویی به جای دوربین
۴۰.....	۴-۲) ایجاد نقشه و چیدن دوربین‌ها روی نقشه
۴۳.....	۵-۲) تنظیمات مربوط به مدیریت ویدیوها و تصاویر
۴۵.....	۶-۲) برپایی فنس مجازی و فعال‌سازی هوش مصنوعی
۵۱.....	۷-۲) راهنمای ثبت‌نام اشخاص شناس (کارمندان-پرسنل)
۵۱.....	۱-۷-۲) راهنمای ثبت‌نام گروهی اشخاص با استفاده از فایل اکسل
۵۵.....	۲-۷-۲) ثبت‌نام مجزای اشخاص
۶۰.....	۸-۲) افزودن و ویرایش کاربر
۶۳.....	۹-۲) راه‌اندازی کیوسک

۲-۱) ملاحظات کلیدی برای افزایش دقت و کارایی سامانه آماد..... ۶۵

۶۶.....	۱-۱۰-۲) یکارگیری توان پردازشی GPU
۶۶.....	۲-۱۰-۲) الزامات دوربین‌های نظارت محیطی
۶۶.....	۳-۱۰-۲) الزامات دوربین‌های پلاک‌خوان
۶۷.....	۴-۱۰-۲) الزامات دوربین‌های تشخیص و شناسایی چهره
۶۷.....	۵-۱۰-۲) شرایط نمونه‌برداری از چهره اشخاص
۶۸.....	۶-۱۰-۲) راهنمای تنظیمات مربوط به نوع تشخیص
۷۳.....	۷-۱۰-۲) انتخاب نوع جریان
۷۳.....	۸-۱۰-۲) تنظیمات ویدیو و تصویر دوربین

بخش سوم: راهنمای نسخه ناظر سامانه ۷۵

۷۶.....	۳) مقدمه
۷۶.....	۱-۳) ورود به حساب کاربری
۷۷.....	۲-۳) تنظیمات
۷۹.....	۳-۳) تعریف ابزارهای هشدار و قوانین امنیتی
۸۲.....	۴-۳) اجرا
۸۸.....	۱-۴-۳) نمایش جریان اصلی و کنترل دوربین
۸۸.....	۲-۴-۳) قابلیت زوم اُپتیکال و دیجیتال
۹۰.....	۳-۴-۳) بازپخش ویدیوهای ضبط شده
۹۱.....	۵-۳) آمار و گزارش‌گیری
۹۲.....	۶-۳) ثبت‌نام برخط اشخاص

بخش چهارم: راهنمای نسخه تحت وب سامانه ۹۶

۹۷.....	۴) مقدمه
---------	----------



۹۸..... (۱-۴) ورود به حساب کاربری

۹۸..... (۲-۴) نظارت آنلاین

۹۹..... (۳-۴) گزارش گیری

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 به‌موقع 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 این‌رو، ضروری است با بهره‌گیری از فناوری‌های پیشرفته، عملیات نظارت و کنترل را هوشمند کرده و به حداکثر کارایی دست یافت.

در این راستا، سامانه پایش هوشمند تصویری **آماندا**^۱ با طراحی کاملاً بومی و مبتنی بر دانش روز معرفی می‌گردد. این سامانه با بهره‌گیری از فناوری‌های نوین، از قابلیت‌های پیشرفته و منحصربه‌فردی برخوردار است که آن را به گزینه‌ای متمایز در حوزه نظارت و مدیریت تصویری هوشمند تبدیل می‌سازد.

بومی بودن این سامانه سه مزیت کلیدی و ارزشمند به همراه دارد:

- (۱) امکان شخصی‌سازی و سفارشی‌سازی سامانه بر اساس نیازهای خاص کارفرما
- (۲) امکان بررسی کدهای منبع به‌منظور اطمینان از موارد زیر:
 - عدم نشت یا سرقت اطلاعات، از جمله اطلاعات مرتبط با دوربین‌ها و تصاویر ثبت‌شده
 - نبود بدافزار در ساختار نرم‌افزاری^۲
 - عدم وجود بمب‌های ساعتی یا کدهای مخرب پنهان^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 کشور بر پایه آخرین دستاوردهای علمی در حوزه فناوری اطلاعات و هوش مصنوعی توسعه یافته است. سیستم یکپارچه مذکور، علاوه بر ارائه مدیریت و نظارت تصویری پیشرفته، طیف وسیعی از قابلیت های هوشمندسازی را نیز در اختیار کاربران قرار می دهد. در ادامه، ویژگی های متنوع و برجسته این سامانه معرفی خواهد شد که آن را به گزینه ای بی رقیب در زمینه مدیریت پیشرفته سیستم های نظارتی بدل می سازد.

۱-۱) مدیریت دوربین ها و تصاویر ضبط شده

برای دستیابی به حداکثر کارایی در سامانه های نظارت تصویری، نخستین و مهم ترین گام، ایجاد بستری است که در آن کاربر بتواند به سادگی دوربین های 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 دوربین ها روی نقشه، ارسال تصاویر دریافت شده از طریق شبکه یا بستر وب برای مشاهده آنلاین از راه دور، از دیگر ویژگی های مهم چنین سامانه هایی به شمار می روند.

ما مفتخریم که تمامی این قابلیت ها را به شکلی بهینه و کارآمد در سامانه **آماندا** پیاده سازی و توسعه داده ایم، به گونه ای که کاربران با حداقل آشنایی با چنین سیستم هایی، می توانند بدون درگیر شدن با پیچیدگی های فنی رایج، از امکانات متنوع بخش مدیریت تصاویر (VMS^۲) این سامانه بهره مند شوند. این امکانات شامل تعریف دوربین ها، تنظیمات مربوط به ضبط تصاویر، ایجاد گروه های ضبط، جستجو و بازپخش ویدئوهای ضبط شده، تعریف نقشه و جانمایی دوربین ها روی آن، مشاهده تصاویر و وضعیت فعلی دوربین ها 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 فنس های فلزی و سیم های خاردار، رویکردی متداول در حفاظت فیزیکی برای جلوگیری از ورود غیرمجاز به حریم های ممنوعه است. با این حال، هزینه خرید، نصب و نگهداری چنین تجهیزات سخت افزاری بسیار بالاست و با گذر زمان این هزینه ها به طور قابل توجهی افزایش می یابد.

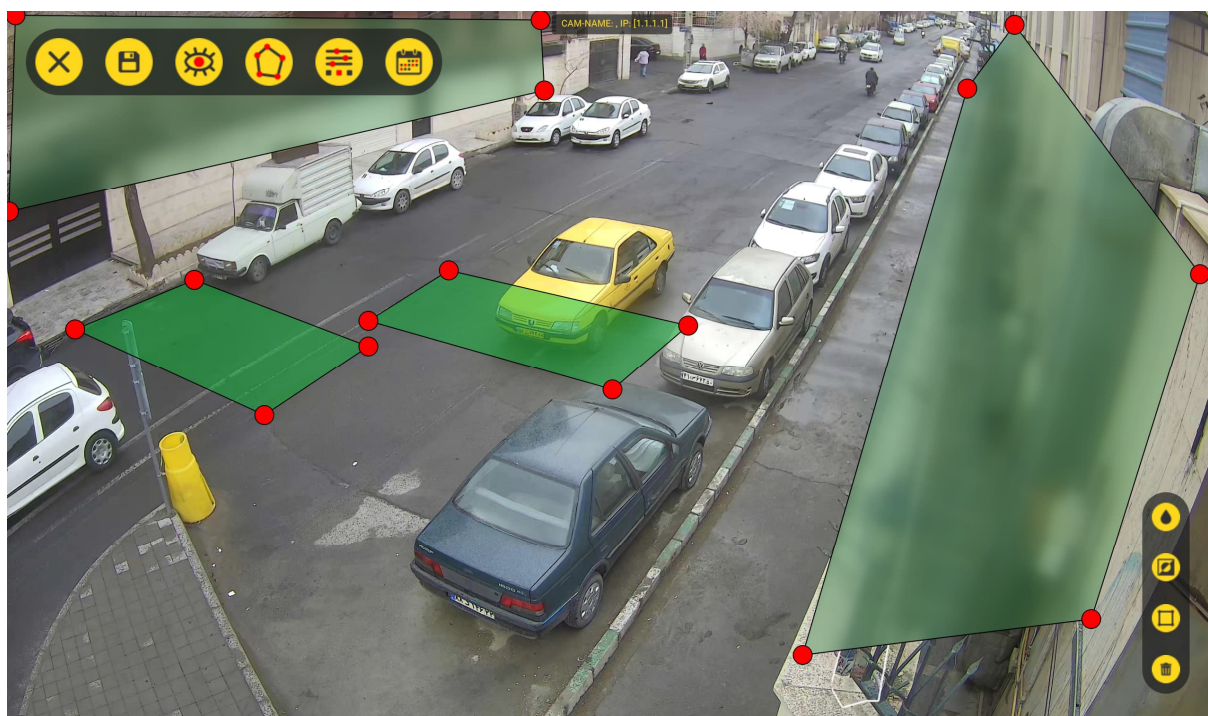
سامانه آماندا امکان تعریف و برپایی فنس های مجازی را به سادگی و تنها با چند کلیک در میدان دید دوربین مورد نظر فراهم می کند. کاربران می توانند این محدوده ها را مطابق با نیاز خود تعریف کرده و سامانه را نسبت به هرگونه نقض قوانین حفاظتی در این محدوده ها حساس سازند. این رویکرد نه تنها نیاز به خرید و نصب تجهیزات سخت افزاری گران قیمت را به طور کامل برطرف می کند، بلکه دقت و انعطاف پذیری بیشتری در مدیریت حریم های ممنوعه به کاربران ارائه می دهد. شکل ۱-۱ نمونه ای از فنس های مجازی ایجاد شده توسط کاربر را که به رنگ سبز نمایان

^۱ Video Wall

^۲ Video Management System

^۳ Restream

شده‌اند، نشان می‌دهد. همچنین، کاربر می‌تواند ناحیه‌ای مشخص را تار کند تا در هنگام نظارت، این بخش از دید اپراتور مخفی بماند و حریم خصوصی حفظ شود.



شکل ۱-۱: نمونه‌ای از حریم‌های (فنس مجازی) ایجاد شده در سامانه آماندا

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.



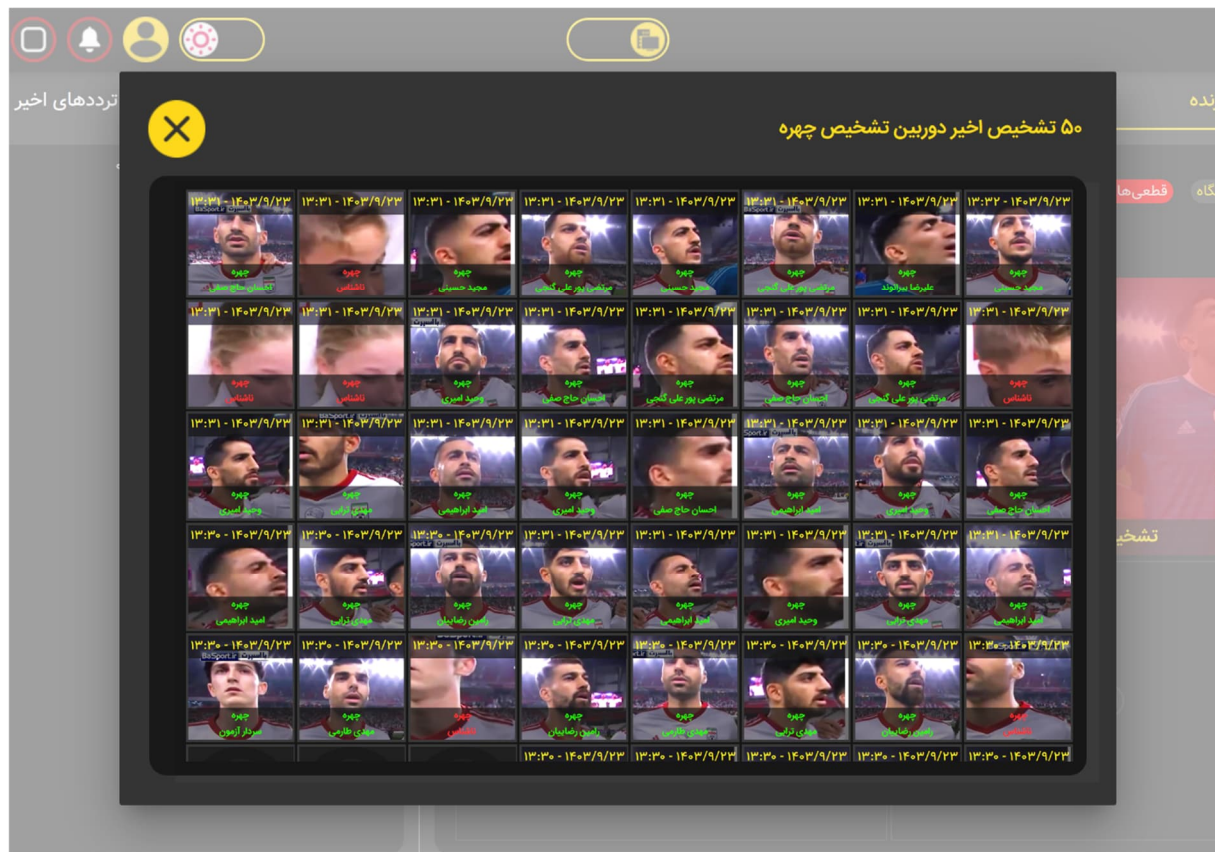


شکل ۱-۲: نمونه‌ای از توانایی سامانه آماندا در تشخیص اشیاء مختلف

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 به‌صورت 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.

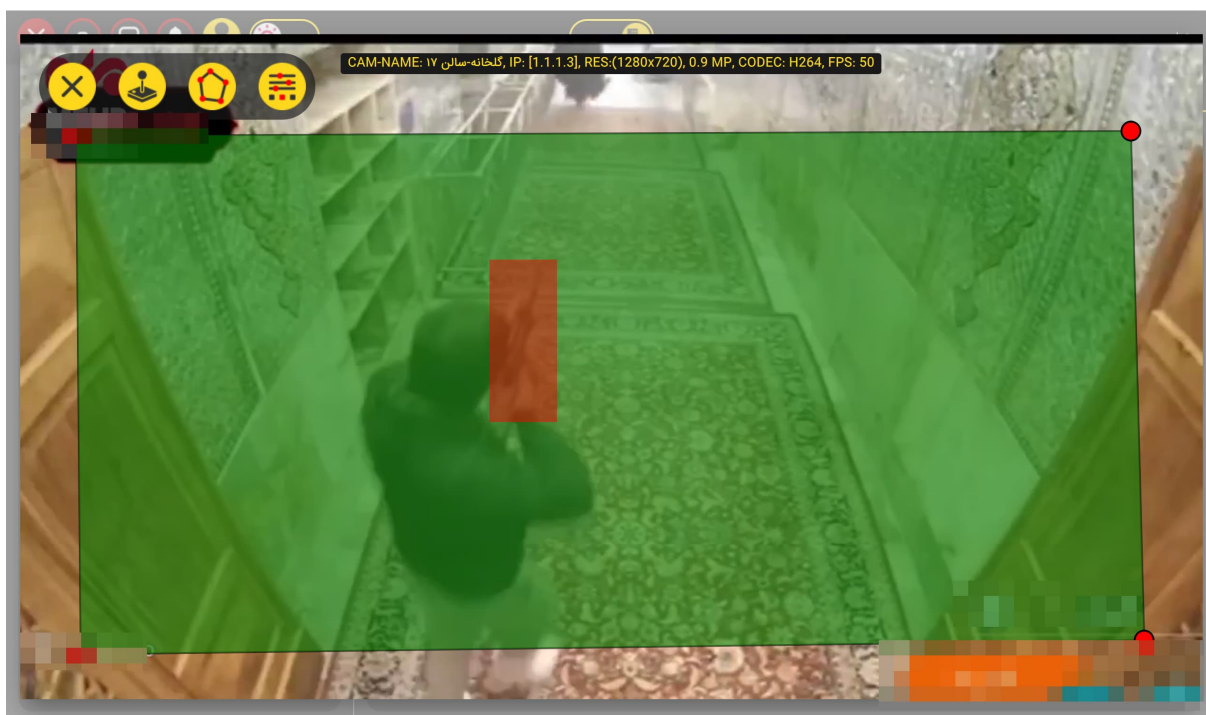


شکل ۱-۳: نمونه‌ای از توانایی سامانه آماد در تشخیص هویت افراد از روی چهره

نمونه‌ای از عملکرد سامانه در شکل ۱-۳ 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.

۱-۵) 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.





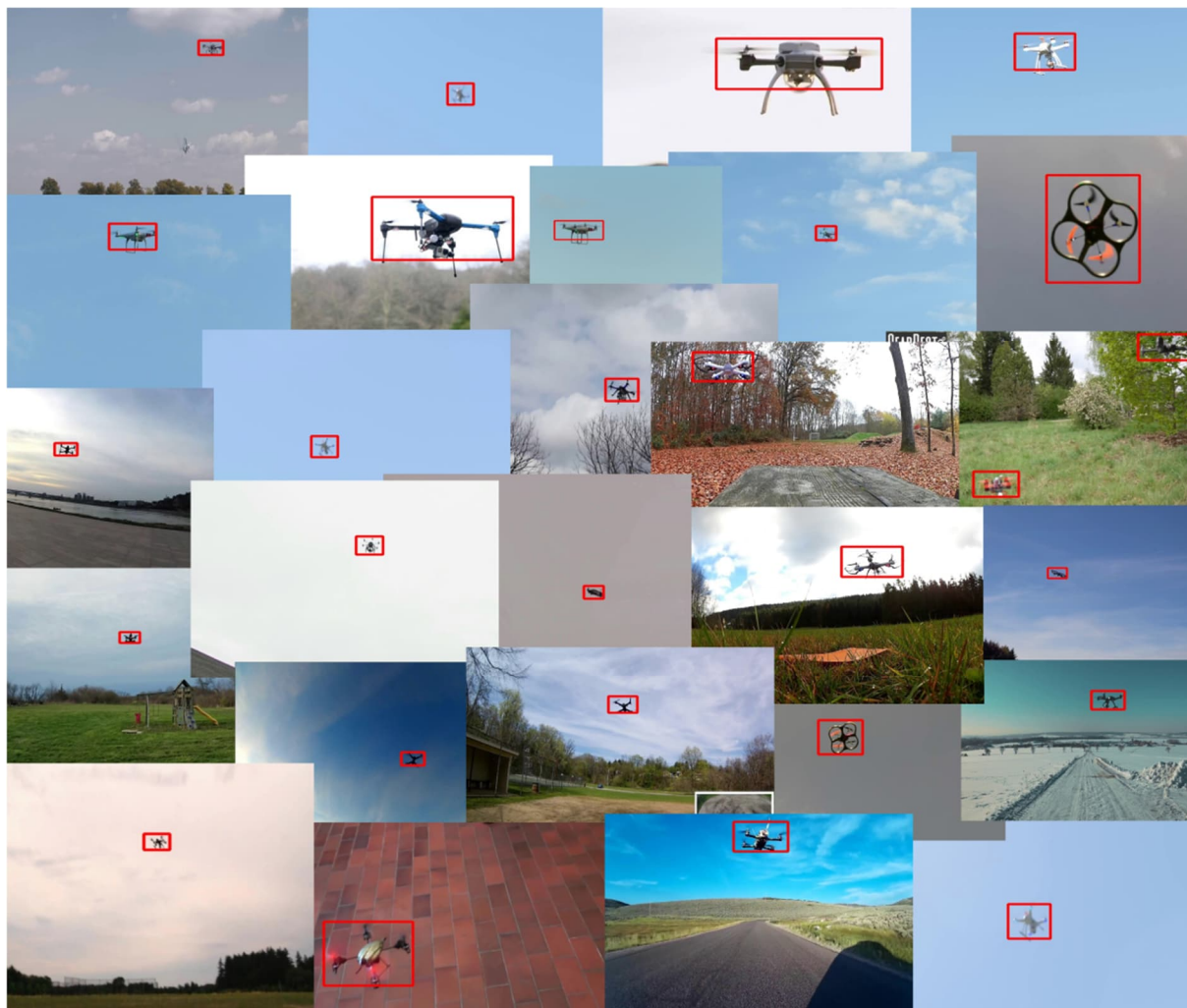
شکل ۱-۴: نمونه‌ای از عملکرد آماندا در تشخیص اسلحه در حالت‌های مختلف

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.



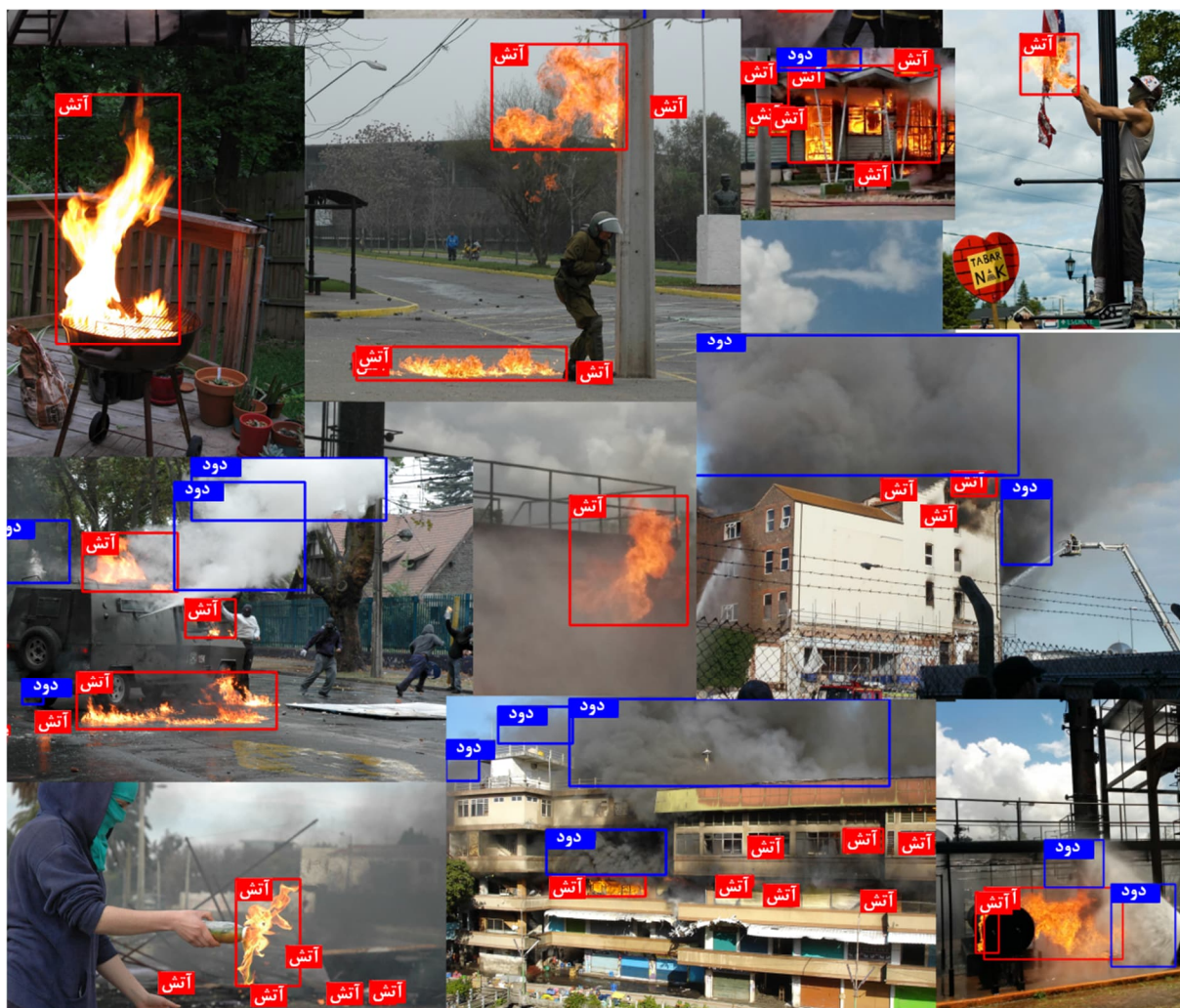
شکل ۱-۵: نمونه‌های از اشیای پرنده شناسایی شده توسط سامانه آماندا

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.



