УДК 004.9

ПРОБЛЕМЫ И УЯЗВИМОСТИ В РАБОТЕ С АЛГОРИТМАМИ КОМПЬЮТЕРНОГО ЗРЕНИЯ

Живаев Л.В.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»
Научный руководитель – преподаватель Кривоносова Н.В.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Компьютерное зрение — это область науки, которая занимается задачами, связанными с анализом изображений и видео. Можно считать, что при этом требуется ответить на вопрос, что изображено на картинке. Несмотря на кажущуюся тривиальность вопроса, ответить на него не так просто.

Как и любые алгоритмы, алгоритмы компьютерного зрения не идеальны и имеют свои уязвимости. Но чаще всего уязвимости открываются тогда, когда правильный алгоритм применяют в неправильной среде. Данные тезисы посвящены обзору уязвимостей в использовании алгоритмов компьютерного зрения.

Общие проблемы определения

1.Плохая выборка тренировки нейросетей

Зачастую набор данных для тренировок нейросетей неравномерен, т.е. в наборе фотографий людей со светлой кожей будет больше, чем людей с темной кожей, что может привести к трагическим ситуациям: например, автомобиль не распознает.

2.Проблемы анализа изображений

Неверная определение по общим элементам (проблема общего фона).

В большинстве случаев в задачах сравнения изображений, после анализа изображения формируется массив опорных точек которые сравниваются с аналогичным массивом у второго обьекта , и если зафиксирован достаточный процент совпадений то изображения признаются эквивалентными. При этом разработчиками должен учитыватся тот факт что большую часть анализируемого изображения может содержать фон, и схожесть фона будет играть большую роль чем схожесть обьектов для сравнения.

Face ID

Существующий на данный момент комплекс процедур по распознаванию лица достаточно надежен при соответствующем применении

В большинстве случаев данная функция используется в качестве биометрической идентификации пользователя смартфона. В этих случаях нужно понимать, что эта система работает по назначению только при соответствующем контроле среды, т.е. когда очевидно, что не используются специальные маски, фотографии владельца и иные способы имитации внешности пользователя. Но при этом нужно учитывать, что это лишь статистическое сравнение показателей внешности. Это означает, что люди с одинаковой внешностью (например, близнецы) способны успешно проходить процедуру идентификации, заменяя друг друга.

QR

QR имеет более сложный алгоритм декодирования и интерпретирования в отличии от например схожих штрихкодов.

Большинство приложений при считывании QR кодов сразу же открывают ссылку в браузере по умолчанию, что дает мошенникам возможность использовать уязвимости браузеров и сетевых протоколов.

Кроме того, на сегодня актуальна проблема безопасности платежей с помощью QR кода.

Существует два способа оплатить покупку с помощью QR-кода:

1) созданный заранее или перед покупкой QR код продавца, при котором главной уязвимостью является возможность поддельного QR-кода;
2) QR-код создает покупатель при помощи платежного приложения, в таком случае так же есть уязвимость: достаточно сфотографировать QR с экрана смартфона и сделать оплату на свой счет до того, как QR код прекратит свое действие.

Хотя популярность QR кодов и побудила производителей встраивать программное обеспечение для их распознавания в новые устройства, программы от сторонних разработчиков все ещё имеют большую популярность. Рассчитывая на невнимательность и спешку пользователя, мошенник может создать программу, требующую дополнительные разрешения для своей работы и фоново выполняющее неизвестные пользователю команды мошенника.