

УДК 004.056.53

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ СЪЕМКИ МОНИТОРА МОБИЛЬНЫМ УСТРОЙСТВОМ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВОГО ПОДХОДА

© Бекетова В.А.

e-mail: vera_beketova@mail.ru

Визуальный канал утечки информации остается незащищенным в большинстве организаций. У большей части сотрудников есть телефон с камерой приемлемого разрешения, что позволяет быстро и малозаметно зафиксировать, вероятно, ключевую часть информации в устройстве и использовать полученную информацию в своих целях. Наибольшую актуальность данная угроза имеет для систем, основанных на взаимодействии с потребителем, в частности операторов связи, банков, различных финансовых организаций. Наиболее опасным является не единичный случай несанкционированного доступа к информации, а отсутствие реакции и предотвращения такого инцидента.

Было принято решение в качестве источника изображений использовать камеры наблюдения.

Общая схема работы системы выглядит следующим образом.

1. В систему поступает видеопоток;
2. Происходит получение местоположения рабочих мест на кадре:
 - 1) Кадр передается в нейронную сеть 1 для детектирования положения мониторов, на выходе получаем координаты монитора;
 - 2) Производится статическая разметка рабочих мест.
3. Производится обрезка изображения таким образом, чтобы монитор оказался в середине итогового изображения. Количество изображений на выходе равно количеству обнаруженных/размеченных мониторов.
4. Обрезанные изображения передаются в нейронную сеть 2:
 - 1) Детектируется мобильное устройство, на выходе получаем координаты мобильного устройства на изображении;
 - 2) Происходит классификация изображения.
5. Осуществляется принятие решение на основе полученных данных.

Для проведения экспериментов для классификации были выбраны архитектуры InceptionV3, DanceNet201, InceptionResNetV2. Ключевыми факторами в выборе моделей были количество параметров модели и существующие оценки точности на различных наборах данных.

Был проведен ряд экспериментов и подобраны параметры обучения, позволяющие достичь более высокой точности. На текущий момент наилучшие результаты для этапа классификации показала модель InceptionV3 с точностью 95 %.

Для решения задачи детектирования выбраны следующие модели: CenterNet Resnet101 V1 FPN; CenterNet HourGlass104; EfficientDet D2; EfficientDet D4; YOLO v4. Выбор моделей происходил на основании результатов работы модели, обученной на датасете COCO, а именно – скорость работы и точность. В настоящий момент проводятся эксперименты.

Для ситуации ограниченности вычислительных ресурсов более подходящим является подход с ручной разметкой и последующей классификацией. Необходимое условие в данной ситуации – стационарность камеры.

В случае поворотной камеры, более подходящим будет подход, в котором используется детектирование рабочих мест.

Плюсы разработанной системы: система масштабируема, обладает достаточно высокой точностью, позволяет снизить количество инцидентов и оперативно реагировать на них.

Минусы: необходимость большого количества вычислительных ресурсов.