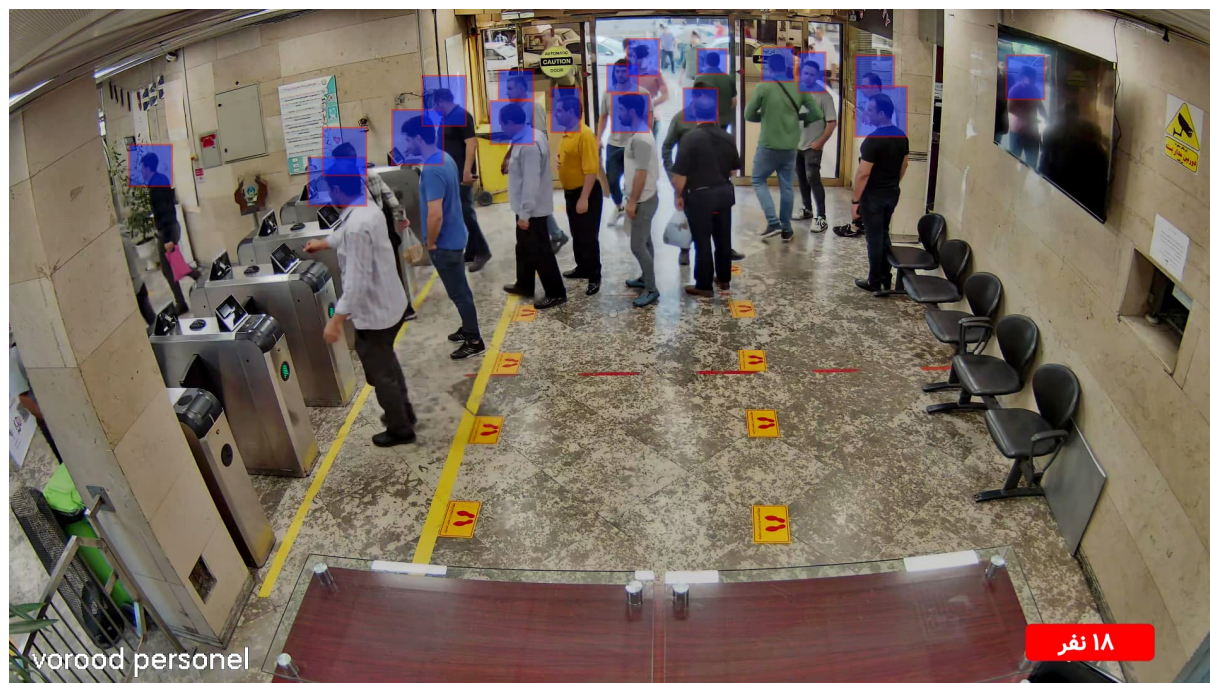
شکل ۷-۱: نمونه‌ای از کارایی سامانه آماندا در تشخیص به سر داشتن یا نداشتن کلاه ایمنی

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.

[illegible]

۱-۱۱) تشخیص ترک پُست نگهبانی-بازرسی یا محل کار

۱-۱۲) باز-ارسال تصاویر و ایجاد محدودیت در دسترسی مستقیم به دوربین‌ها

17

راحتی به تصاویری که به طور زنده از دوربین‌ها ارسال می‌شود، به صورت 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.

۱-۱۳) معماری، انعطاف‌پذیری و مقیاس‌پذیری

سامانه آماد از دو معماری متفاوت پشتیبانی می‌کند:

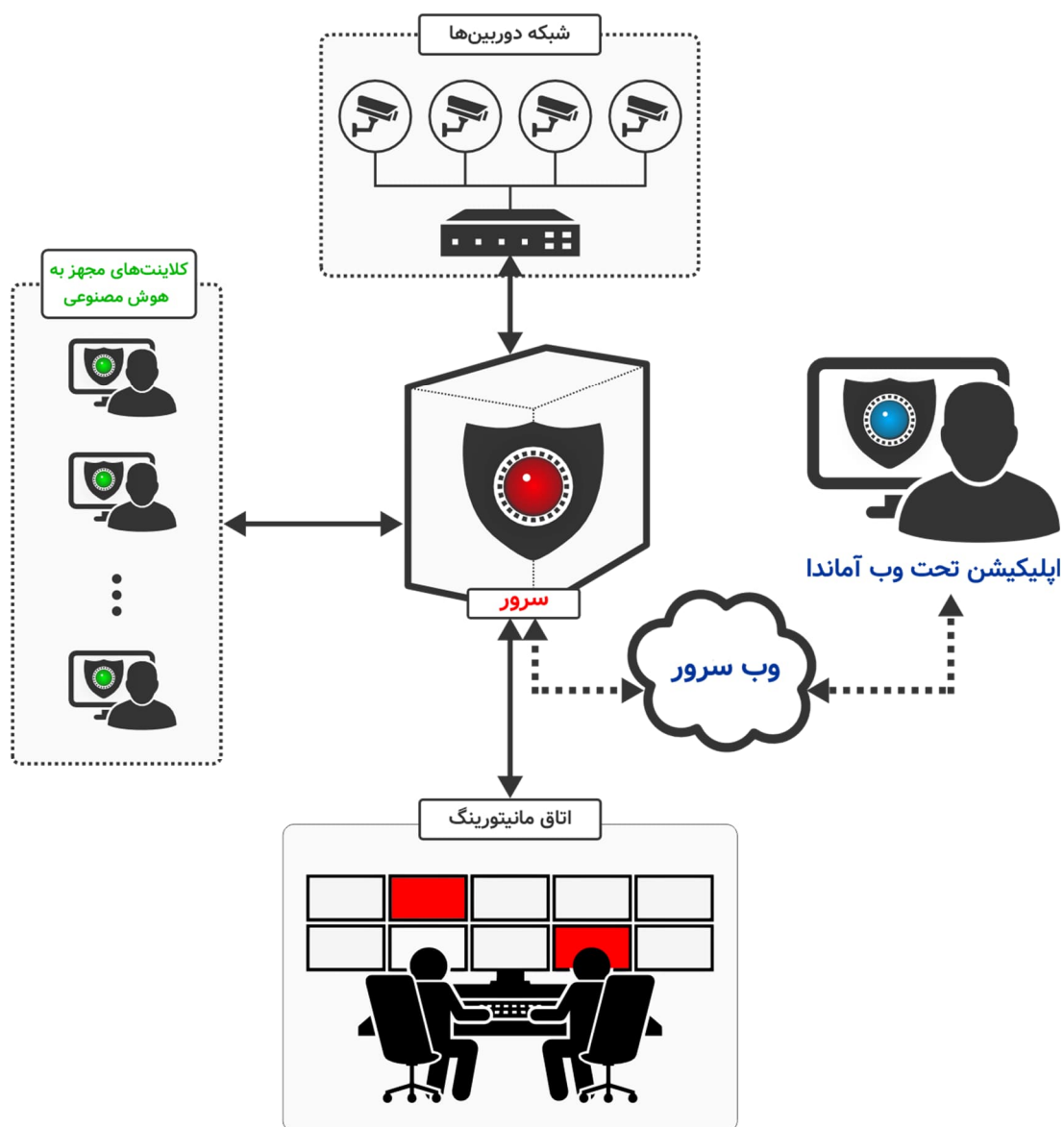
۱) معماری متمرکز: در این معماری تمامی فرآیندها از جمله مدیریت و نظارت تصویری و تشخیص‌های هوشمند به‌طور متمرکز در سرور انجام می‌گیرد.

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 جمع و یکپارچه شده و در اختیار اپراتورهای مستقر در اتاق مانیتورینگ قرار می‌گیرد. در شکل ۱-۱۰ شمای معماری توزیع شده، نشان داده شده است.

۱-۱۳-۱) 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.

- **مقیاس پذیری ساده:** امکان اضافه کردن کلاینت‌های جدید در هر زمان وجود دارد. این کلاینت‌ها توان پردازشی بیشتری برای انجام عملیات هوش مصنوعی فراهم می‌کنند، بدون اینکه نیازی به تغییرات در سرور باشد.
- **افزایش پایداری سیستم:** انتقال بار پردازشی از سرور به کلاینت‌ها خطر از کار افتادن سرور به دلیل بار زیاد پردازشی را کاهش می‌دهد و اطمینان از عملکرد پایدار سیستم را فراهم می‌کند.
- **انعطاف پذیری در طراحی و پیاده سازی:** 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 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.

۱-۱۴) 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 آمادها 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.



پیچینگ و پخش فایل صوتی دلخواه: این اقدام با تعریف فایل‌های صوتی دلخواه برای هر دوربین انجام می‌شود، به‌طوری‌که 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 اتصال سامانه به پل پیامکی و یا با اضافه کردن یک یا چند دستگاه مودم GSM به سامانه انجام می‌شود که پیامک‌های هشدار را به شماره‌های از پیش تعیین‌شده ارسال می‌کند.



ارسال پیام (دستور) به دستگاه‌های آدرس‌پذیر: سامانه آمادها 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 آمادها (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 سامانه‌های مدیریت منابع انسانی ارسال نماید.



¹ Security Information and Event Management



۱-۱۵) آمار و گزارش گیری

بخش «آمار و گزارش گیری» به عنوان یکی از اصلی ترین و کلیدی ترین بخش های سامانه آماندا تلقی می شود و نقش مهمی در تحلیل و مدیریت داده ها ایفا می کند. این بخش با ارائه امکانات متنوع برای گزارش گیری، به کاربران این امکان را می دهد تا اطلاعات مورد نیاز خود را به صورت دقیق و جامع استخراج و تحلیل کنند. طراحی این بخش به گونه ای است که پاسخگوی نیازهای مختلف کاربران بوده و ابزارهای کاربردی متعددی برای تسهیل فرآیند گزارش گیری فراهم کرده است.

۱-۱۶) ایجاد کیوسک های متعدد برای ثبت ورود-خروج

سامانه آماندا قابلیت راه اندازی و مدیریت کیوسک های متعدد برای تشخیص چهره را داراست و اطلاعات تمامی کیوسک ها به صورت متمرکز و یکپارچه در سامانه جمع می شود. این ویژگی امکان ایجاد کیوسک های تشخیص چهره را برای مقاصد مختلف فراهم می کند، از جمله کیوسک های اختصاصی برای فقط ورود، فقط خروج، یا ورود و خروج همزمان، که می توانند بر اساس زمان بندی های دلخواه پیکربندی شوند. این انعطاف پذیری به کاربران اجازه می دهد تا با توجه به نیازهای خاص خود، انواع مختلفی از کیوسک ها را برای کاربردهای گوناگون راه اندازی کرده و اطلاعات ورود-خروج تمامی نقاط را به صورت جامع در اختیار داشته باشند.

۱-۱۷) ویژگی های فنی سامانه

ویژگی های فنی منحصر بفرد سامانه آماندا این امکان را می دهد که در شرایط و نیازهای مختلف عملکردی بسیار قابل قبول و بهینه از خود ارائه دهد و به کاربران اجازه می دهد تا در تمامی محیط ها و با انواع دستگاه ها از آن بهره برداری 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 راه اندازی سریع: سامانه آماندا به گونه ای طراحی شده که نصب و راه اندازی آن به سرعت و به راحتی انجام می شود. فرآیند راه اندازی بدون نیاز به تنظیمات پیچیده، امکان استقرار سریع و کم هزینه را فراهم می آورد.



قابل استفاده در سیستم عامل های ویندوز و لینوکس: سامانه آماندا به طور کامل با سیستم عامل های ویندوز و لینوکس سازگار بوده و امکان اجرای بی دردسر در محیط های نرم افزاری متنوع را فراهم می کند. این سطح از سازگاری و انعطاف پذیری، سامانه آماندا را به گزینه ای ایده آل برای سازمان ها، کسب و کارها، و پروژه های چندپلتفرمی تبدیل کرده و امکان استفاده در محیط های مختلف نرم افزاری و سخت افزاری را بدون محدودیت فراهم می کند.





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.



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



انعطاف‌پذیری بی‌نظیر در اتصال به انواع دوربین‌ها: سامانه آماندا با پشتیبانی از اتصال به انواع دوربین‌ها، بدون توجه به برند، مدل، یا پروتکل ارتباطی، یکی از انعطاف‌پذیرترین راه‌حل‌ها در مدیریت و نظارت تصویری به شمار می‌رود. این سامانه قابلیت یکپارچه‌سازی با دوربین‌های تحت شبکه، دوربین‌های آنالوگ با مبدل‌های مناسب، و حتی دوربین‌های خارج از مدار مانند وب‌کم‌ها یا سایر دستگاه‌های ضبط تصویر را داراست. این ویژگی به کارفرمایان امکان می‌دهد تا بدون محدودیت در انتخاب تجهیزات، از زیرساخت‌ها و دوربین‌های موجود حداکثر بهره‌وری را داشته باشند یا دوربین‌های متناسب با نیازها و بودجه خود را آزادانه انتخاب کنند. علاوه بر این، سازگاری گسترده آماندا با انواع تجهیزات، کاهش هزینه‌های پیاده‌سازی و به‌روزرسانی سیستم‌ها را ممکن ساخته و از هدررفت منابع ناشی از عدم سازگاری جلوگیری می‌کند. این انعطاف‌پذیری، سامانه را برای کاربردهای گوناگون، از نظارت صنعتی و شهری گرفته تا پروژه‌های خانگی و کوچک، به یک راه‌حل جامع و کارآمد تبدیل کرده است.



استفاده از توان پردازشی GPUها: سامانه آماندا از قابلیت پردازش موازی GPUها بهره‌برداری می‌کند تا سرعت پردازش تصاویر و ویدئوها را افزایش دهد. این امکان به ویژه در پردازش‌های سنگین و بلادرنگ برای پردازش تصویر و ویدئوهای با کیفیت بالا نکته حیاتی بشمار می‌رود.

^۱ Raspberry Pi

^۲ Edge Computing

^۳ IoT



توسعه داده شده با زبان C++: سامانه آماندا با استفاده از زبان برنامه‌نویسی C++ توسعه داده شده است که به‌طور طبیعی به‌خاطر ویژگی‌های خود مانند پردازش سریع، بهره‌وری بالا از منابع، و دسترسی مستقیم به سخت‌افزار، عملکرد عالی را فراهم می‌کند. این انتخاب موجب شده تا سامانه بتواند در پردازش‌های پیچیده و زمان‌بری که به منابع بالایی نیاز دارند، با استفاده بهینه از قدرت پردازشی سیستم، به‌طور چشمگیری مصرف منابع سخت‌افزاری را کاهش دهد. این ویژگی به‌طور خاص در محیط‌هایی که تعداد زیادی دوربین باید همزمان تحت پوشش قرار بگیرند، مزیت بزرگ و کلیدی به شمار می‌آید. در نتیجه، این سامانه نه تنها کارایی بالایی را ارائه می‌دهد بلکه برای کاربران به‌صرفه‌تر و کارآمدتر خواهد بود.

۱-۱۸ ویژگی‌های کاربردی سامانه

سیستم‌های نظارتی هوشمند امروزی نقش کلیدی را در حفظ امنیت و مدیریت بهینه ایفا می‌کنند. این سیستم‌ها نه تنها قادر به شناسایی دقیق و لحظه‌ای تهدیدات مختلف هستند، بلکه به کمک الگوریتم‌های پیشرفته، می‌توانند داده‌ها را تحلیل کرده و تصمیمات صحیح را در زمان مناسب اتخاذ کنند. با توجه به پیچیدگی و تنوع نیازهای نظارتی، این سیستم‌ها باید انعطاف‌پذیر و قابل تنظیم بوده تا قادر به پاسخ‌گویی به شرایط مختلف و متنوع باشند. در این راستا، قابلیت‌های کاربردی متعددی برای افزایش کارایی و بهبود عملکرد سامانه آماندا 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 به‌صورت مجزا: تنظیم زمان شروع و پایان فعالیت‌های

نظارتی برای هر دوربین به‌صورت 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 گزارش گیری و جستجو در ویدیوهای ضبط شده:** امکان مشاهده و تحلیل داده‌های جمع‌آوری شده و

جستجوی آسان در میان ویدیوهای ضبط شده 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 شناسایی شده در حریم:** تنظیم حساسیت سیستم در شناسایی اجسام مختلف،

به گونه‌ای که برای هر نوع شیء شناسایی شده، 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 به کارگیری 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 به طور همزمان با هدف کنترل نامحسوس:** قابلیت تشخیص و شناسایی همزمان هویت

چندین فرد در محیط، به منظور کنترل و نظارت نامحسوس و بهبود امنیت.

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

و ارسال هشدارهای فوری در این باره.

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

و شناسایی شباهت‌های احتمالی به منظور 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 راهنبد یا درب‌ها برای دسترسی محدود و امن: کنترل دقیق و اتوماتیک درب‌ها یا راهنبد‌ها 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 به‌صورت 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 به‌صورت اختصاصی.

بخش دوم

راهنمای استفاده

نسخه سرور



۲) مقدمه

در این بخش، مراحل اصلی تنظیمات **نسخه‌ی سرور**^۱ 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 به‌صورت کامل انجام دهند.

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

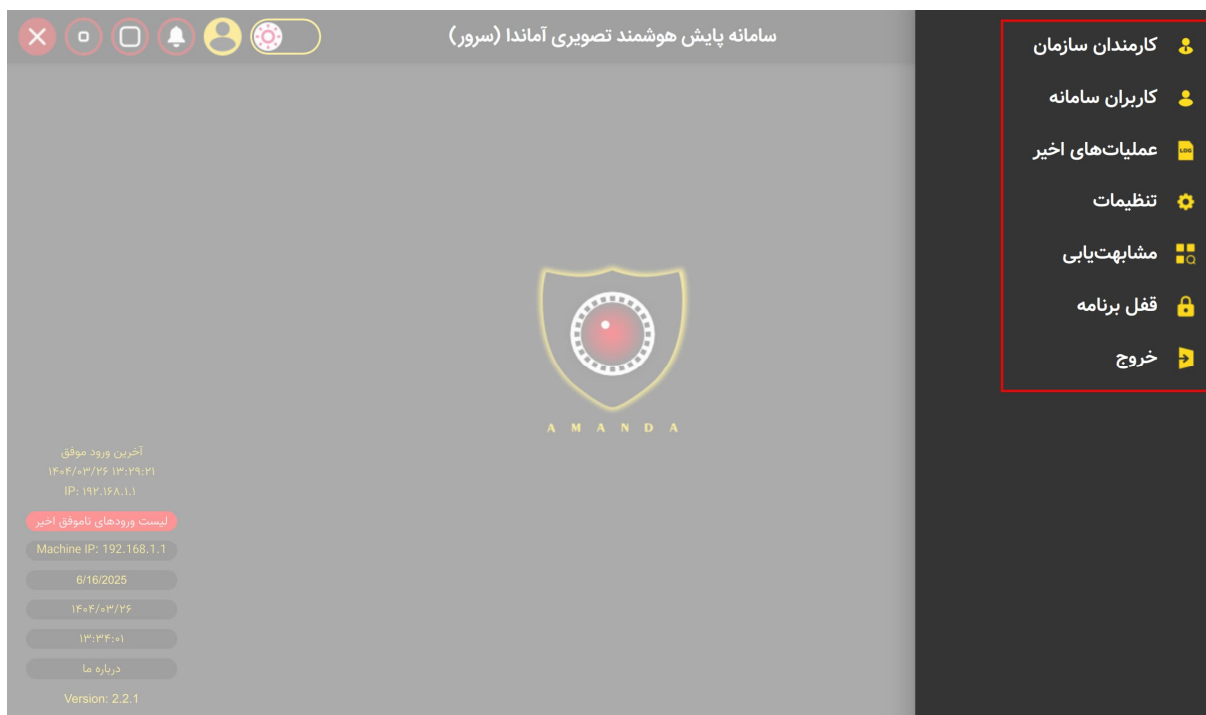


نام کاربری پیش‌فرض **admin** و کلمه عبور پیش‌فرض **Admin-123** است.



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 به‌صورت گام‌به‌گام برای تضمین عملکرد بهینه سامانه باید اجرا شوند. توجه داشته باشید که در متن راهنمای پیش‌رو، به‌صورت مکرر به **منوی اصلی** و آیتم‌های مختلف آن اشاره شده است. در شکل ۱-۲، نمایی از این منو نشان داده شده است.

¹ Amanda-Server



شکل ۲-۱: نمایی از منوی اصلی سامانه آماندا

۲-۱) راه اندازی سرویس ها

سامانه آماندا 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 به صورت 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.



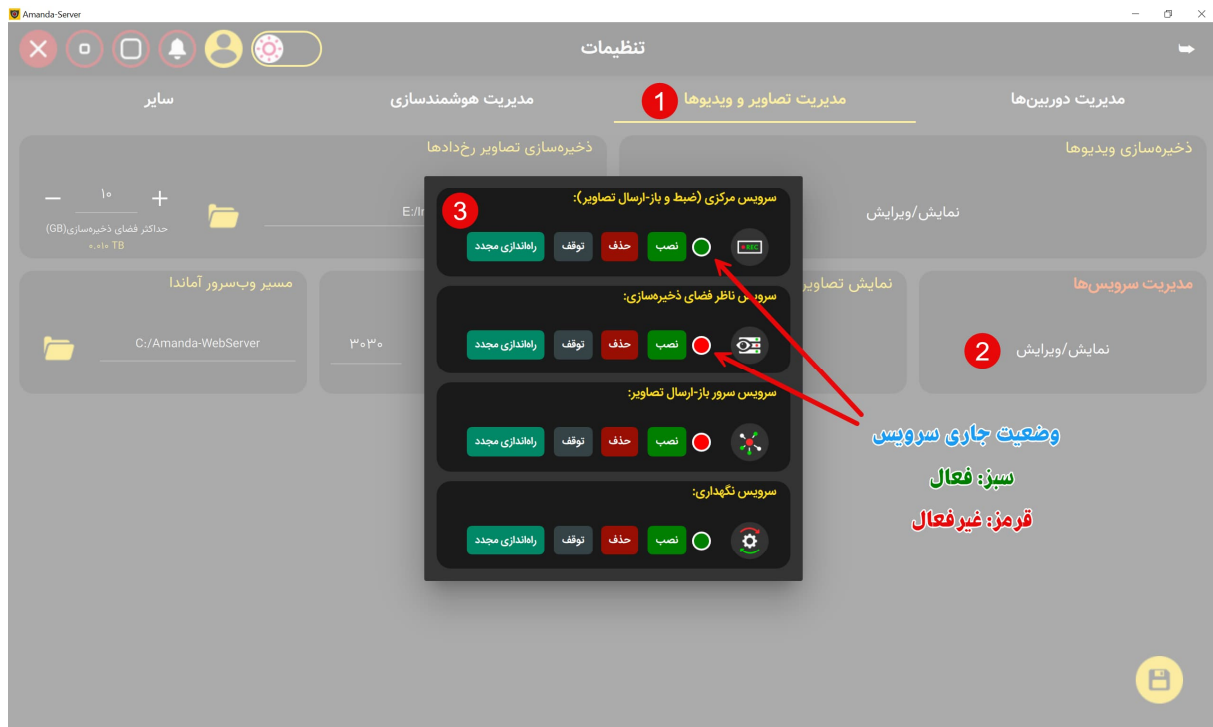
سرویس سرور باز-ارسال تصاویر: این سرویس نقش سرور باز-ارسال تصاویر دریافتی از دوربین ها را ایفا می کند. با اجرای این سرویس، تصاویر دریافتی از دوربین ها به صورت بلادرنگ در اختیار ناظران قرار می گیرد.



