Restricted areas/times

> Secure restricted areas with our powerful AI-based monitoring system that detects and prevents unauthorized access in real-time

Overview

Unauthorized access to restricted zones at the workplace can lead to theft, accidents, and other security breaches. Be it valuable assets, sensitive information or providing employee safety, maintaining high-security and controlled access for restricted zones at the workplace is essential for all organizations. However, monitoring and controlling access to these areas is often an expensive and error-prone process, requiring continuous manual surveillance by security personnel.

Another major problem with existing systems cannot detect intrusion after an unauthorized access has been made.This renders biometric, sensors and security personnels ineffective after an unauthorized access has been already made.

Vision AI based monitoring

With our Vision AI monitoring you can authorize access as well as continuous monitor live feeds inside a restricted area for real-time detection of unauthorized personnel. Our fully automated detection models are not only more powerful and accurate than existing systems but also more affordable and easy to integrate into existing infrastructure allowing users to scale the power of i-based real-time detection with a few simple clicks.

Detection of unauthorized entry event

Events

VisionAI model's generated events would be:

- Person detected in restricted area
- Movement detected in restricted area
- Person detected after hours
- Movement detected after hours"

It is recommended that any instance of unauthorized entry be reported to the appropriate authority. An event data for a unauthozrized entry in exclusion zones may include information such as:

- Date and time of the event
- Location of the event
- Image of the event

Configuration

It is recommended to set up camera in ceiling view to detect unauthorized entry events.

Model Details

Dataset

The dataset consists of images and videos collected from diverse sources and is designed to reflect real-world scenarios. It is evenly distributed with:

- *Different environments*: Both indoor and outdoor with varying/contrasting surrounding and infrastructure details
- *Different angles and perspectives*: The dataset includes images captured from different angles and perspectives, such as from above, below, or from the side of subjects
- *Different modes of unauthorized access*: The dataset includes images of individuals attempting to gain unauthorized access in different ways, such as climbing over fences, breaking locks, using counterfeit credentials, or attempting to sneak past security personnel.

- *Diversity of individuals*: The dataset includes images of individuals from different genders, ages, and ethnicities, to ensure that the AI model is able to accurately detect unauthorized access attempts regardless of the individual's appearance.

Model

The model to detect unauthorized entry event is in progress and it will be released soon.

Scenario details

Real-time detection and alerts for different kinds unauthorized access which includes but are not limited to:

- When an unauthorized person follows an authorized person through a secure area without proper authorization
- When an individual lingering around restricted areas without proper authorization
- Forceful entry
- Use of counterfeit access credentials
- Unauthorized access attempts during off-hours

Test now with online Web-Cam

To test this model & scenario, you can use the following steps:

- Install the visionai package from PyPI

  ```
  $ pip install visionai
  ```

- Test the scenario from your local web-cam

  ```
  $ visionai scenario test exclusion-detection

  Downloading models for scenario: exclusion-detection
  Model: miss-fire-exting-detection:
  https://workplaceos.blob.core.windows.net/models/yolov5s-people/yolov5s-
  people-0.0.4.zip


  Starting scenario: exclusion-detection..
  ```

- You should be able to see the events generated on your console window with the detections of unauthorized access or forceful entry within the camera field of view.

With RTSP Camera - Pipelines

[TODO]

With Azure Setup

VisionAI app is available at a Azure Market place, one can download and use it by following steps mentioned here

Features

Some potential features of VisionAI for detecting missing fire extinguishers could include:

- *Lightning Fast and Response Time*: Ultra-fast Processing for real-time inference results and feedback (~30 frames per second processing) with customizable telemetry and inference results for your requirements.
- *Scalability and Instant Deployment*: Our pre-trained/custom models can be deployed instantly and are camera independent which means they can be pre-installed with existing cameras on site.
- *Custom Integrations*: Our custom smart dashboards and real-time alert/notification systems can be tailored to fit your specific needs be it simple dashboards or complex ERP integrations.
- *Multiple channels for notifications*: Employee Role-based notifications and alerts through different omni channels like emails, messages, custom alert systems, etc.
- *Pre-Processing and Privacy by design*: Our Pre-processing enhances Image quality before further analysis While maintaining data privacy by blurring out faces and other sensitive information present in a frame.

Training with custom data

The scenario is provided as part of our GPL-v3 package for VisionAI. If you wish to train this with custom datasets, please contact us and we can provide you with the training code. You can do custom training with your own datasets for free, as long as it complies with GPLv3 license (you give back the code to the community). If you are interested in a custom license, please contact us.

Contact Us

- For technical issues, you can open a Github issue here.
- For business inquiries, you can contact us through our website.