Кооперативная классификация наличия живого присутствия по оптическому потоку

Соколов Артём Константинович

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: s02230515@gse.cs.msu.ru

Научный руководитель *— Конушин Антон Сергеевич*

Алгоритмы распознавания лиц используются для решения широкого спектра практических задач, требующих идентификации личности, например, для оплаты по лицу или контроля на пропускных пунктах. Такие системы идентификации часто подвергаются попыткам взлома со стороны злоумышленников. Уязвимость моделей распознавания лиц заключается в том, что они одинаково трактуют настоящие лица и поддельные, которые могут быть изображены на листе бумаги или дисплее. Из-за этого, если система идентификации не защищена от подобных атак, присутствие любого человека может быть легко сымитировано. Чтобы предотвратить подмену личности при биометрической идентификации, используются алгоритмы классификации наличия живого присутствия, позволяющие определить, является ли лицо на изображении настоящим или нет.

Базовые методы классификации наличия живого присутствия, принимающие на вход только одно изображение, не всегда способны точно распознать атаки на системы идентификации при использовании высококачественных поддельных лиц. Поэтому для повышения точности классификации могут быть использованы алгоритмы, принимающие на вход видео последовательность кадров. Такой подход позволяет модели учитывать не только статическую информацию о текстуре лица и его окружении, но и временную информацию о движении лица. Для дополнительного повышения точности входное видео может быть записано в кооперативном режиме, в котором пользователя просят следовать набору инструкций во время записи видео. Наложение таких ограничений на процесс сбора данных может увеличить общее время идентификации личности, но значительно снижает вероятность успешной атаки на систему.

В данной работе предлагается алгоритм кооперативной классификации наличия живого присутствия по видео последовательности. Входные видео для алгоритма должны быть сняты по определенному сценарию, в котором человек медленно приближает лицо, ориентированное фронтально к камере, между двумя заранее определен-

ными контрольными точками. Детектор оптического потока используется в качестве основной компоненты предварительной обработки видео последовательности. Идея предлагаемого метода заключается в использовании предсказанного оптического потока входного видео, снятого по описанному сценарию, для нейросетевой классификации. Такой подход оказался особенно эффективным, поскольку оптический поток видео, снятого по сценарию с приближающимся лицом, содержит информацию об объеме лица, полезную для предсказания. Кроме того, предсказанный оптический поток передается в нейросетевую модель вместе с оригинальным кадром из видео, чтобы также учитывать информацию о текстуре и окружении лица.

Для оценки качества алгоритма был собран набор данных с видео последовательностями, снятыми по ранее описанному сценарию. При съемке использовались как настоящие лица, так и искусственные различного типа: распечатанные фотографии, фотографии на дисплее, бумажные маски, видео. Результаты экспериментов показали, что предложенный метод имеет более высокую точность классификации на собранном наборе данных по сравнению с выбранными для сравнения методами.

Также было показано, что предложенный алгоритм имеет высокую точность на части набора данных SIW [1], содержащей видео, снятые по описанному сценарию. Подвыборка содержит 1094 видео для обучения и 928 для тестирования. В результате тестирования алгоритмом было допущено 2 ошибки классификации (1 на настоящем лице, 1 на искусственном).

Литература

1. Yaojie L., Amin J., Xiaoming L. Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision // In Proceeding of IEEE Computer Vision and Pattern Recognition (CVPR 2018), Salt Lake City, UT, Jun. 2018.