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 نمایی از این منو را نشان می دهد.



شکل ۲-۲: نمایشی از منوی سرویس‌ها

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 به‌صورت 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 آمادنا، ساختار سلسله مراتبی برای این منظور در نظر گرفته شده است:

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

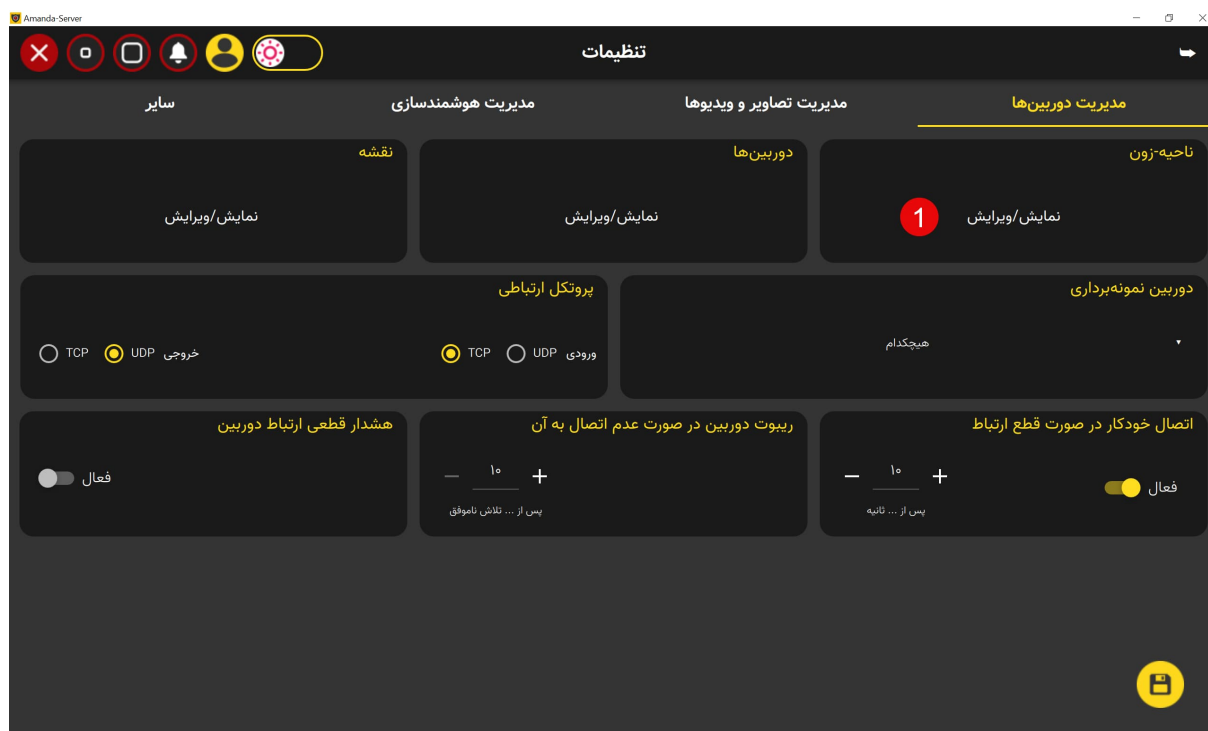
۲) **واحد:** زیرمجموعه‌ای از یک زون، مانند طبقه یا بخش خاصی از ساختمان

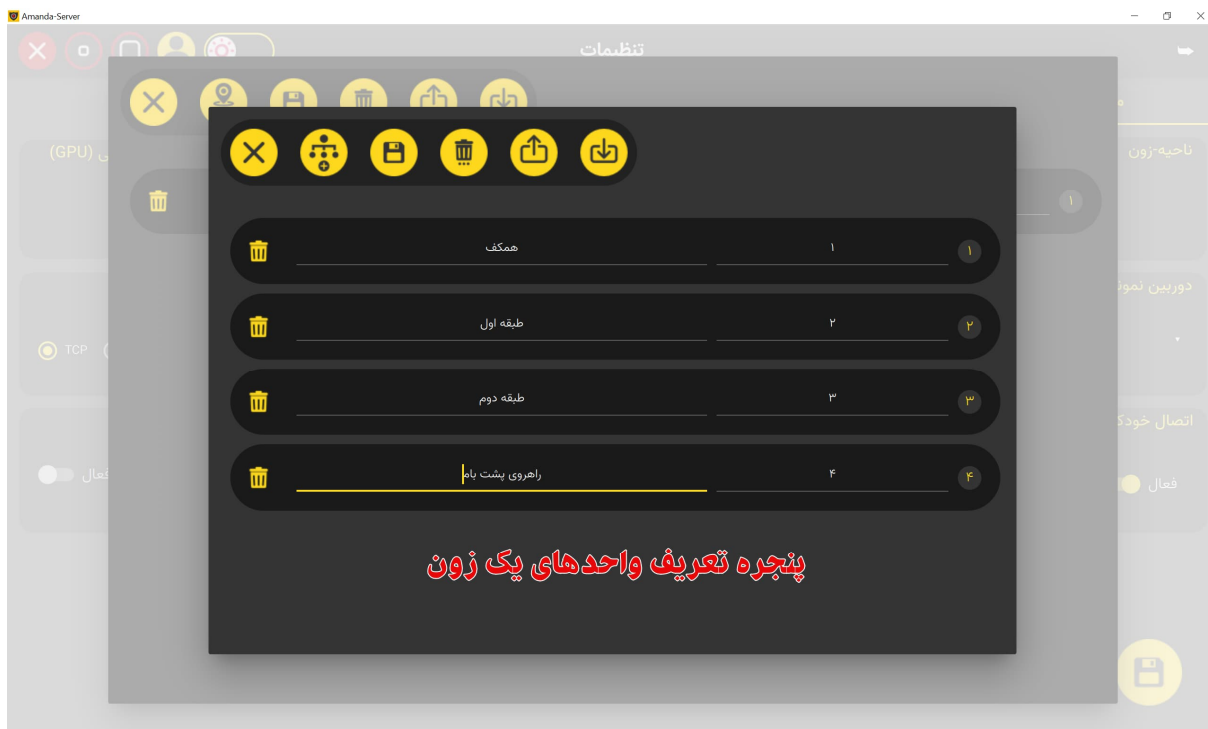
هر دوربین باید به‌طور دقیق در یک زون-واحد مشخص طبقه‌بندی شود. پیش از تعریف و مدیریت دوربین‌ها، ضروری است که زون‌ها و واحدهای مرتبط به‌طور کامل معرفی شوند. این کار امکان اختصاص دقیق دوربین‌ها به نواحی مشخص را فراهم می‌کند. به‌عنوان مثال، در مجموعه‌ای

^۱ Zone

^۲ Unit

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.

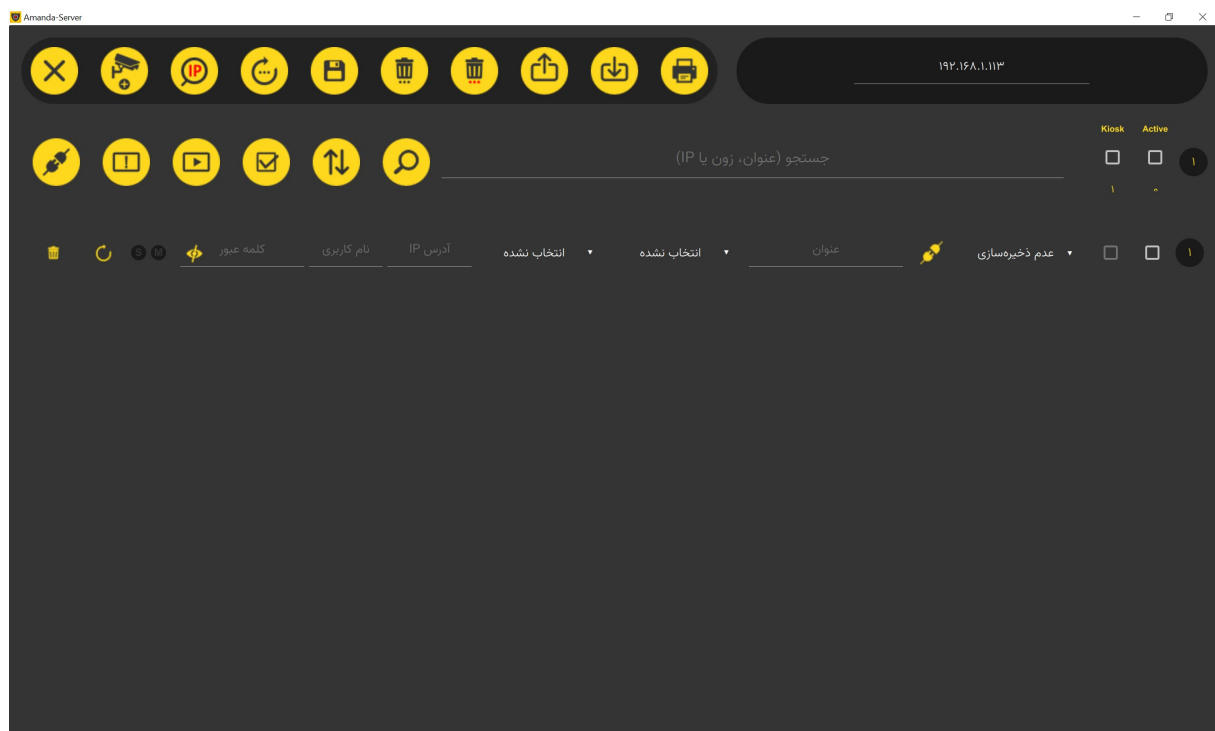
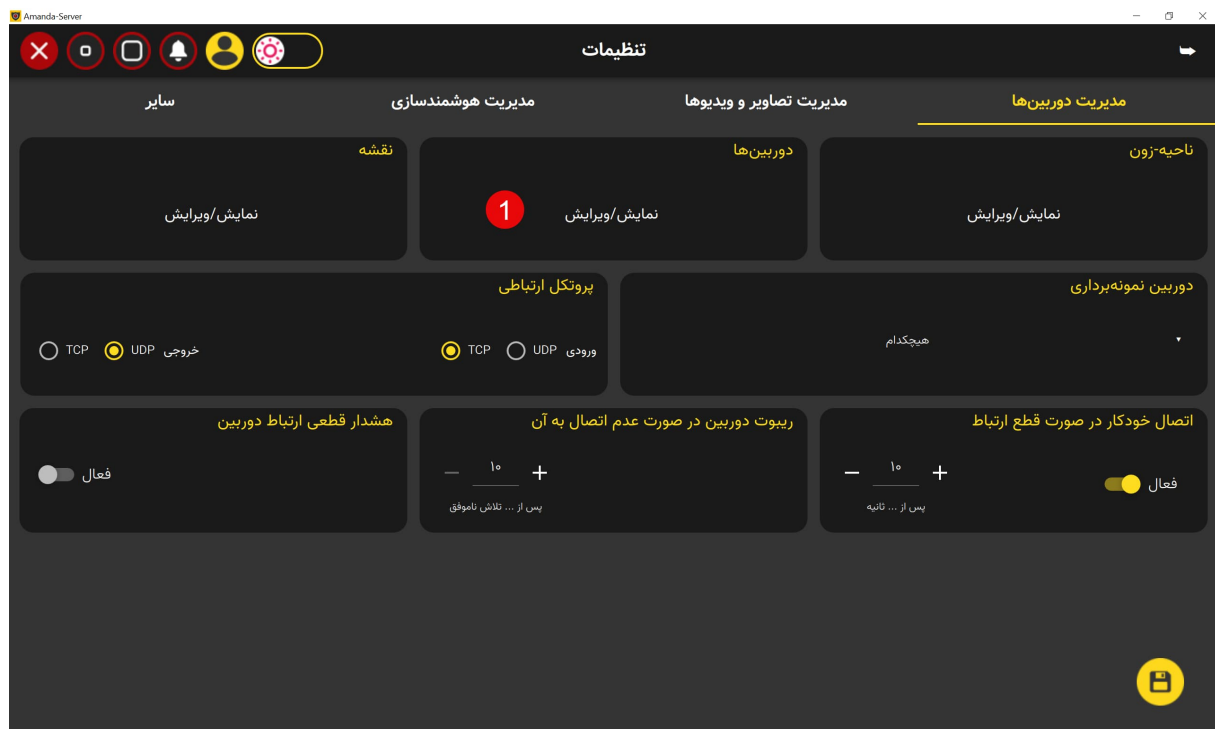




شکل ۲-۳: مراحل تعریف زون-واحد

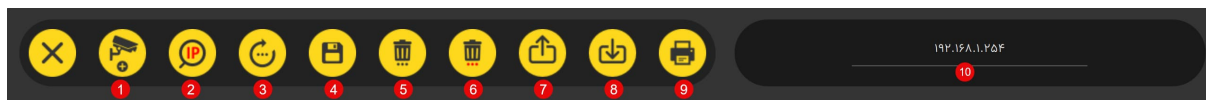
۲-۳) تعریف و اتصال به دوربین‌ها

برای تعریف اطلاعات دوربین‌ها و اتصال به آنها، از منوی اصلی به تنظیمات رفته و به ترتیب مراحل نشان داده شده در شکل ۲-۴ 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 این کار، تسریع در فرآیند افزودن دوربین‌هایی با اطلاعات یکسان است.

(۲) دکمه جستجوی دوربین‌ها به صورت 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 اطلاعاتش همچنان نگه دارید، می‌توانید تیک چک‌باکس آن را 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.

۱-۳-۲ پنل دوربین

پس از بروزرسانی دوربین، با نگه داشتن کلید Ctrl و فشردن دکمه بروزرسانی دوربین (آیتم شماره ۱۲ در شکل ۲-۶)، منوی **تنظیمات پیشرفته**

دوربین ظاهر می‌شود. شکل ۲-۷ نمایی از این منو را نشان می‌دهد.

^۱ Snapshot

^۲ Codec (H264 or H265)

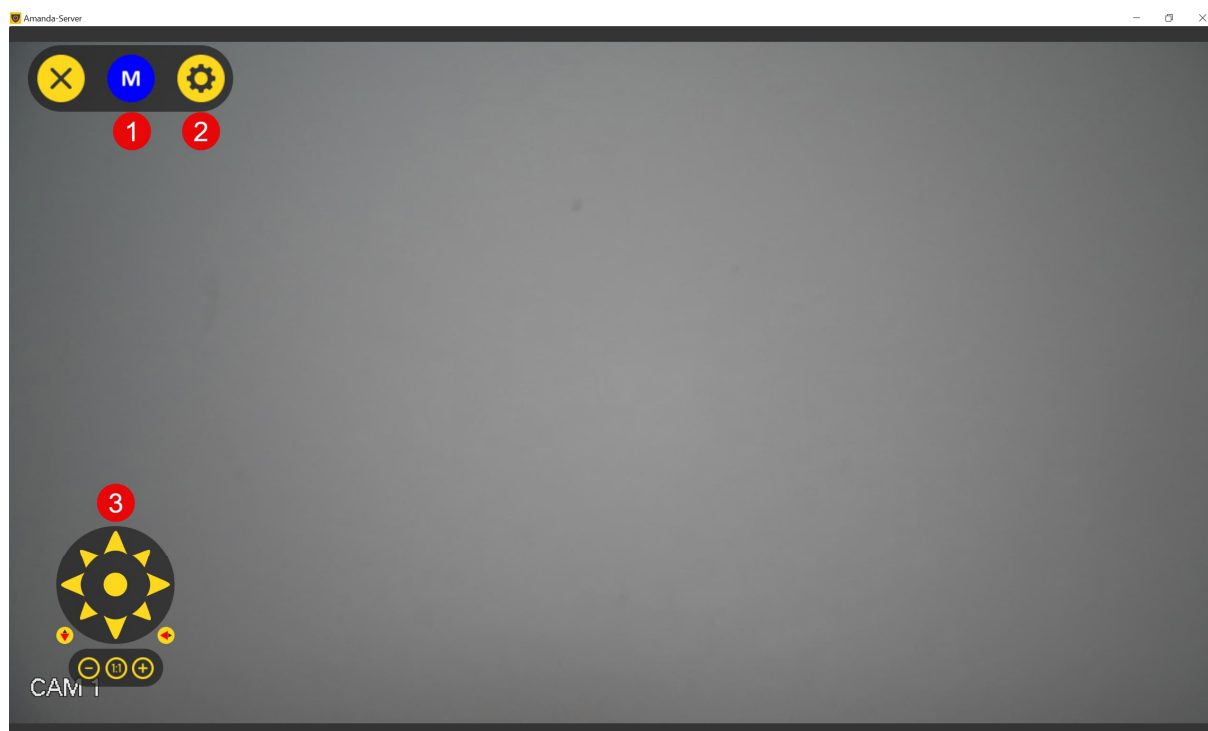
^۳ Main-Stream

^۴ Sub-Stream



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 می‌دهد.



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، تصویر، شبکه و تنظیمات سیستمی پرکاربرد 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 S^1 و T^2 استاندارد ONVIF^۳ به صورت همزمان پشتیبانی می‌کند.

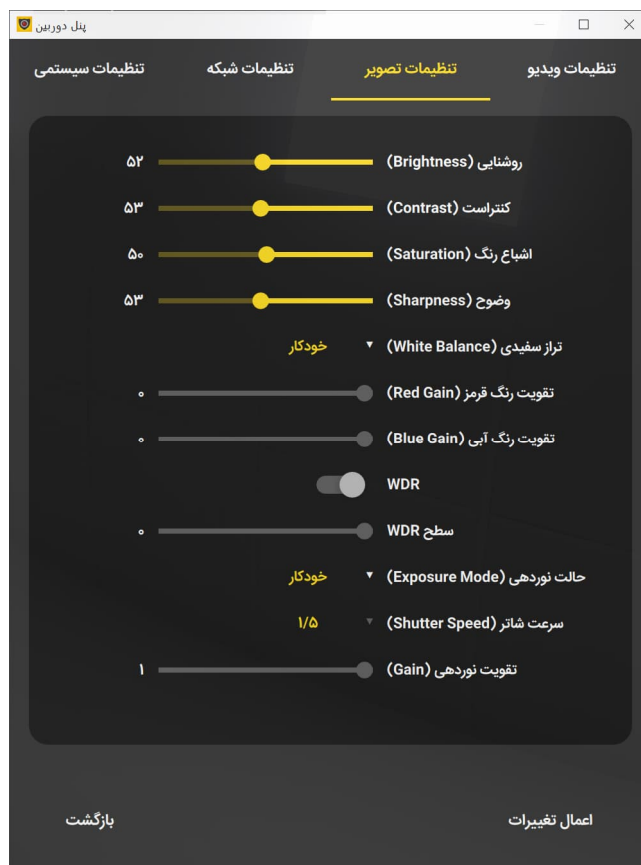


(الف)

¹ ONVIF Profile S

² ONVIF Profile T

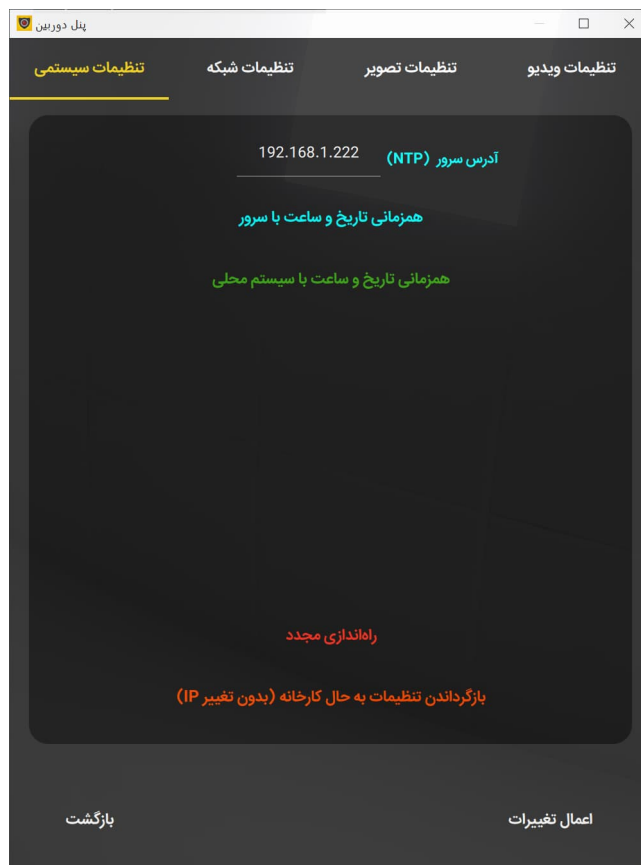
³ Open Network Video Interface Forum



(ب)



(پ)



(ت)

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

۲-۳-۲) 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:

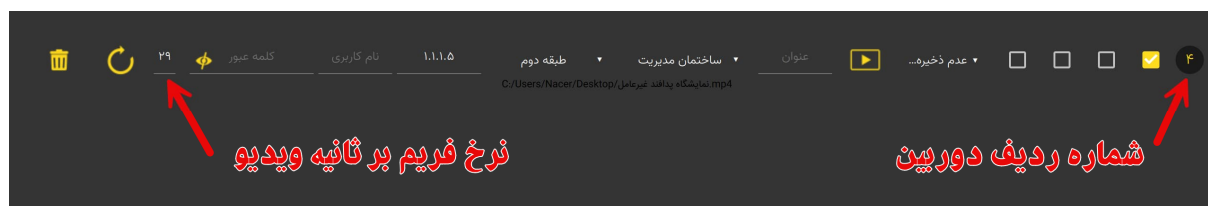
۱) ابتدا یک دوربین خالی ایجاد کنید.

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

۳) از منوی باز شده، فایل ویدیویی مورد نظر را انتخاب کنید.

توجه داشته باشید که IP فایل ویدیویی باید در قالب *۱.۱.۱ باشد؛ به جای 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 به جای دوربین بارگذاری خواهد شد. بعد از بارگذاری

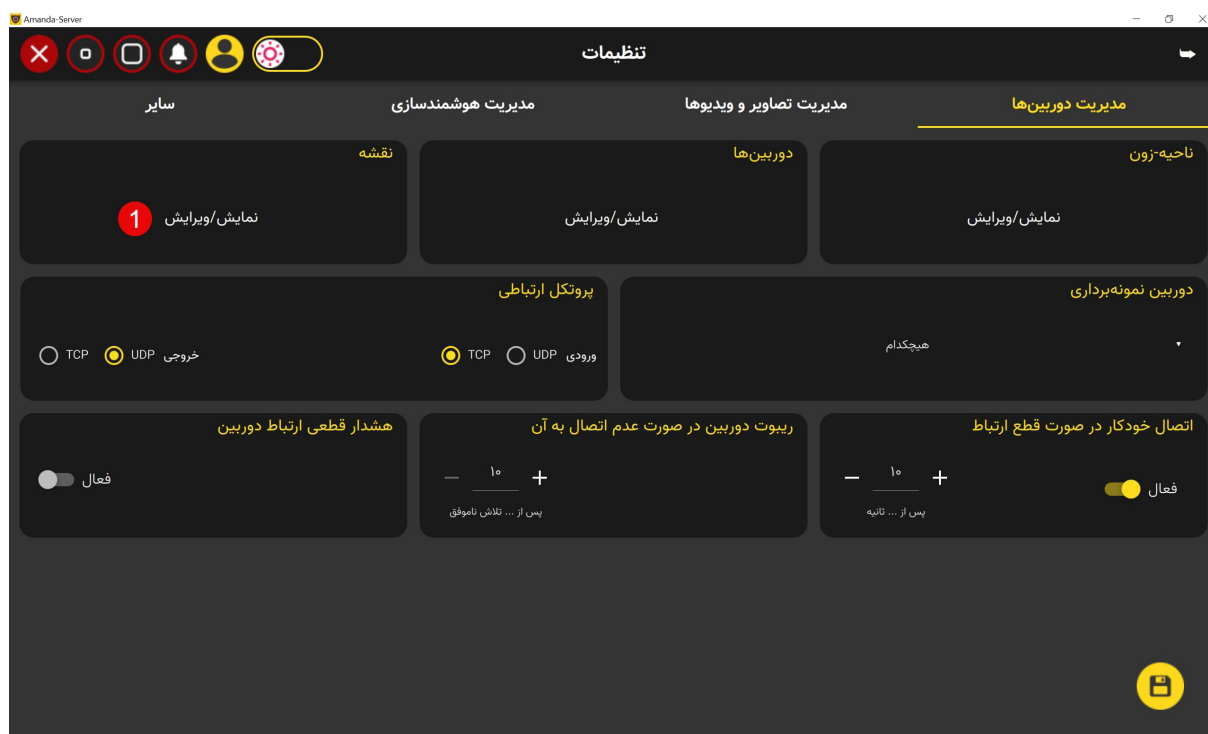
فایل، نرخ فریم بر ثانیه (FPS) ویدیو نمایش داده می‌شود که می‌توانید این مقدار را تغییر داده تا سرعت پخش ویدیو را مطابق نیازتان تنظیم کنید. شکل ۲-۱۰ نمونه‌ای از فرآیند تعریف دوربین مجازی را نشان می‌دهد.

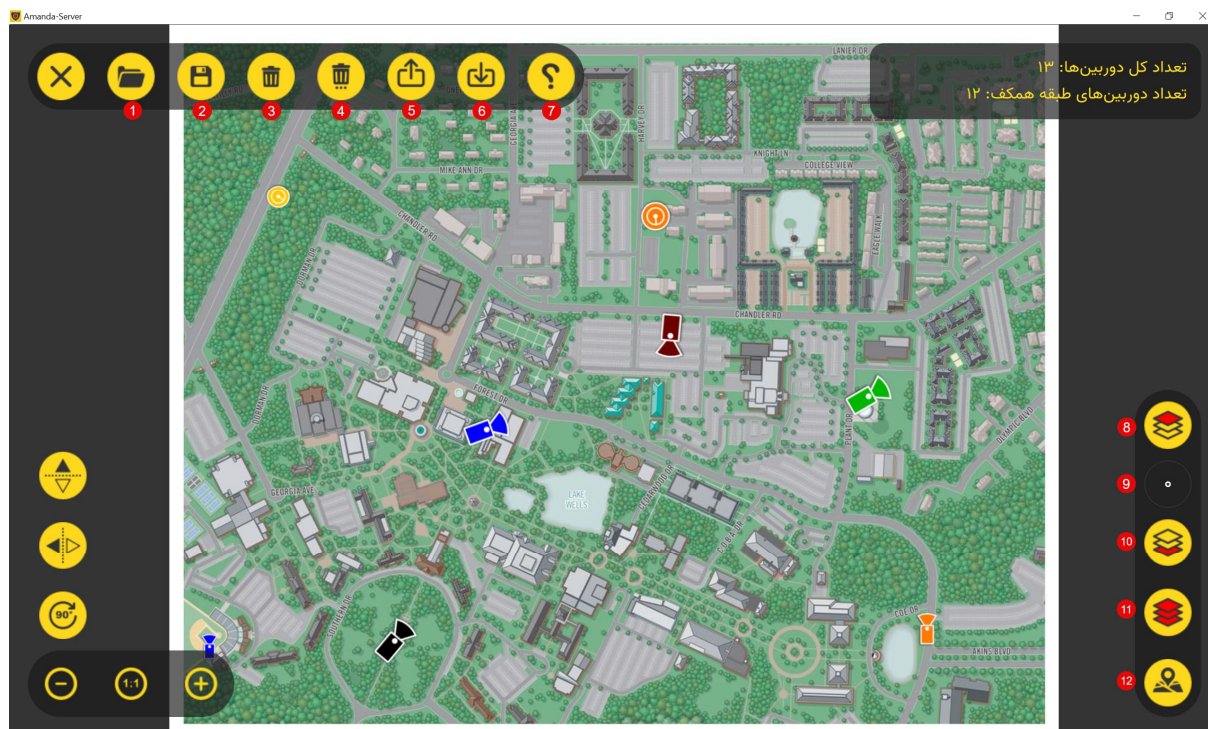


شکل ۲-۱۰: تعریف و ایجاد دوربین مجازی با استفاده از فایل ویدیویی

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.





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 ۲-۱۲، 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 ماوس 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.

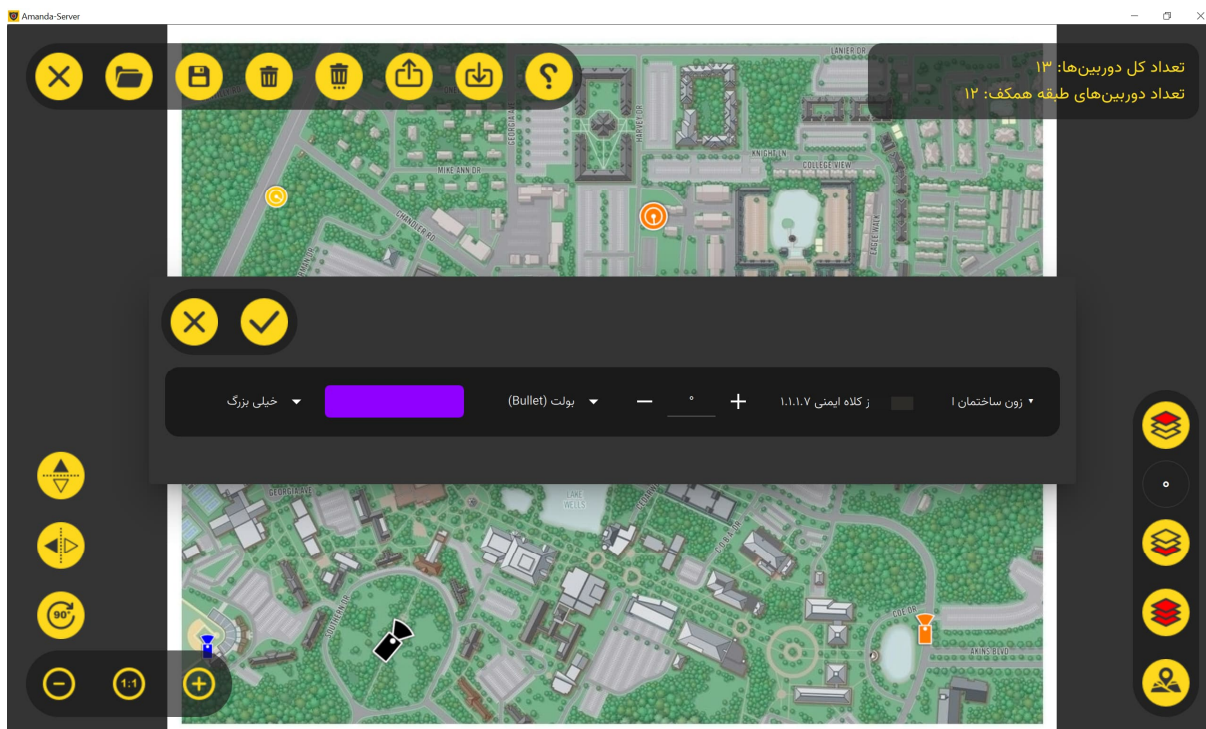
۱۲) دکمه برجسته کردن دوربین‌های قرار گرفته در طبقه جاری: در مواقعی که پیدا کردن محل قرارگیری دوربین‌ها به دلیل شلوغی نقشه کار سختی باشد، با زدن این دکمه می‌توانید به راحتی دوربین‌های روی نقشه را شناسایی کنید.

- 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).

^۱ Double-Click



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

۲-۵) تنظیمات مربوط به مدیریت ویدیوها و تصاویر

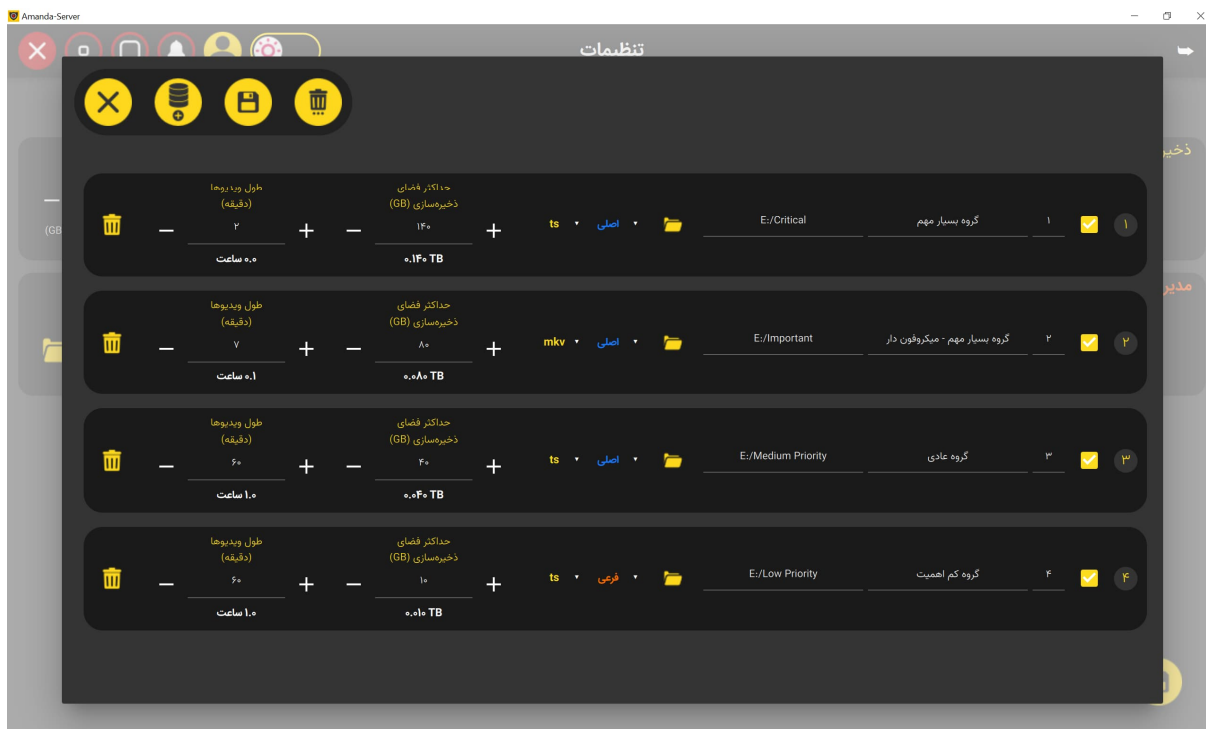
برای انجام تنظیمات مربوط به ذخیره‌سازی ویدیوهای دریافتی از دوربین‌ها، ذخیره‌سازی تصاویر ایجاد شده در فرآیند اعمال هوش مصنوعی و سایر تنظیمات مرتبط، از **منوی اصلی** به بخش **تنظیمات** رفته و برگه^۱ **مدیریت تصاویر و ویدیوها** را انتخاب کنید. در شکل ۲-۱۴، بخش‌های مختلف این برگه نشان داده شده است.

^۱ Tab



شکل ۲-۱۴: 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 ۲-۱۵ 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.



شکل ۲-۱۵: نمایش از منوی تعریف گروه‌های ذخیره‌سازی

در صورتی که دوربین مورد استفاده شما دارای میکروفون داخلی است و تمایل دارید صدای محیط نیز به همراه تصویر ضبط شود، لطفاً در تنظیمات ضبط، فرمت ویدیویی MKV را انتخاب نمایید. تنها این فرمت امکان ذخیره‌سازی همزمان تصویر و صدا را در سامانه فراهم می‌سازد. فرمت TS تنها تصویر را ذخیره می‌کند.



۲-۶) برپایی فنس مجازی و فعال‌سازی 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 ۲-۱۶ را دنبال کنید.



شکل ۲-۱۶: 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 ۲-۱۷، نمونه‌ای از این منو را نشان می‌دهد.

همانطور که گفته شد، دکمه شماره ۲ در شکل ۲-۱۶، 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 ۲-۱۷، ارائه می‌شود.



(الف)

^۱ Snapshot



(ب)

شکل ۲-۱۷: پنجره تنظیمات هوش مصنوعی دوربین

در ابتدای ورود به منوی تنظیمات هوش مصنوعی دوربین، تعداد و حالت دکمه‌های نوار ابزار به شکل ۲-۱۷ (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 ۲-۱۷ 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 ۲-۱۸)

۴) دکمه نمایش منوی تنظیمات مربوط به هوش مصنوعی (شکل ۲-۱۹): 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 ۲-۲۰): 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^۱ کردن حریم: با فعال کردن این آیتم، محدوده فنس در زمان اجرا به منظور حفظ حریم خصوصی افراد به صورت تار

نمایش داده می شود.

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، می توانید فنس را حول حریم مورد نظر ایجاد کرده و سپس آن را برعکس نمایید. نمونه ای از فنس برعکس شده در شکل ۲-۲۱ 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 می گیرد.

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

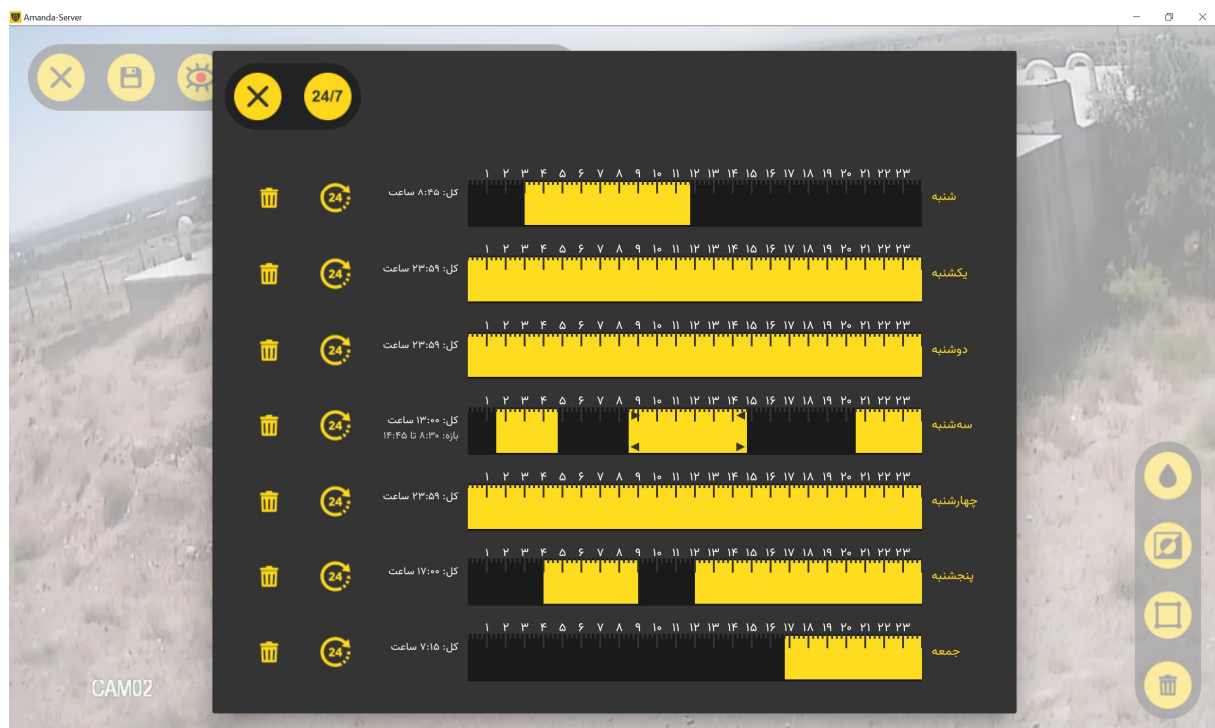


شکل ۲-۱۸: نمایشی از منوی راهنمای ایجاد فنس مجازی

¹ Blur



شکل ۲-۱۹: نمایی از منوی تنظیمات هوش مصنوعی



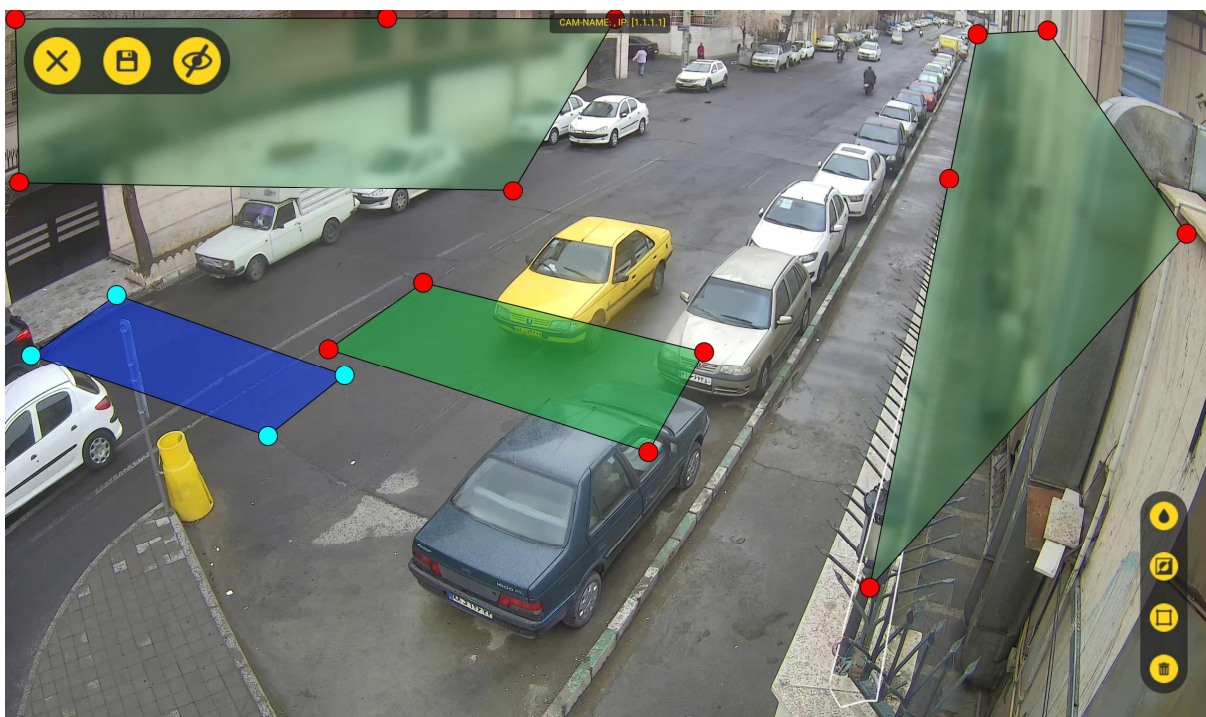
شکل ۲-۲۰: منوی تنظیمات زمانبندی فعال یا غیرفعال بودن نظارت هوشمند: با کلیک و کشیدن^۱ ماوس رو نوار ساعت هر روز، می‌توانید یک یا چند بازه زمانی ایجاد کنید. فلش‌های سیاه کوچک در انتهای بازه‌های زمانی، امکان تنظیم جزئی‌تر با دقت ۱۵ دقیقه را فراهم می‌کنند.

^۱ Drag



شکل ۲-۲۱: نمونه‌ای از فنس مجازی برعکس

کاربر می‌تواند در محدوده‌های مورد نظر خود چندین فنس مجازی ایجاد کند و در صورت نیاز، هر یک را تار^۱ نماید. برای تار کردن، حذف یا ویرایش هر فنس، کافی است روی آن کلیک کنید تا فعال شود (با تغییر رنگ به آبی).



شکل ۲-۲۲: نمونه‌ای از چهار عدد فنس مجازی که دو عدد از آنها تار و یکی دیگر انتخاب شده است (به رنگ آبی).

^۱ Blur



در شکل ۲-۲۲، نمونه‌ای از ایجاد چندین فنس مجازی و تار کردن برخی از آنها نمایش داده شده است.

برای تنظیم میزان تار ناحیه‌ی مورد نظر، چرخ ماوس را به سمت جلو یا عقب بچرخانید.



۲-۷) راهنمای ثبت‌نام اشخاص شناسی (کارمندان-پرسنل)

در سامانه آمادها سه روش برای ثبت‌نام اشخاص پیش‌بینی شده است: ۱) ثبت‌نام گروهی اشخاص با استفاده از فایل اکسل، ۲) ثبت‌نام مجزای اشخاص و ۳) ثبت‌نام در زمان اجرا و به‌صورت برخط^۱. در ادامه، راهنمای به‌کارگیری ثبت‌نام گروهی و ثبت‌نام مجزا توضیح داده می‌شود و راهنمای ثبت‌نام برخط، در بخش ۳-۵ ارائه شده است.

۲-۷-۱) راهنمای ثبت‌نام گروهی اشخاص با استفاده از فایل اکسل

در این روش می‌توانید با استفاده از اطلاعات تجمیعی کارمندان-پرسنل که در فایل اکسلی با فرمت CVS^۲ ذخیره شده‌اند، به‌صورت یکپارچه اقدام به ثبت‌نام کارمندان کنید. به همین منظور از **منوی اصلی** به بخش **کارمندان سازمان** رفته و مراحل نشان داده شده در شکل ۲-۲۳ را دنبال کنید.

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^۳ اطلاعاتی که ممکن است قبلاً گردآوری کرده باشید، می‌توانید ترتیب ستون‌ها را در فایل الگو براساس نیاز تغییر دهید.

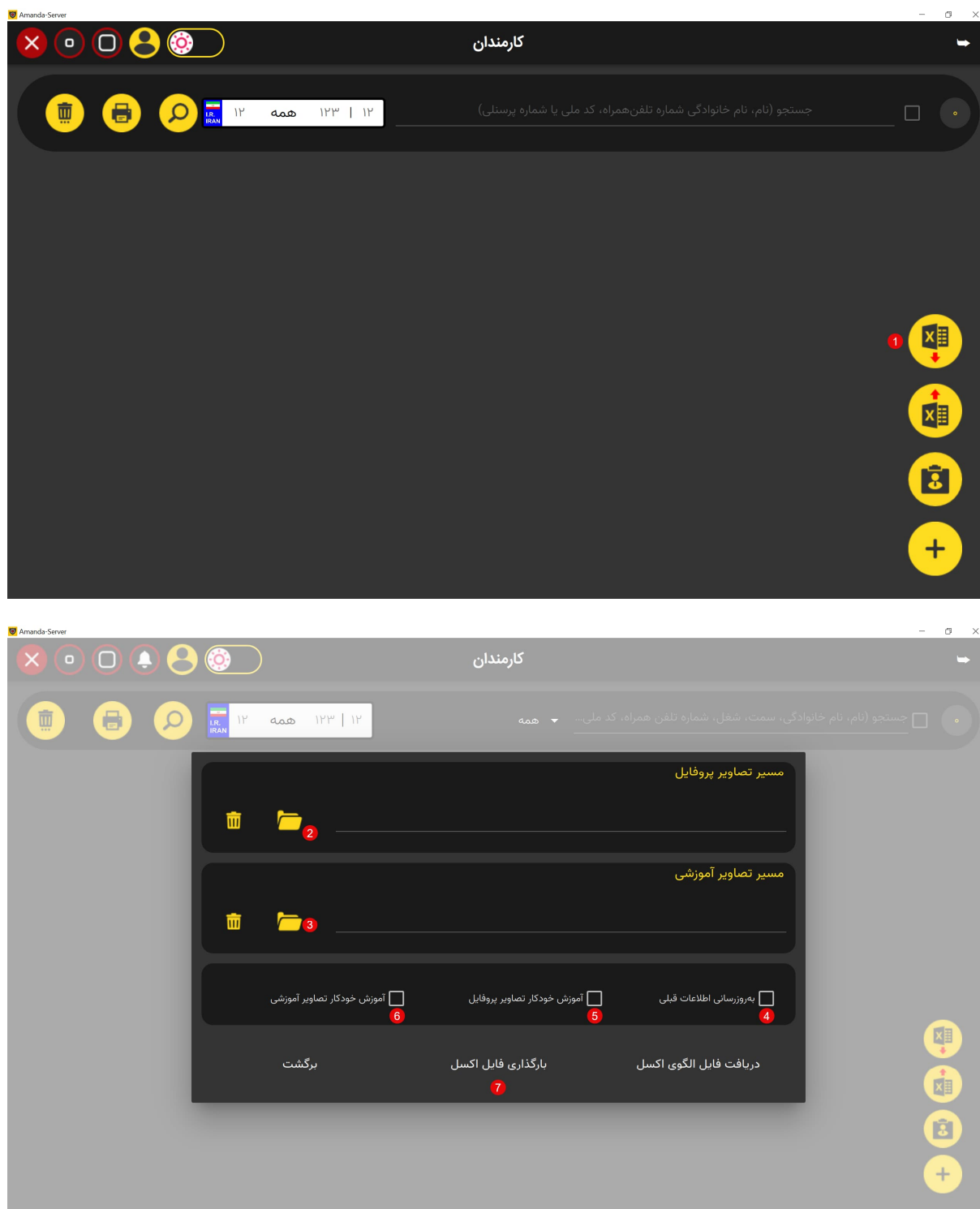
از بین ستون‌های موجود در فایل الگو، تنها سه ستون: نام (فارسی)، نام خانوادگی (فارسی) و کد ملی جز ستون‌های ضروری هستند. بنابراین، وارد کردن یا نکردن بقیه ستون‌ها خللی در فرآیند ثبت اطلاعات ایجاد نمی‌کند.



^۱ Online

^۲ Comma Separated Value

^۳ Copy-Paste



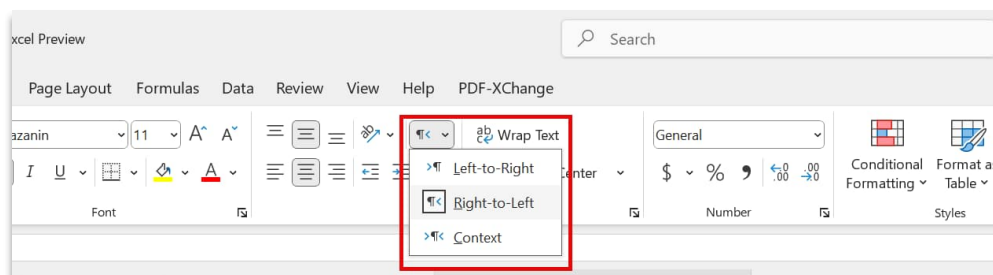
شکل ۲-۲۳: مراحل ثبت نام گروهی کارمندان-پرسنل (اشخاص شناس)

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:



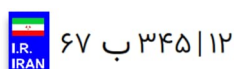
(۱) ستون پلاک‌ها را انتخاب کنید.

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

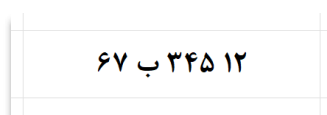


(۳) صفحه کلید را فارسی کنید.

(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 به صورت شکل زیر باشد:

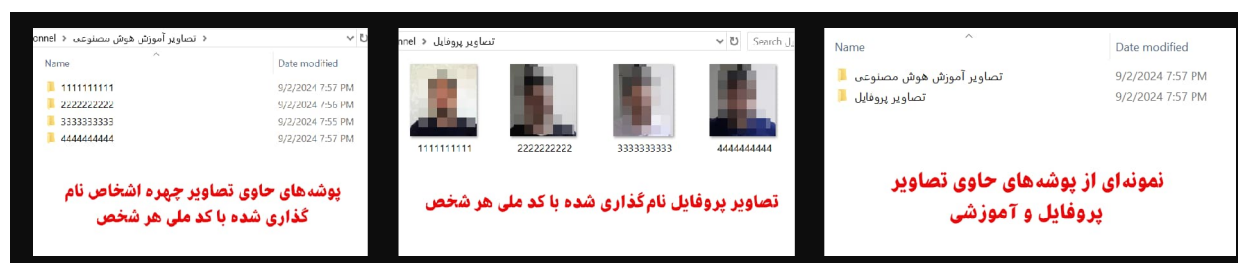


بارگذاری تصویر پروفایل و تصاویر آموزشی: اگر تصاویر پروفایل و تصاویر آموزشی کارمندان را از قبل جمع‌آوری کرده‌اید، می‌توانید هنگام ورود اطلاعات کارمندان، این تصاویر را نیز در سامانه ثبت کنید. به همین منظور، مسیر تصاویر پروفایل و همچنین مسیر تصاویر آموزشی کارمندان را به ترتیب با استفاده از آیتم‌های شماره ۲ و ۳ نشان داده شده در شکل ۲-۲۳، به سامانه اعلام کنید.

^۱ Space

^۲ Enter

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 ۲-۲۴ نمونه‌ای از این نام‌گذاری‌ها را نشان می‌دهد.



شکل ۲-۲۴: نمونه‌ای از نام‌گذاری تصاویر پروفایل و پوشه‌ی 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 به صورت 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 خطایی 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.



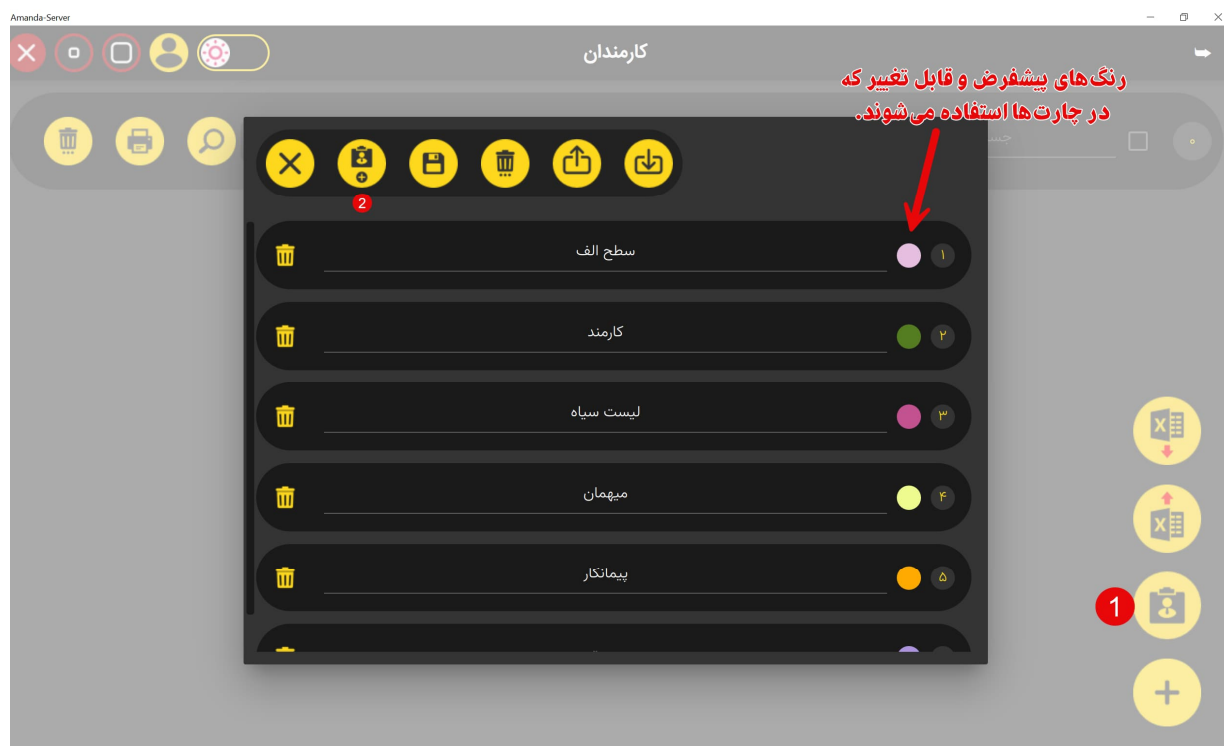
توجه داشته باشید که پس از وارد کردن اطلاعات به صورت تجمیعی از فایل اکسل و تصاویر آموزشی برای هر فرد، لازم است فرآیند آموزش تصاویر به صورت دستی انجام شود. این کار به شما امکان می‌دهد تا از صحت تصاویر آموزشی اختصاص یافته به هر شخص اطمینان حاصل کرده و تصاویر مناسب را از میان تصاویر موجود برای فرآیند آموزش انتخاب کنید. این اقدام تأثیر مستقیمی بر دقت و عملکرد سامانه خواهد داشت (رجوع شود به بخش ۲-۷-۲).



¹ Atomic

۲-۷-۲) ثبت نام مجزای اشخاص

برای ثبت نام افراد به صورت مجزا، پیشنهاد می شود ابتدا عناوین گروه های 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 می کند. شکل ۲-۲۵ فرآیند اضافه و یا ویرایش گروه های کارمندی را نشان می دهد.



شکل ۲-۲۵: مراحل افزودن گروه های کارمندی

تعریف انواع گروه ها و یا سمت های شغلی و اختصاص آن به اشخاص، انعطاف پذیری بیشتری به شما در زمان گزارش گیری و یا تعریف قوانین امنیتی خواهد داد.



پس از تعریف گروه های کارمندی، مراحل نشان داده شده در شکل ۲-۲۶ را جهت ثبت نام شخص مورد نظر دنبال کنید.

کارمندان

ورود اطلاعات نام (فارسی)، نام خانوادگی (فارسی) و کد ملی ضروری است.

نام (انگلیسی) فرج زاده نام (انگلیسی) سطح الف

شماره پرسنلی شماره تلفن همراه ۱۳۳۴۵۶۷۸۹۰ تاریخ تولد شغل

فعال محدودیت ورود و خروج

تا تاریخ از تاریخ روز

جمعه پنجشنبه چهارشنبه سه شنبه دوشنبه یکشنبه شنبه کل هفته

شکل ۲-۲۶: مراحل ثبت نام یک شخص

پس درج اطلاعات شخص مورد نظر، آن را ذخیره کرده و از منو خارج شوید. سپس آیتم شماره ۱ نشان داده شده در شکل ۲-۲۷ را انتخاب کنید تا منوی ویرایش اطلاعات شخص نمایش داده شود (شکل ۲-۲۸).

کارمندان

جستجو (نام، نام خانوادگی، شماره تلفن همراه، کد ملی یا شماره پرسنلی)

۱۲ همه ۱۲۳ | ۱۲

حذف ویرایش افزود

۱۳۳۴۵۶۷۸۹۰ ناصر فرج زاده

نمایش لیست ورود-خروج های ثبت شده توسط دستگاه های کیوسکی (خود اظهاری)

نمایش لیست تشخیص های نامحسوس (خودکار)

شکل ۲-۲۷: نمایش از لیست اشخاص (کارمندان) تعریف شده

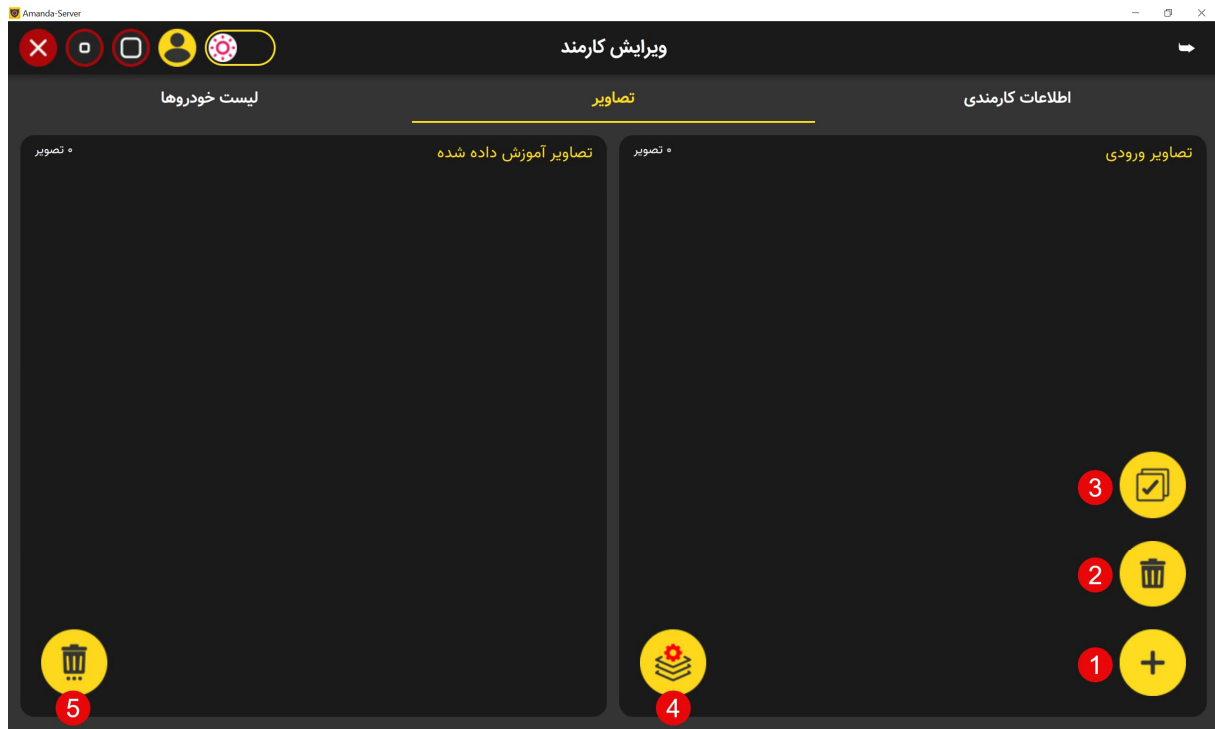
پس از ورود به منوی ویرایش اطلاعات کارمند، سه برگه با عناوین زیر در دسترس خواهد بود:

(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 ۲-۲۸: 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، به عنوان 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 به عنوان 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.

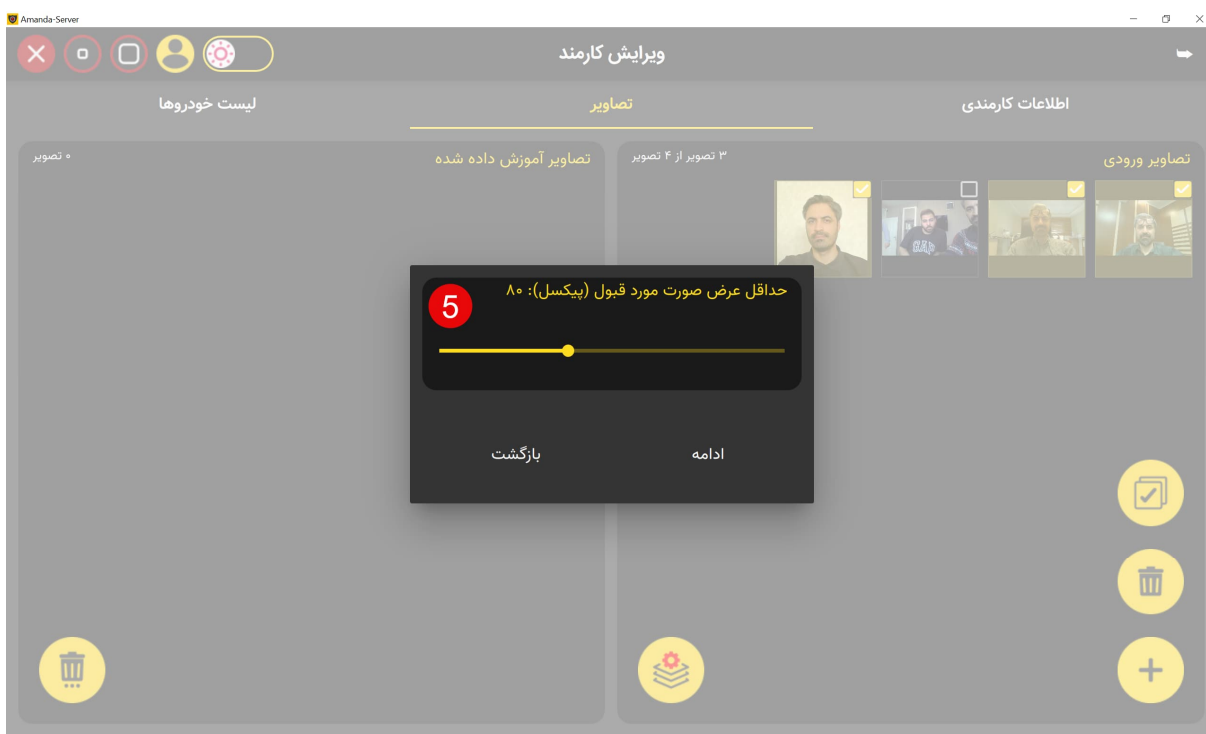
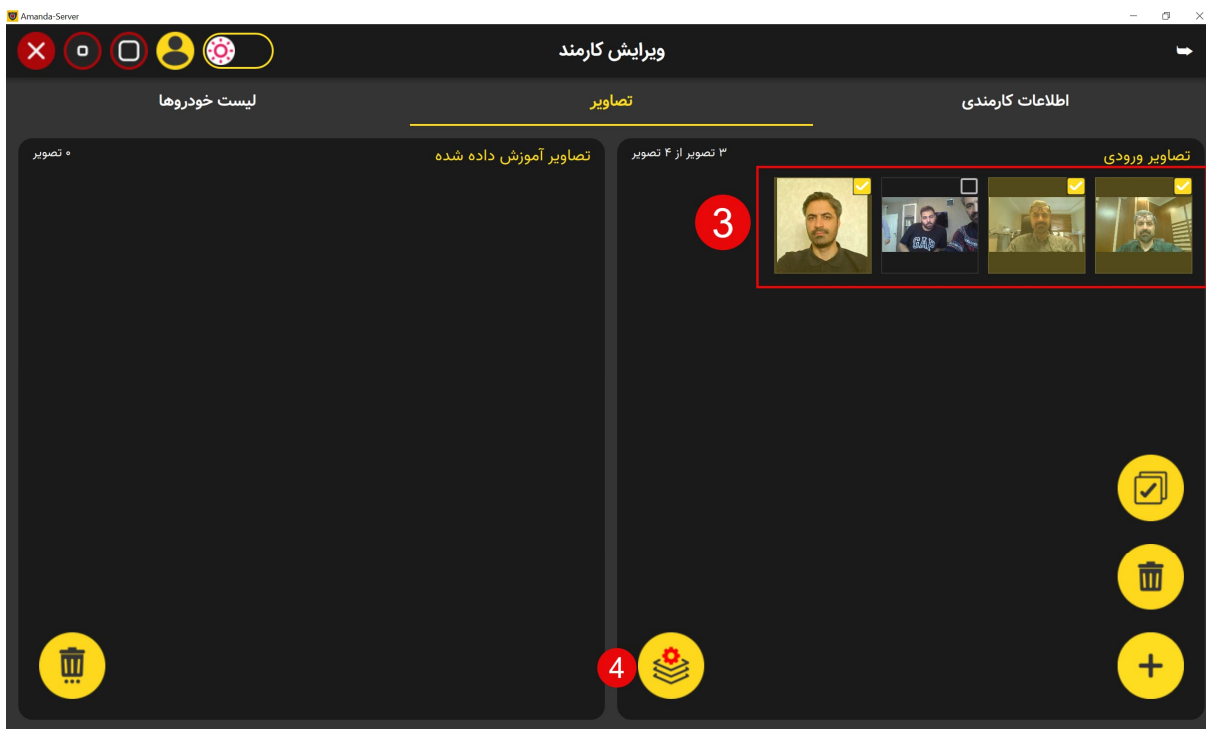
۳) انتخاب یا عدم انتخاب همه تصاویر آموزشی: با فعال کردن تیک این چک‌باکس، همه تصاویر بارگذاری شده برای انجام عملیات مورد نظر انتخاب می‌شوند (یا نمی‌شوند).

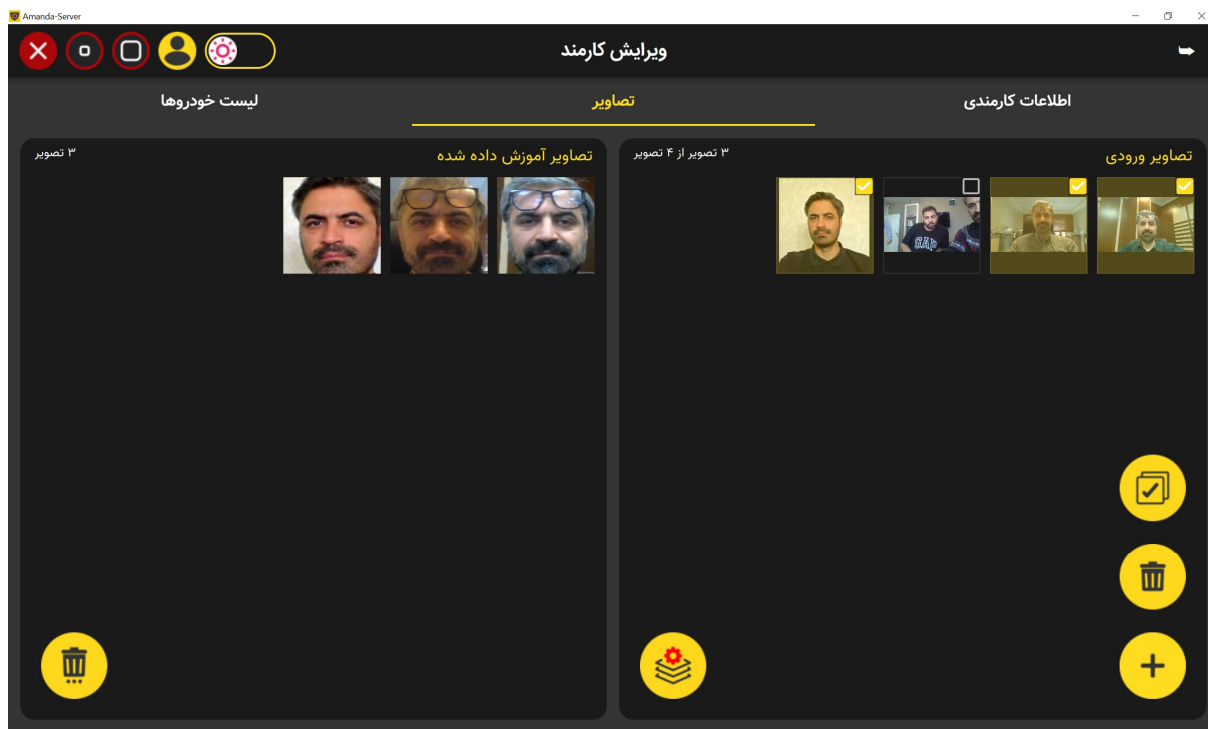
۴) آموزش تصاویر انتخاب شده: با فشردن این دکمه، تصاویر چهره آموزشی انتخاب شده جهت آموزش به سامانه پردازش می‌شوند.

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 ۲-۲۹، نمونه‌ای از فرآیند بارگذاری تصاویر چهره آموزشی و آموزش آنها به سامانه نشان داده شده است.



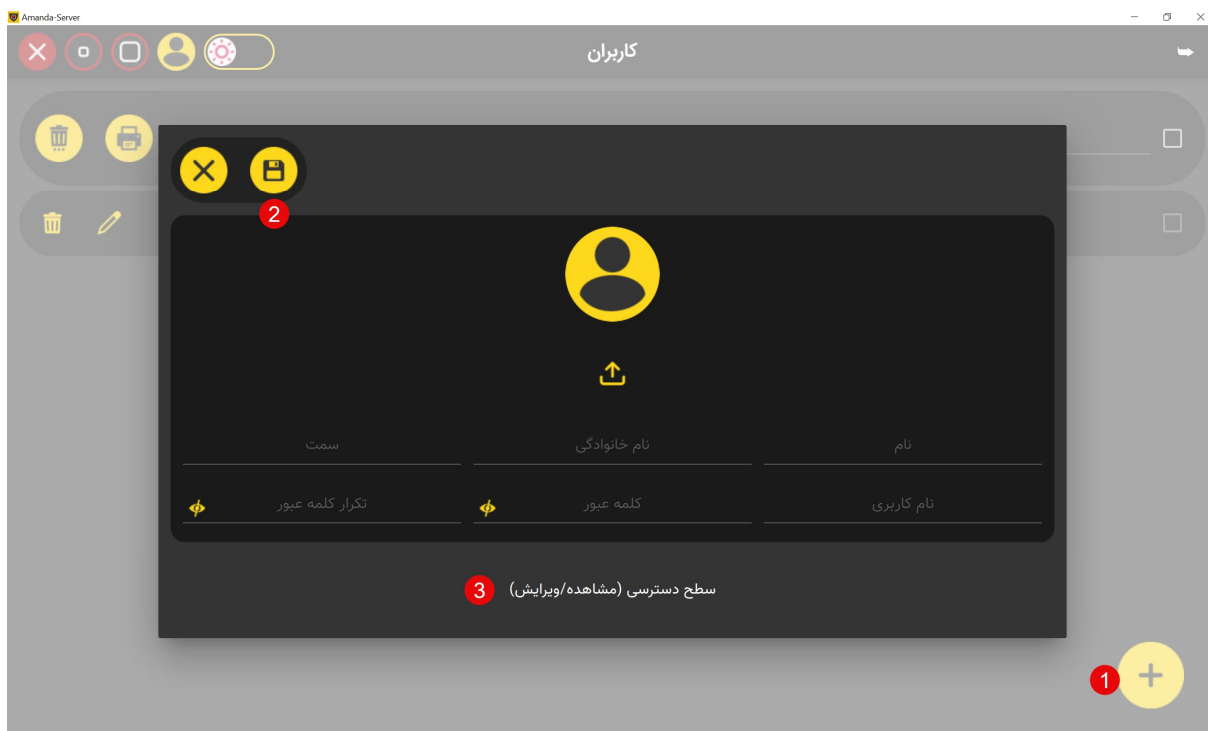




شکل ۲-۲۹: مراحل افزودن تصاویر چهره آموزشی و آموزش آن به سامانه

۸-۲) 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 ۲-۳۰ را دنبال کنید.



شکل ۲-۳۰: 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 ۲-۳۰ کلیک کنید تا وارد منوی ویرایش سطح دسترسی کاربر شوید. شکل ۲-۳۱ نمونه‌ای از این منو را نشان می‌دهد.



شکل ۲-۳۱: نمایش از منوی تعیین سطح دسترسی کاربر

در ادامه توضیح هر یک از آیتم‌های موجود در شکل ۲-۳۱ 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 به‌صورت 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 به صورت 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 (رجوع شود به ۲-۱۰).

۲-۹) راه‌اندازی کیوسک

برای راه‌اندازی 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، گزینه‌ی 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 می‌توانید محدوده زمانی را روی کیوسک ورودی-خروجی اعمال کنید تا در ساعت مشخصی ثبت ورود و ثبت خروج فعال باشد. شکل ۲-۳۱

نمایی از این قسمت را نشان می‌دهد.

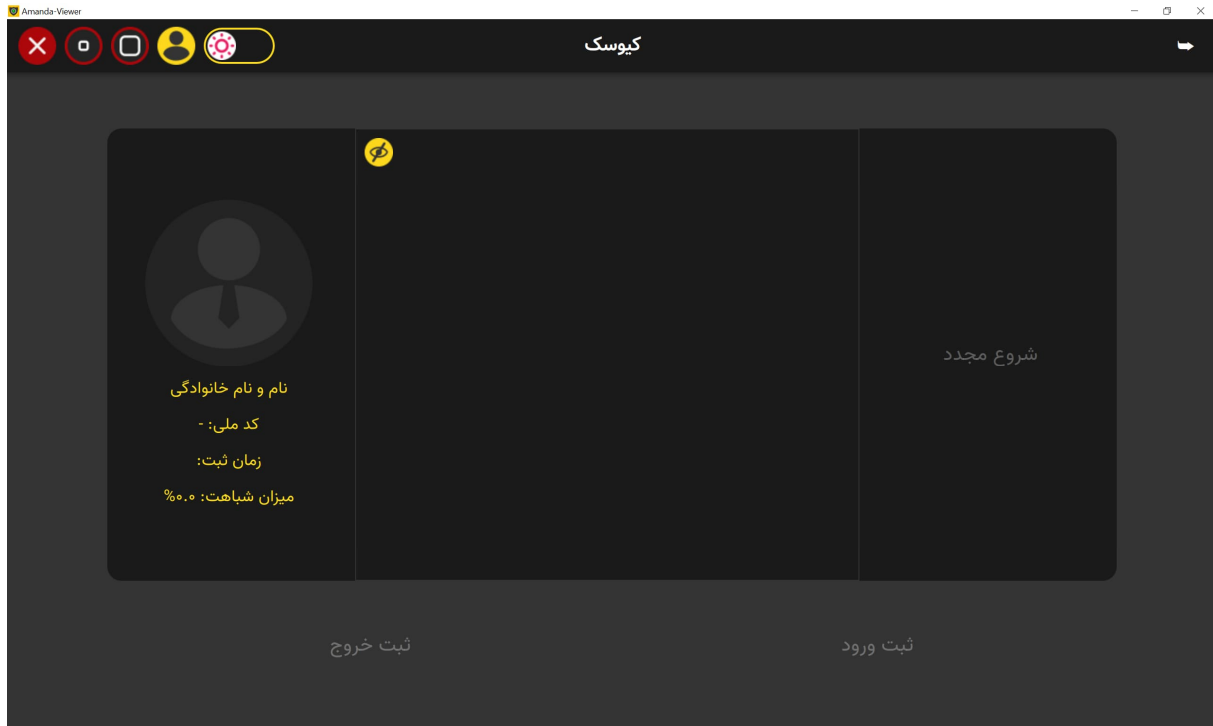


شکل ۳۱-۲: نمایی از بخش تعیین سطح دسترسی کاربر به دوربین کیوسک

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 این صورت 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 ۳۲-۲ نمای قبل از شروع این بخش را نشان می‌دهد.



شکل ۲-۳۲: 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.

۲-۱۰) ملاحظات کلیدی برای افزایش دقت و کارایی سامانه آماندا

در طراحی و بهره برداری از سامانه های پیشرفته ای مانند آماندا، 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.

۲-۱۰-۱) بکارگیری توان پردازشی GPU

تمامی عملیات و فرآیندهای مرتبط با بخش هوشمند سیستم به‌صورت 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.

۲-۱۰-۲) 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.

۲-۱۰-۳) 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.



۲-۱۰-۴) الزامات دوربین‌های تشخیص و شناسایی چهره

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

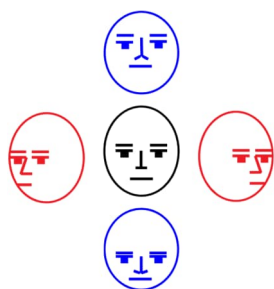
- ارتفاع دوربین از سطح زمین نباید بیش از ۲ متر باشد؛ زاویه دوربین نسبت به سطح افق برای ثبت چهره نباید از ۲۰ درجه تجاوز کند.
- زاویه انحراف افقی دوربین نیز نباید بیشتر از ۳۰ درجه باشد.
- حداقل تراکم پیکسلی مورد نیاز برای شناسایی چهره ۵۰۰ پیکسل بر متر است، به‌طوری که عرض چهره ثبت شده باید حداقل ۸۰ پیکسل باشد.
- فاصله کانونی دوربین باید به‌صورت دستی یا خودکار قابل تنظیم باشد تا امکان زوم و تمرکز دقیق روی محل ورود-خروج مورد نظر فراهم شود.
- در صورت استفاده از دوربین‌هایی 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.

۲-۱۰-۵) 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 به‌صورت 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:

^۱ 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.

۲-۱۰-۶ راهنمای تنظیمات مربوط به نوع تشخیص

در شکل ۲-۳۳، 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 ۲-۳۳: 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 به صورت 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 تعیین شده، 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 به طور 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 شرایط 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. به عنوان مثال، اگر مدت زمان عبور و مرور از گیت بازرسی به طور 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 این حال، 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.

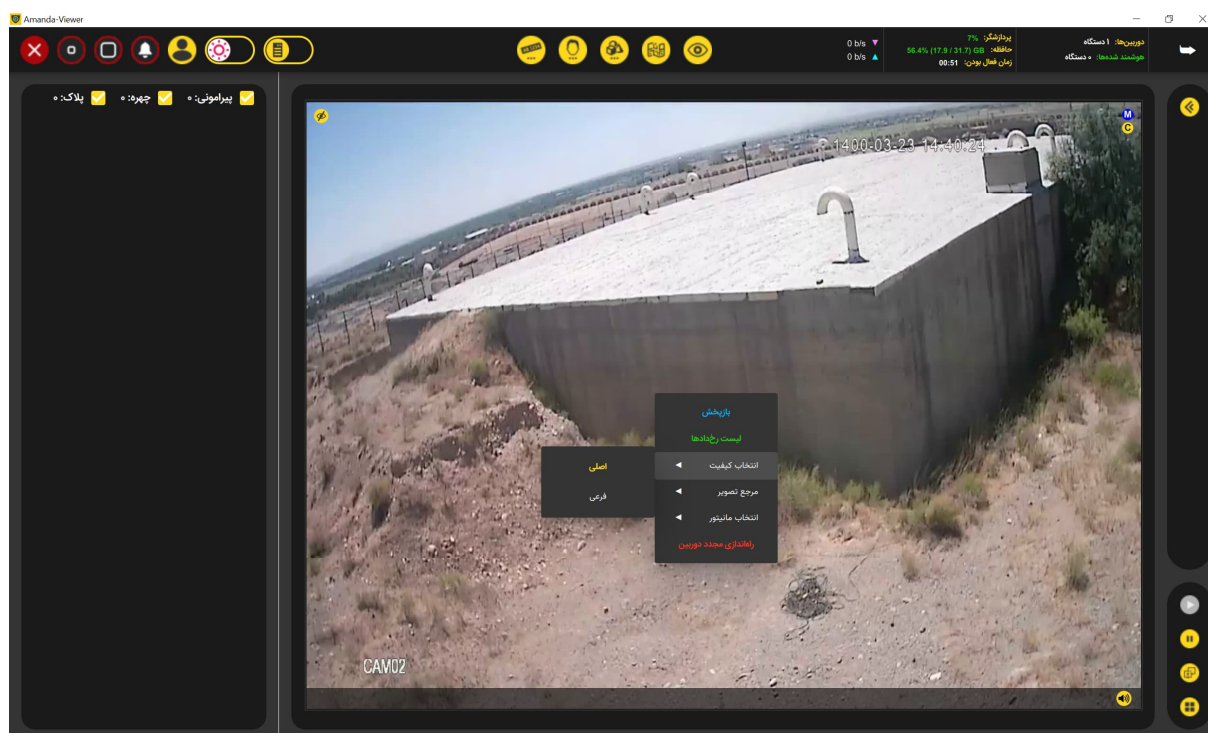
۳) پلاک‌خوان

- **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 المان‌های 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.

۲-۱-۷) 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 بخش ۳-۴) روی دوربین مورد نظر کلیک-راست کرده و از گزینه **انتخاب کیفیت** اقدام به تغییر جریان نمایید. شکل ۲-۳۴ نمونه‌ای از این فرآیند را نشان می‌دهد.



شکل ۲-۳۴: نمایی از نحوه انتخاب جریان اصلی یا فرعی برای یک دوربین

۲-۱-۸) تنظیمات ویدئو و تصویر دوربین

با استفاده از **پنل تنظیمات دوربین** که در سامانه فراهم شده است (رجوع شود به بخش ۲-۳-۱)، اپراتور می‌تواند تنظیمات ویدیویی و تصویری هر دوربین را با هدف افزایش دقت و بهینه‌سازی عملکرد هوش مصنوعی، شخصی‌سازی کند. به همین منظور، آشنایی اپراتور با مفاهیم تخصصی موجود در این پنل و کاربردهای هریک از آن‌ها، اهمیت ویژه‌ای دارد. در ادامه، مهم‌ترین پارامترهای تنظیمات تصویری به صورت خلاصه معرفی می‌شوند:



- **میزان تقویت (Gain):** میزان تقویت معیاری برای تنظیم روشنایی تصویر است که با افزایش آن، حسگر دوربین نور بیشتری از محیط دریافت می‌کند. این ویژگی در شرایط نوری ضعیف کاربرد دارد؛ هرچند افزایش بیش‌ازحد آن می‌تواند باعث افزایش نویز در تصویر شود.
- **تفاوت بین Gain و ISO:** هر دو به افزایش حساسیت حسگر به نور کمک می‌کنند، اما Gain بیشتر در تنظیمات دوربین‌های نظارتی استفاده می‌شود، درحالی‌که ISO اصطلاح رایج در دوربین‌های عکاسی دیجیتال است. هر دو عملکرد مشابهی دارند ولی مقیاس‌بندی متفاوتی دارند.
- **مقدار بهینه Gain:** مقدار بهینه Gain به شرایط محیطی بستگی دارد، اما به طور معمول توصیه می‌شود تا حد امکان آن را پایین نگه دارید تا از افزایش نویز جلوگیری شود. استفاده از نورپردازی مناسب می‌تواند نیاز به افزایش Gain را کاهش دهد.
- **نوردهی (Shutter):** شاتر تعیین می‌کند که حسگر دوربین چه مدت در معرض نور قرار بگیرد. زمان نوردهی بیشتر منجر به روشن‌تر شدن تصویر می‌شود ولی در مقابل می‌تواند باعث ایجاد تاری در اجسام متحرک شود.
- **سرعت نوردهی (Shutter Speed):** سرعت نوردهی مشخص می‌کند که شاتر چقدر سریع باز و بسته می‌شود. سرعت‌های بالاتر برای ثبت اجسام متحرک (مانند خودروها) کاربرد دارند و از تاری تصویر جلوگیری می‌کنند، درحالی‌که سرعت‌های پایین‌تر در محیط‌های کم‌نور مفیدتر هستند.
- **DWR: DWR** تکنولوژی‌ای است که به دوربین اجازه می‌دهد تا جزئیات بیشتری را در مناطق بسیار روشن یا بسیار تاریک یک صحنه ثبت کند. این ویژگی از طریق پردازش دیجیتالی تصویر انجام می‌شود و نسبت به WDR ساده‌تر و اقتصادی‌تر است.
- **تفاوت DWR و WDR:** WDR ترکیبی از دو تصویر با نوردهی متفاوت است که در سطح سخت‌افزاری انجام می‌شود و کیفیت بالاتری نسبت به DWR ارائه می‌دهد. در مقابل، DWR به صورت نرم‌افزاری پیاده‌سازی می‌شود و اغلب در دوربین‌های اقتصادی‌تر مورد استفاده قرار می‌گیرد.
- **تراز نور سفید (White Balance):** تراز نور سفید به تنظیم رنگ تصویر کمک می‌کند تا سفید، واقعاً سفید دیده شود و رنگ‌ها طبیعی‌تر به نظر برسند. بسته به نوع نور محیط (خورشید، لامپ فلورسنت، ال‌ای‌دی و ...) تنظیم این پارامتر می‌تواند کیفیت تصویر را به شکل قابل توجهی بهبود دهد.

بخش سوم

راههای استفاده

نسخه ناظر



۳) مقدمه

در این بخش، مراحل راه‌اندازی و استفاده از نسخه **ناظر**^۱ سامانه آمندا 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 آمندا روی آن نصب شده است. توجه داشته باشید که پس از وارد کردن آدرس، شماره پورت اتصال (به‌صورت پیش‌فرض ۳۰۳۰ است) را هم باید طبق شکل درج کنید.



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

^۱ Amanda-Viewer

^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 به صورت 127.0.0.1:3030 وارد شود.



نام کاربری پیش فرض admin و کلمه عبور پیش فرض Admin-123 است.



۲-۳) 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.

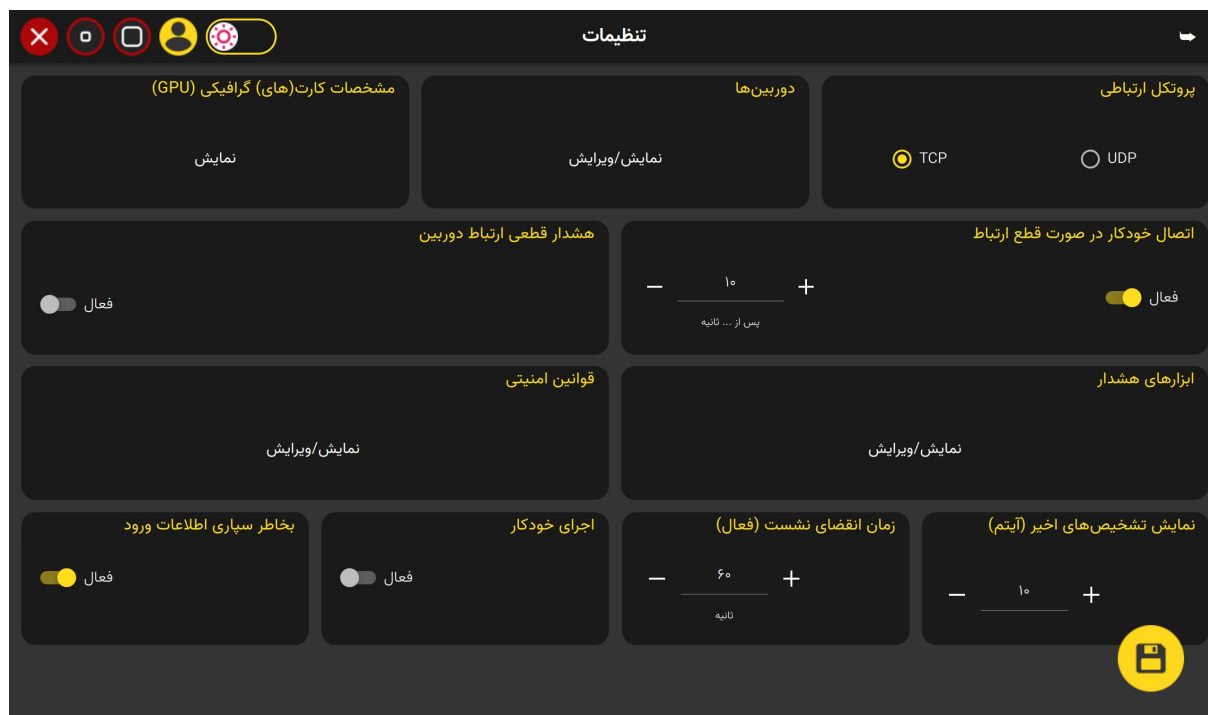
اگر شبکه دوربین ها به درستی پیکربندی شده و از پایداری مناسبی برخوردار است (بدون از دست رفتن بسته های داده)^۲ توصیه می شود از پروتکل ارتباطی UDP برای دریافت تصاویر استفاده کنید، زیرا این پروتکل تأخیر کمتری دارد و عملکرد بهتری در انتقال ویدئو ارائه می دهد. با این حال، اگر در هنگام استفاده از UDP متوجه شدید که تصاویر به صورت 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.



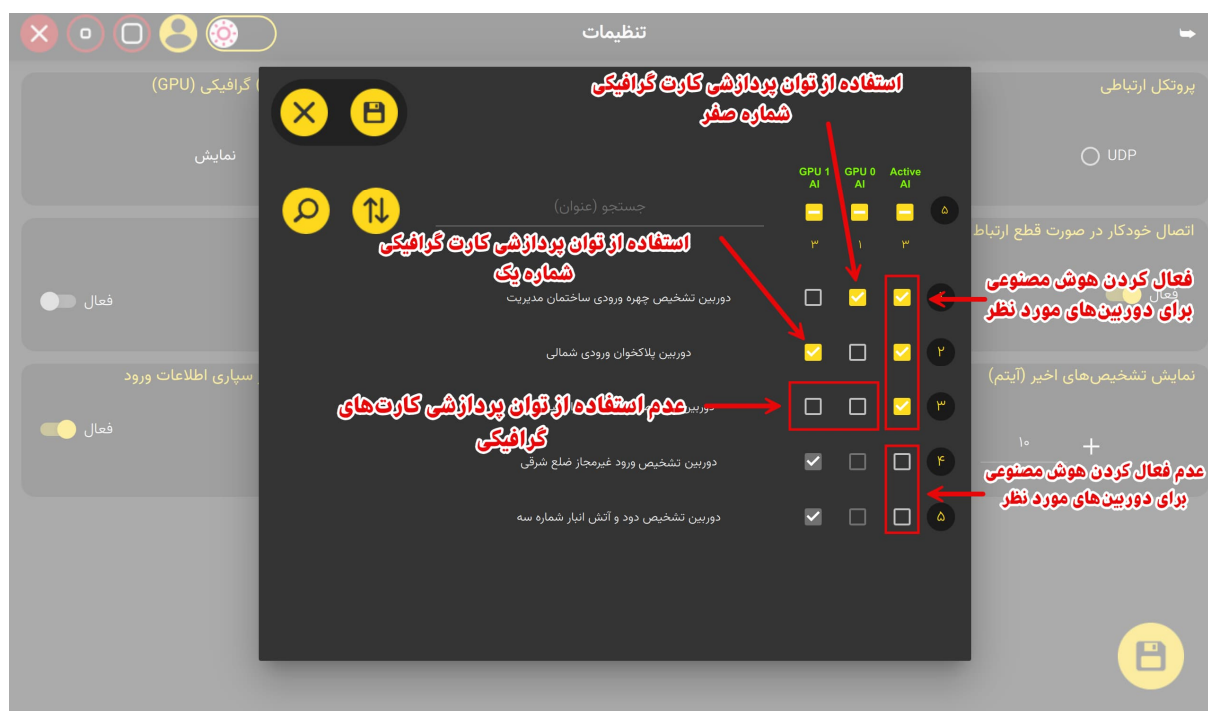
اگر امکان پردازش هوش مصنوعی به کاربری داده شده باشد، کاربر می تواند از طریق بخش **تنظیمات** و ورود به **منوی ویرایش/نمایش دوربین ها**، قابلیت هوش مصنوعی هر دوربین را فعال یا غیرفعال کرده و تعیین کند که هر دوربین از توان پردازشی کدام کارت گرافیکی (GPU0 یا GPU1) استفاده کند. شکل ۲-۳ نمایی از منوی **تنظیمات**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



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

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

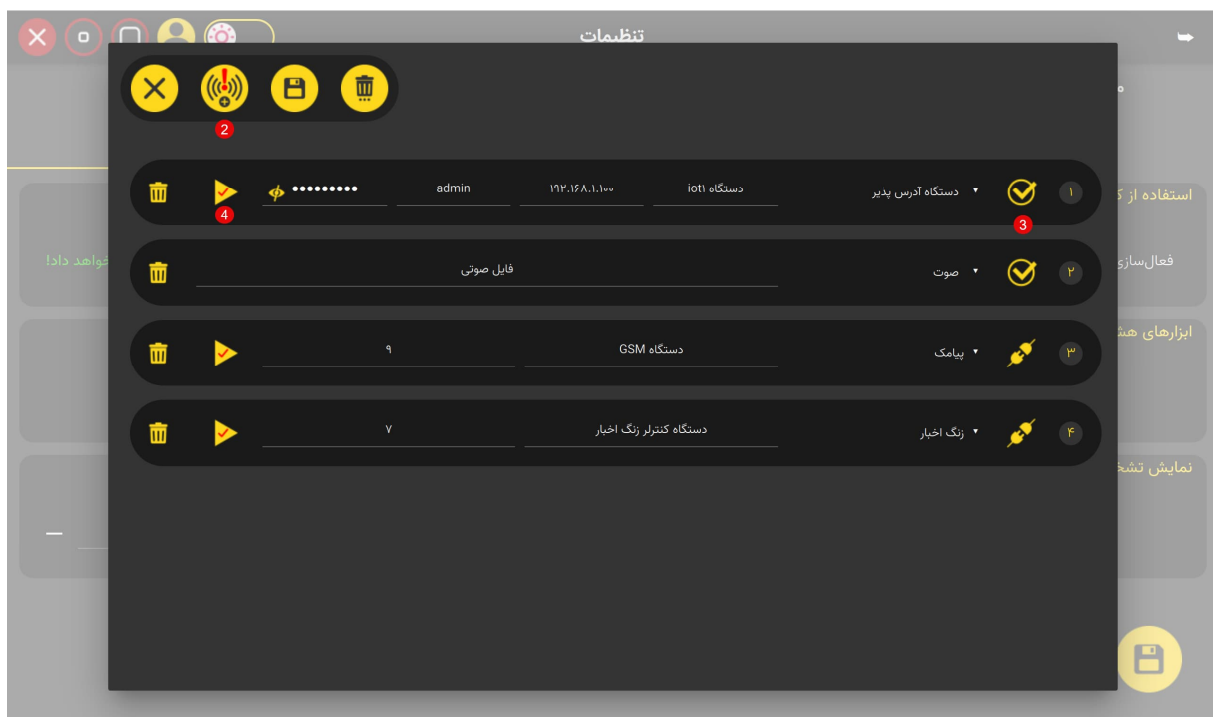
انتخاب صحیح کارت گرافیکی و یا عدم انتخاب آن برای هر دوربین، تاثیر مستقیمی در عملکرد سامانه در تشخیص‌های هوشمند خواهد داشت.



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 به‌طور 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).

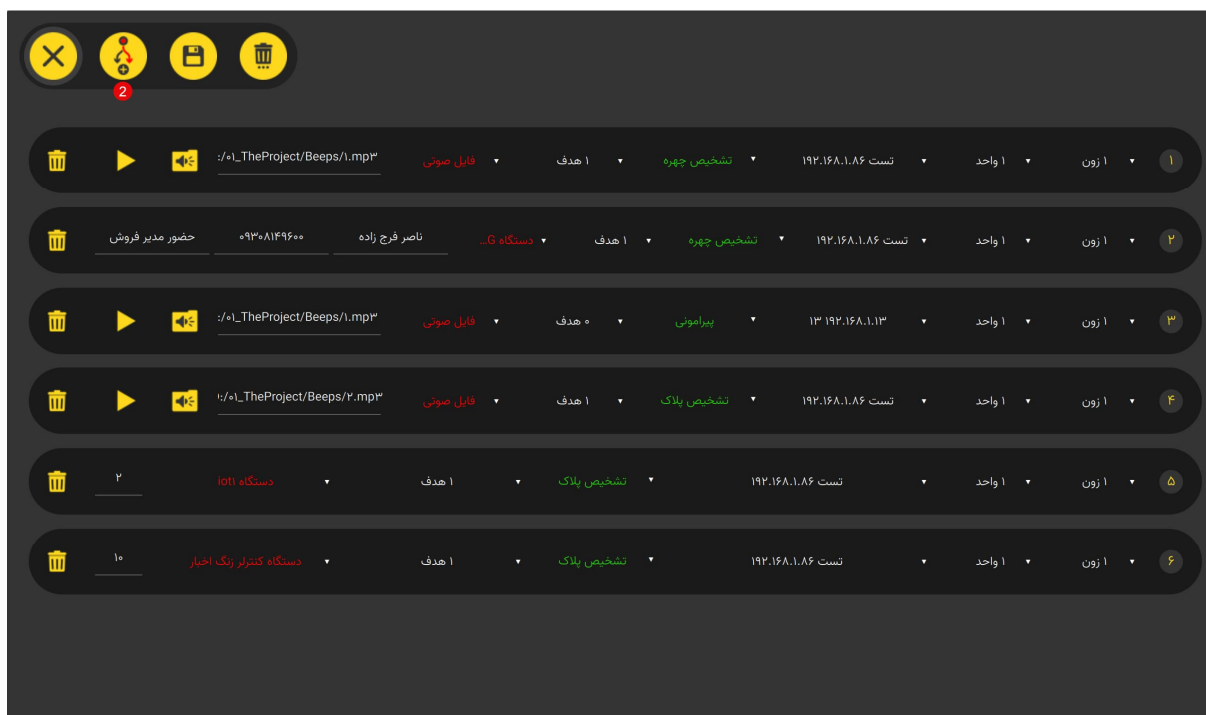


ابزار هشدار متصل است.



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، می‌توان به تعداد نامحدودی قانون امنیتی تعریف کرد. به‌عنوان مثال، اگر دوربینی مجهز به هوش مصنوعی تشخیص چهره است، می‌توانید براساس گروه کارمندی، قوانین امنیتی متفاوتی تعریف کنید. به‌عنوان مثال دیگر، اگر دوربینی مجهز به هوش مصنوعی تشخیص پلاک است، می‌توانید برای پلاک‌های خاص، قوانین مجزایی تعریف کنید.



ابزارهای هشدار و قوانین امنیتی تعریف‌شده در هر ماشین (کامپیوتر) به‌صورت محلی ذخیره شده و مختص همان ماشین می‌باشند. 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 به‌صورت محلی و جداگانه تعریف کند.

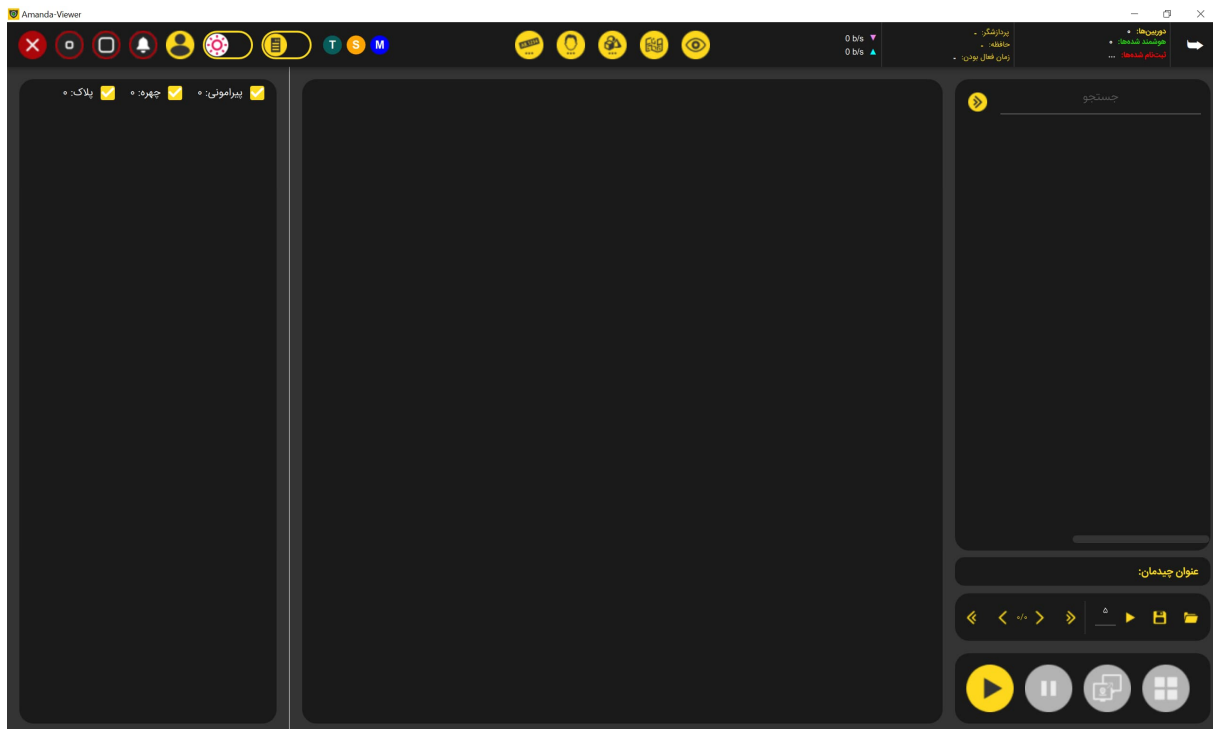


برای تسریع و سهولت تعریف قوانین مشابه، با نگه داشتن کلید Ctrl و فشردن دکمه افزودن قانون امنیتی جدید، می‌توانید کپی آخرین قانون تعریف شده را ایجاد کرده و تغییرات جزئی مورد نظر خود را روی آن اعمال کنید.

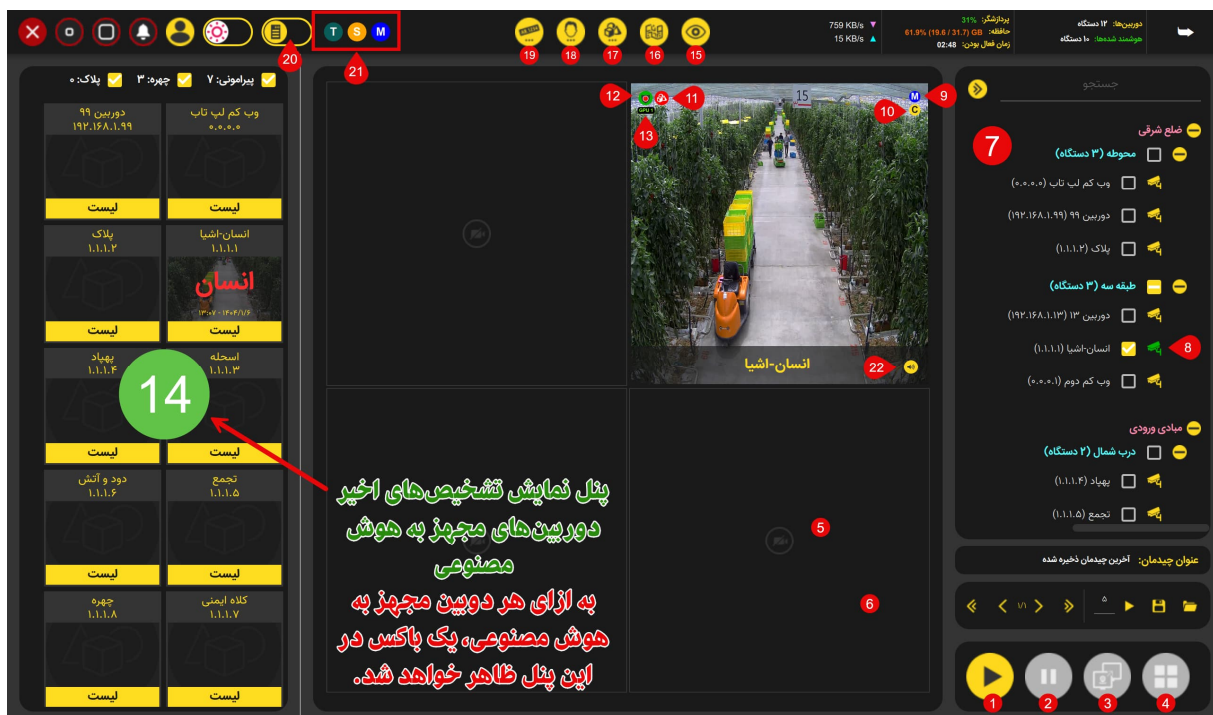


۳-۴) اجرا

پس از انجام تنظیمات مربوط به دوربین‌ها، زمان آن فرا رسیده است که سامانه را اجرا کرده و از آن بهره‌برداری 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 می‌دهد.



(الف)



(ب)

شکل ۳-۷: 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 ۳-۷ (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 ۷)، دوربین‌های مورد نظر خود را می‌توانید برای نمایش تصویرش، انتخاب کنید (چک‌باکس‌ش را فعال کنید). توجه داشته باشید که ترتیب ظاهر شدن دوربین‌ها در صفحه نمایش، به ترتیب انتخاب آنها از پنل درختی است. همچنین، می‌توانید با گرفتن باکس نمایش دوربینی و کشیدن آن روی باکس دیگر، جای نمایش دو دوربین را عوض 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 آن را 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:

¹ Layout



اتصال به دوربین برقرار نیست.



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.



جریان سوم (مناسب برای موبایل) در حال نمایش است.



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

تصاویر از سرور (به‌صورت غیر مستقیم) دریافت می‌شوند.



تصاویر به‌صورت مستقیم از دوربین دریافت می‌شوند.



۱۱) نشانگر نوع تشخیص هوش مصنوعی دوربین:

تشخیص حرکت



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



تشخیص ترک پُست نگهبانی-بازرسی یا محل کار





تشخیص شیء 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 فnsی 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) پنل نمایش لیست تشخیص‌های دوربین‌ها: در این پنل، 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 دو برگه‌ی دیگر (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 به صورت 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 به صورت 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.



(۲۱) تغییر کیفیت تصاویر: با استفاده از این آیتم، می‌توانید به یکباره کیفیت همه تصاویر در حال نمایش را به یکی از حالت‌های اصلی، فرعی و موبایل تغییر دهید.

تغییر کیفیت تصاویر تمامی دوربین‌ها به حالت کیفیت اصلی، نیازمند پردازش بالایی بوده و ممکن است منجر به کاهش عملکرد یا بروز اختلال در سیستم شود.

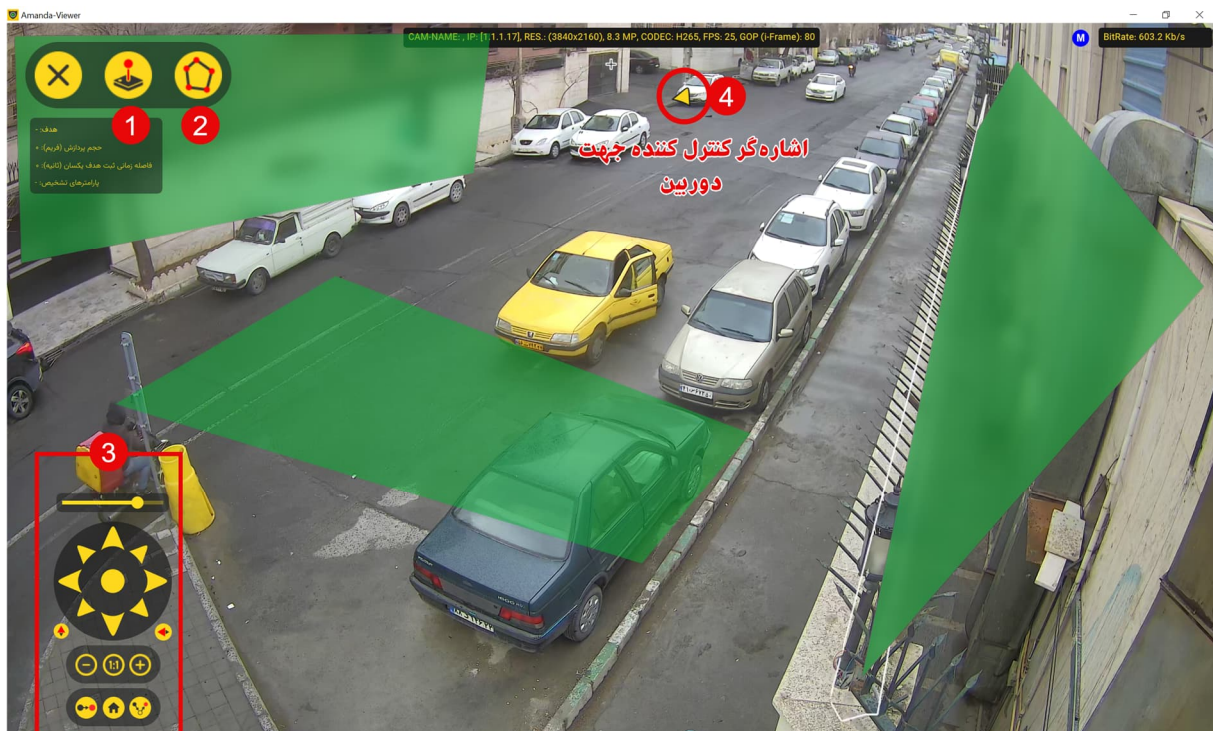


(۲۲) پخش صدا: اگر دوربین مورد نظر دارای میکروفون باشد، با کلیک روی این آیتم، صدای دریافت شده از دوربین پخش می‌شود.

۳-۴-۱) نمایش جریان اصلی و کنترل دوربین

برای مشاهده‌ی جریان اصلی (کیفیت اصلی) هر یک از دوربین‌ها، کافی است روی دوربین مورد نظر کلیک کنید تا تصویر آن با کیفیت اصلی نمایش داده شود. شکل ۳-۸ از منوی نمایش جریان اصلی دوربین را نشان می‌دهد.

با فشردن آیتم شماره ۱ در شکل ۳-۸، کنترل دوربین چرخشی^۱ ظاهر می‌شود (آیتم شماره ۳). این کنترلر به کاربر امکان تغییر زاویه‌ی دید دوربین را می‌دهد. علاوه بر این، در صورت فعال بودن کنترلر، کاربر می‌تواند با حرکت ماوس به سمت نقطه‌ی مورد نظر و نگه داشتن دکمه‌ی چپ آن (مطابق نشانگر مشخص شده در آیتم شماره ۴)، زاویه‌ی دوربین را در همان جهت تنظیم کند. توجه داشته باشید که هرچه این نشانگر از مرکز تصویر فاصله‌ی بیشتری داشته باشد، سرعت تغییر زاویه بیشتر خواهد بود. برعکس، اگر نشانگر به مرکز نزدیک‌تر باشد، حرکت دوربین آهسته‌تر و دقیق‌تر خواهد شد.



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

علاوه بر این، از طریق این بخش امکان استفاده از پریست‌های تعریف‌شده در دوربین و همچنین اجرای تور^۳ دوربین نیز در دسترس می‌باشد.

با انتخاب آیتم شماره ۲، فنس‌های ترسیم‌شده نمایش داده می‌شوند. با انتخاب مجدد این آیتم، فنس‌ها مخفی خواهند شد.

^۱ PTZ (Pan, Tilt, Zoom)

^۲ Preset

^۳ Tour

۳-۴-۲) قابلیت زوم آپتیکال^۱ و دیجیتال^۲

برای زوم آپتیکال روی ناحیه‌ی مورد نظر، کاربر می‌تواند با چرخاندن چرخ ماووس به جلو یا عقب، بزرگ‌نمایی یا کوچک‌نمایی را انجام دهد. علاوه بر این، اگر کاربر بخواهد روی نقطه‌ی خاصی زوم دیجیتال انجام دهد، کافی است دکمه‌ی چپ ماووس را نگه داشته و روی ناحیه‌ی مورد نظر یک مستطیل بکشد. سپس با چرخاندن چرخ ماووس به جلو یا عقب، می‌تواند در محدوده‌ی انتخاب شده زوم دیجیتالی انجام دهد. همچنین، کاربر می‌تواند مستطیل رسم شده را گرفته و آن را به هر نقطه‌ای از تصویر که نیاز باشد جابه‌جا کند. برای غیرفعال کردن زوم دیجیتال کافی است خارج از مستطیل رسم شده، کلیک کنید. شکل ۳-۹ نمونه‌ای از زوم دیجیتال را نشان می‌دهد.

با دابل-کلیک روی ناحیه بزرگ‌نمایی‌شده (زوم دیجیتال)، امکان ثبت و ذخیره تصویر لحظه‌ای^۳ از همان محدوده فراهم می‌گردد.



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.



شکل ۳-۹: نمایی از قابلیت زوم دیجیتال

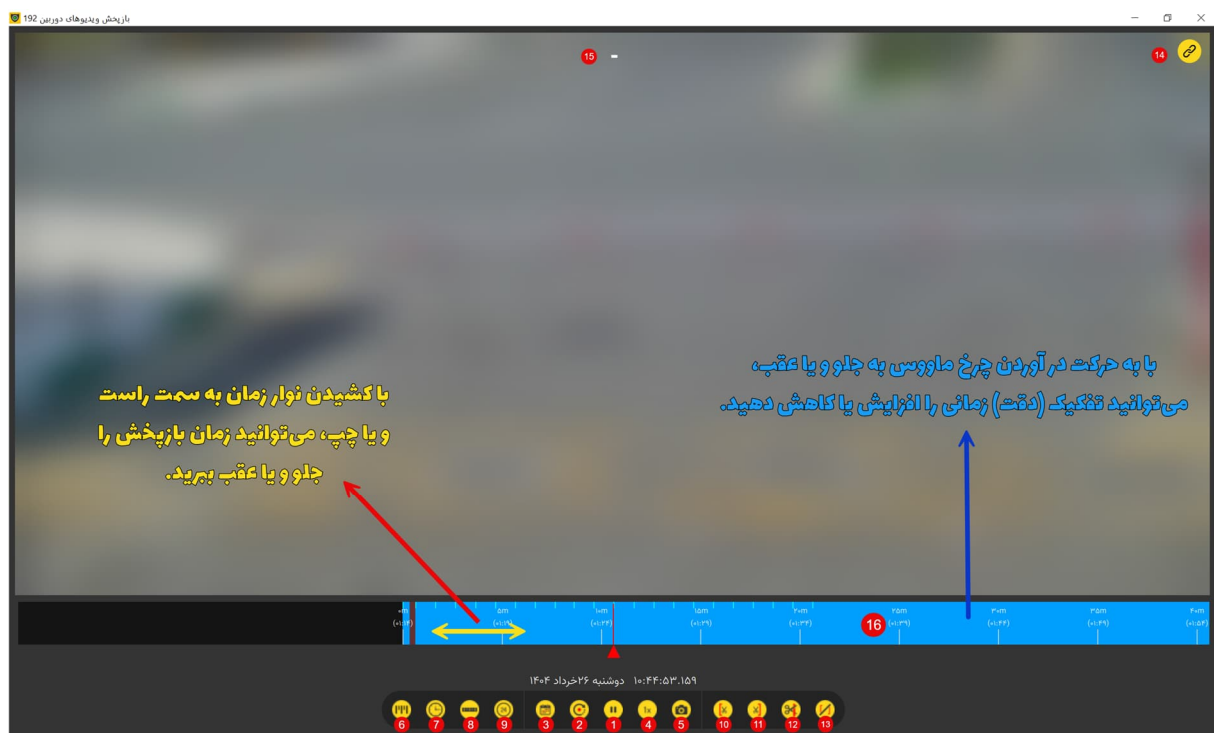
^۱ Optical Zoom

^۲ Digital Zoom

^۳ Snapshot

۳-۴-۳) بازپخش ویدیوهای ضبط شده

برای بازپخش ویدیوهای ضبط شده، روی دوربین مورد نظر کلیک-راست کرده و از منوی ظاهر شده، گزینه **بازپخش** را انتخاب کنید. همچنین، با کلیک-راست کردن روی دوربین مورد نظر در پنل درختی نمایش دوربین‌ها و انتخاب گزینه **بازپخش**، می‌توانید ویدیوهای ضبط شده دوربین مورد نظر را مشاهده کنید. در شکل ۳-۱۰، نمونه‌ای از پنجره بازپخش ویدیوهای ضبط شده نشان داده شده است.



شکل ۳-۱۰: نمایی بازپخش ویدیوهای ضبط شده

در ادامه، کاربرد هر یک از آیتم‌های نشان داده شده در شکل ۳-۱۰ به ترتیب توضیح داده می‌شوند:

- ۱) **شروع/توقف بازپخش:** اجرای و یا توقف بازپخش ویدیوی جاری
- ۲) **بارگذاری مجدد ویدیو:** بازخوانی اطلاعات ویدیویی برای اطمینان از نمایش آخرین داده‌های موجود
- ۳) **انتخاب روز برای بازپخش:** انتخاب تاریخ مورد نظر جهت مشاهده ویدیوهای ضبط شده همان روز
- ۴) **تغییر سرعت بازپخش:** افزایش یا کاهش سرعت پخش ویدیو نسبت به حالت عادی
- ۵) **اسنپ‌شات از فریم جاری:** ثبت اسنپ‌شات از فریم در حال نمایش



۶) نمایش/عدم نمایش زمان روی نوار زمان: تنظیم نمایش یا پنهان سازی مقیاس زمانی روی نوار زمانی

۷) نمایش/عدم نمایش ساعت روزانه روی نوار زمان: نمایش یا مخفی کردن تقسیم بندی ساعت های شبانه روز روی نوار زمانی

۸) بازگشت به تفکیک زمانی پیش فرض: ریست کردن تنظیمات نوار زمان به حالت نمایشی اولیه و پیش فرض

۹) نمایش ۲۴ ساعته نوار زمانی: فعال سازی نمایش کامل بازه ۲۴ ساعته یک روز در نوار زمانی

۱۰) شروع برش: تعیین نقطه شروع بازه ای انتخاب شده جهت برش

۱۱) پایان برش: تعیین نقطه پایان بازه ای انتخاب شده جهت برش

۱۲) انجام عمل برش: استخراج و ذخیره بازه ای انتخابی به عنوان یک فایل ویدیویی مجزا

۱۳) پاک کردن نشان گذاری های برش: حذف نقاط شروع و پایان برش تعریف شده برای برش

۱۴) همزمانی بخش: همگام سازی بازپخش ویدیوها از چند دوربین به صورت همزمان و بر اساس یک زمان مشترک

۱۵) حذف/نمایش دکمه ها و سایر جزییات: پنهان یا نمایش دادن کنترل ها برای ایجاد فضای نمایشی ساده تر

۱۶) نوار زمانی: نوار بصری نمایش بازه ای زمانی ضبط شده، همراه با نشانه های رویداد یا داده

کاربر می تواند هنگام بازپخش ویدیو، همانند حالت نمایش زنده، از قابلیت زوم دیجیتال استفاده کند.



۳-۵) آمار و گزارش گیری

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

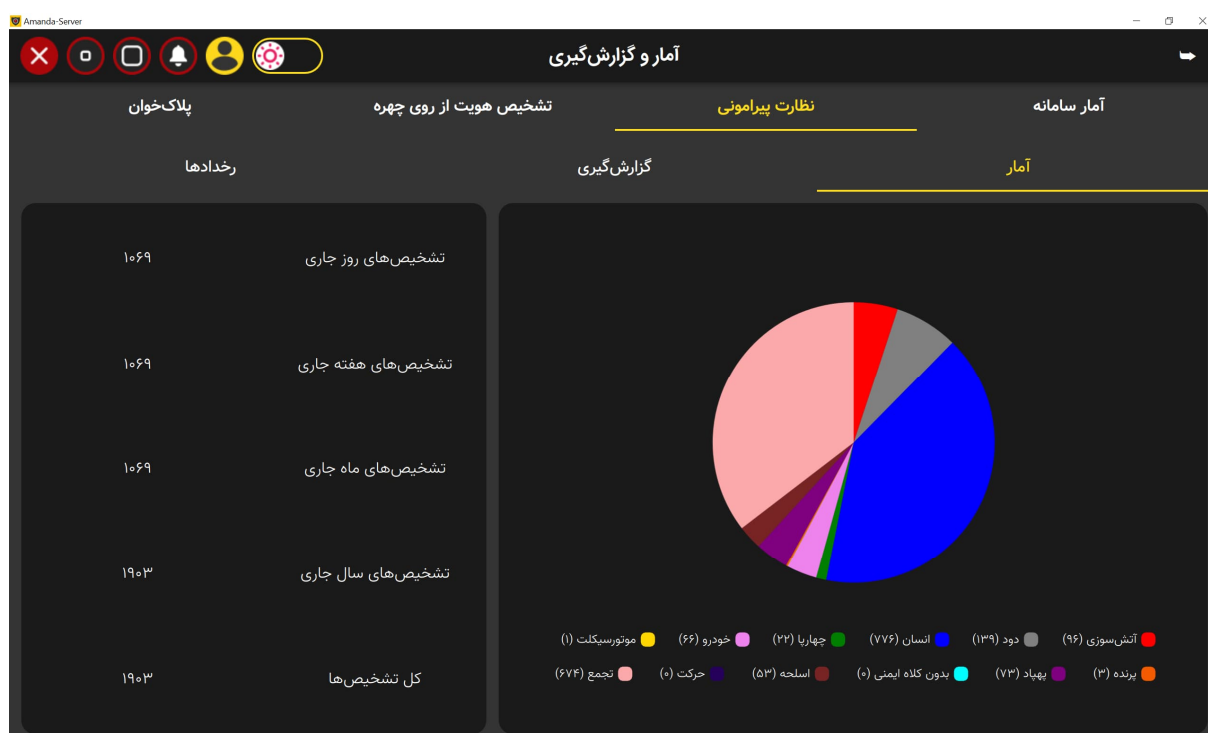
۱) آمار سامانه: در این برگه آمار کلی سامانه در معرض نمایش قرار می گیرد.

۲) نظارت پیرامونی: در این برگه آمار مرتبط با تشخیص های پیرامونی و امکانات گزارش گیری 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 ۳-۱۱، نمایی از این بخش نشان داده شده است.



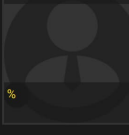
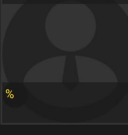
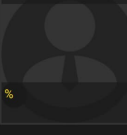
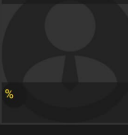
شکل ۳-۱۱: نمایی از بخش آمار و گزارش‌گیری سامانه

۳-۶) ثبت‌نام برخط اشخاص

از این روش زمانی استفاده می‌شود که نیاز به ثبت‌نام برخط و آبی اشخاص باشد؛ در زمان اجرا، لیست تشخیص‌های اخیر دوربین مورد نظر را باز کرده و روی تصویر چهره ثبت شده کلیک نمایید تا متویی که شامل تصویر صورت شخص و جزئیات تشخیص است، ظاهر شود. سپس مراحل نشان داده شده در شکل ۳-۱۲ را برای ثبت‌نام برخط اشخاص دنبال کنید.



✕ ۱۰ تشخیص اخیر دوربین (۱.۱.۱.۲)

 ۱۴:۳۸ - ۱۴:۳۹/۹ چهره: % ناشناس	 ۱۴:۳۸ - ۱۴:۳۹/۹ چهره: % ناشناس	 ۱۴:۳۸ - ۱۴:۳۹/۹ چهره: % ناشناس	 ۱۴:۳۸ - ۱۴:۳۹/۹ چهره: % ناشناس	 ۱۴:۳۸ - ۱۴:۳۹/۹ چهره: % ناشناس
 % چهره: % ناشناس	 % چهره: % ناشناس	 % چهره: % ناشناس	 % چهره: % ناشناس	 ۱۴:۳۸ - ۱۴:۳۹/۹ چهره: % ناشناس

✕ ۱۰ تشخیص اخیر دوربین (۱.۱.۱.۲)



۱۴:۳۸ - ۱۴:۳۹/۹
چهره: %
ناشناس

۱۴:۳۸ - ۱۴:۳۹/۹
چهره: %
ناشناس

میزان شباهت: %

هدف: چهره ناشناس

نام دوربین: بدون نام

زمان تشخیص: ۱۴:۳۸ - ۱۴:۳۹/۹

ویرایش ۲

✕
✓
3

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

مهدی	نام:	
طارمی	نام خانوادگی:	
FirstName	نام انگلیسی:	
LastName	نام خانوادگی انگلیسی:	
↻ 4 ۱۳۳۴۵۶۷۸۹	کد ملی:	
هیچکدام ▼	سمت:	
نامعلوم	شغل:	
۱۳۰۰/۰۱/۰۱	تاریخ تولد:	
۰۹۰۰۰۰۰۰۰۰۰۰	شماره همراه:	
۰	شماره پرسنلی:	

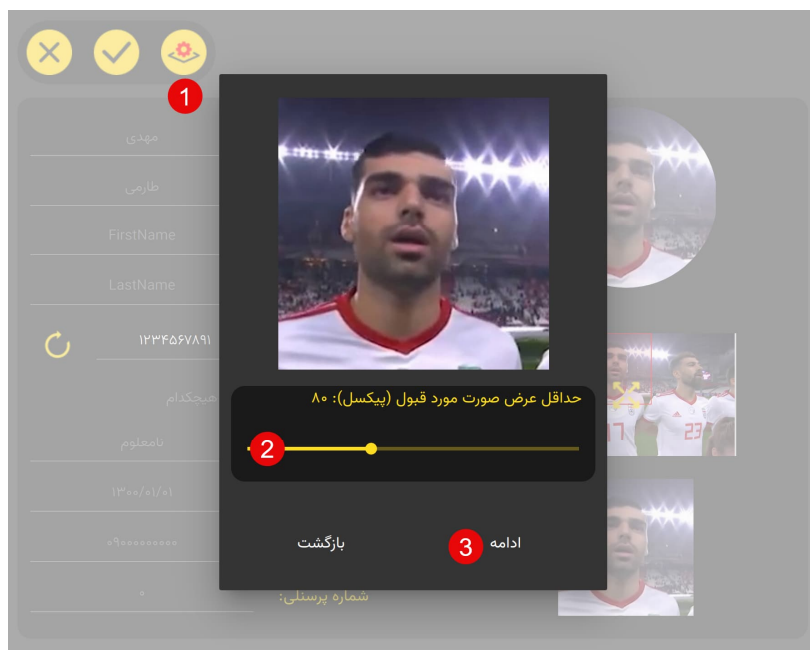



شکل ۳-۱۲: مراحل ثبت نام برخط اشخاص

با فشار دادن دکمه شماره ۳ در شکل ۳-۱۲، فرآیند ثبت نام برخط به اتمام می رسد. 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 ۳-۱۳). 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 می شود. شکل ۳-۱۳ نمونه ای از فرآیند کار را نشان می دهد.

اگر تصویر چهره ی شخصی که قبلا در سامانه ثبت نام شده است، تحت عنوان ناشناس گزارش شده باشد، می توانید با وارد کردن کد ملی آن شخص و فشردن دکمه شماره ۴ (نشان داده شده در شکل ۳-۱۲)، 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 ثبت نام برخط افراد انجام می شود، با این تفاوت که برای ثبت خودرو به نام یک شخص، لازم است ابتدا آن شخص در سامانه ثبت نام شده باشد.



شکل ۳-۱۳: مراحل آموزش برخط تصویر ثبت شده برای شخص مورد نظر

بخش چهارم

راهنمای استفاده

نسخه تحت وب

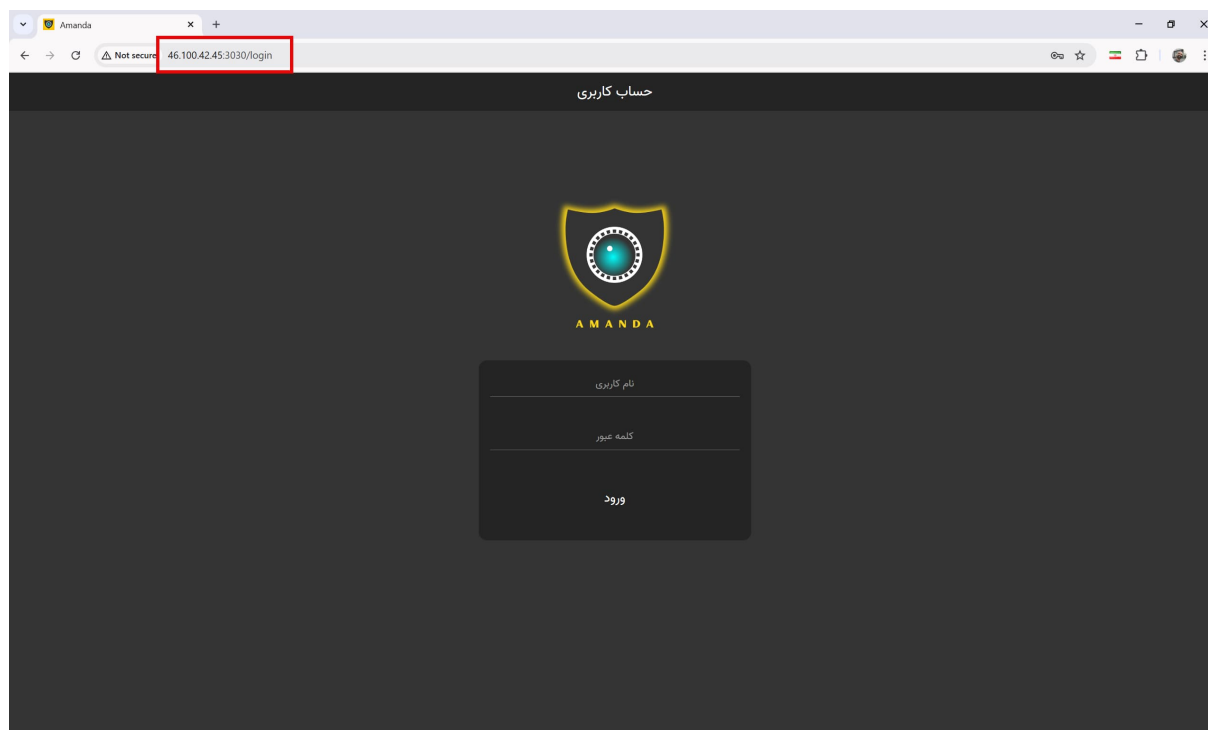


۴) مقدمه

در این بخش، نحوه استفاده از وب-اپلیکیشن^۱ سامانه آماندا ارائه می‌شود. اپلیکیشن تحت وب آماندا بستری یکپارچه و امن برای دسترسی به تصاویر و اطلاعات سامانه مدیریت ویدئویی آماندا از طریق مرورگر وب را فراهم می‌کند. کاربران می‌توانند بدون نیاز به نصب هیچ‌گونه نرم‌افزار یا افزونه، و صرفاً با استفاده از مرورگر کروم^۲، از داخل یا خارج از سازمان به سامانه متصل شوند.

این اپلیکیشن امکان مشاهده زنده تصاویر دوربین‌ها، بررسی و مرور رخدادها، کشف‌شده توسط ماژول‌های هوش مصنوعی، و همچنین تهیه گزارش‌های متنوع و کاربردی را در اختیار کاربران قرار می‌دهد. طراحی مبتنی بر وب این سامانه، دسترسی سریع، سهولت استفاده و انعطاف‌پذیری بالا را برای مدیران و اپراتورها تضمین می‌کند.

به منظور مشاهده تصاویر دوربین‌هایی که از فشرده‌سازی H265 استفاده می‌کنند در اپلیکیشن تحت وب آماندا، لازم است کاربران از مرورگر کروم نسخه ۱۴۰ یا بالاتر استفاده نمایند. در نسخه‌های پایین‌تر مرورگر یا سایر مرورگرها، نمایش این نوع تصاویر ممکن است با محدودیت یا عدم پشتیبانی مواجه شود.



شکل ۴-۱: نمایی صفحه ورود به حساب کاربری در اپلیکیشن تحت وب آماندا

^۱ Web-Application

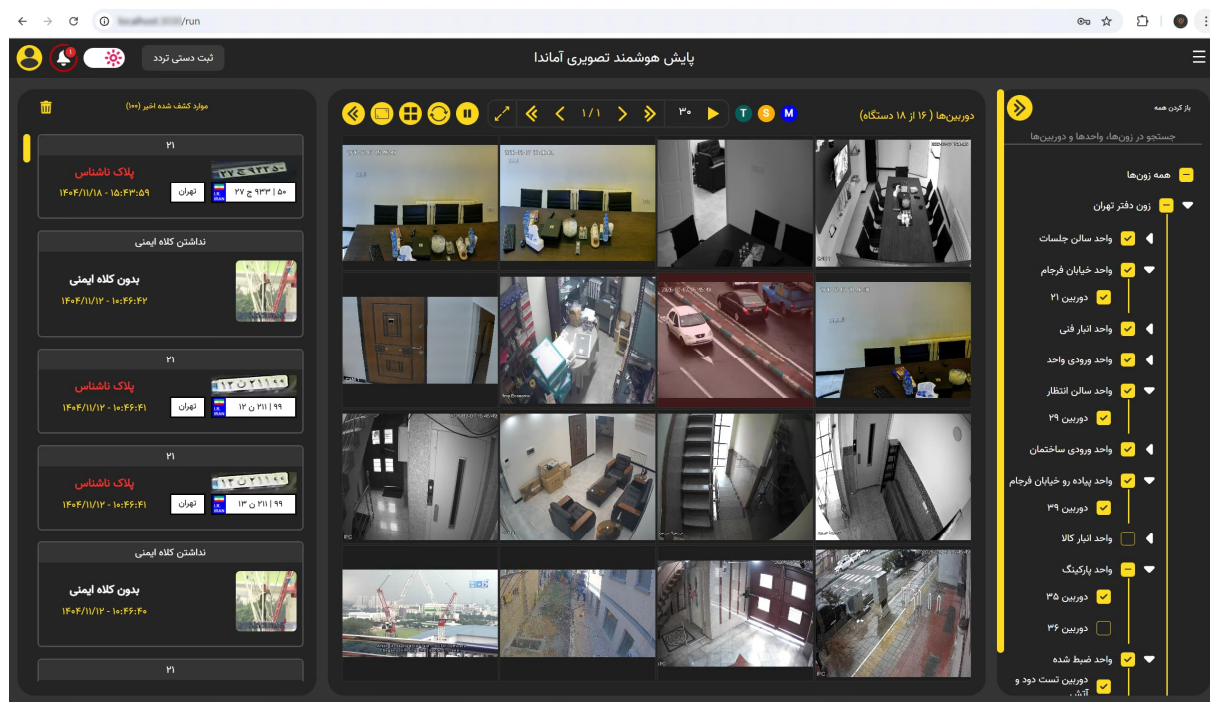
^۲ Google Chrome

۴-۱) ورود به حساب کاربری

مرورگر کروم را اجرا کرده و در نوار آدرس، آدرس سرور آماندا را به همراه شماره پورت مربوطه وارد نمایید. آدرس وب سرور (مطابق شکل ۴-۱) مربوط به همان سیستمی است که نسخه سرور آماندا روی آن نصب شده است. به صورت پیش فرض، شماره پورت ۳۰۳۰ در نظر گرفته شده است. در صورتی که آدرس و شماره پورت به درستی وارد شده باشند، صفحه ورود سامانه مطابق شکل ۴-۱ نمایش داده خواهد شد. در این مرحله با وارد کردن نام کاربری و کلمه عبور خود، می توانید وارد پنل کاربری شوید.

۴-۲) نظارت آنلاین

پس از ورود به پنل کاربری، از منوی اصلی گزینه **نظارت آنلاین** را انتخاب نمایید تا وارد صفحه اجرای سامانه شوید. در این صفحه، امکان مشاهده زنده تصاویر دوربین‌هایی که دسترسی به آن‌ها برای شما تعریف شده است فراهم می‌باشد. در پنل سمت چپ صفحه، فهرست رخدادهای کشف شده توسط سامانه به صورت لیست نمایش داده می‌شود. همچنین در پنل سمت راست، لیست دوربین‌ها قابل مشاهده است و می توانید بر اساس اولویت یا اهمیت، دوربین‌های مورد نظر را برای نمایش انتخاب نمایید. شکل ۴-۲ نمای کلی این صفحه را نشان می‌دهد.



شکل ۴-۲: نمای از صفحه نظارت آنلاین اپلیکیشن تحت وب آماندا

۳-۴) گزارش گیری

با استفاده از منوی و انتخاب گزینه **گزارش گیری** وارد بخش گزارش گیری می‌شود. در این بخش، کاربران می‌توانند از رخدادهای کشف‌شده توسط سیستم، گزارش‌های متنوع تهیه نمایند. در این بخش امکان گزارش گیری از سه نوع رویداد کشف‌شده شامل نظارت پیرامونی، تشخیص چهره و تشخیص پلاک فراهم شده است. همچنین، کاربران می‌توانند با استفاده از ابزارهای فیلترگذاری نتایج، گزارش‌ها را بر اساس معیارهایی مانند بازه زمانی، دوربین، نوع رخداد و سایر پارامترهای قابل انتخاب محدود نمایند. خروجی گزارش‌ها به‌صورت فایل‌های PDF و Excel قابل دریافت بوده و امکان ذخیره‌سازی یا اشتراک‌گذاری آن‌ها وجود دارد. شکل ۳-۴ نمونه‌ای از این بخش را نشان می‌دهد.

شکل ۳-۴: نمایش صفحه گزارش گیری اپلیکیشن تحت وب آماندا



A M A N D A[®]

AI POWERED

دفتر مرکزی و فروش: تهرانپارس، اتوبان باقری، خیابان فرجام شرقی، جنب نمایندگی ایران خودرو، پلاک ۵۲، واحد ۷ و ۸

تلفکس: ۰۲۱-۷۶۷۰۱۵۴۹ / ۰۲۱-۷۶۷۰۱۵۶۲

کد پستی: ۱۶۵۳۹۶۹۳۱۸