УДК 004.032.26

ДЕТЕКТИРОВАНИЕ ПОДМЕНЫ ЛИЧНОСТИ НА ВИДЕОЗАПИСЯХ В СОЦИАЛЬНЫХ СЕТЯХ МЕТОДАМИ НЕЙРОННЫХ СЕТЕЙ

Баулин Г.А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Университет ИТМО»)

Научный руководитель – к.т.н., ассистент Попов И. Ю.

(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Университет ИТМО»)

В докладе будет представлена архитектура нейронной сети, позволяющей эффективно выявлять подмену лица на видеозаписях в социальных сетях, с учетом пониженного качества источника вследствие применения постобработки и алгоритмов видеосжатия.

Введение. За последние годы генерирование гиперреалистичных поддельных видео с помощью нейросетей (Deepfake) стала более совершенной. Методы манипуляции, подмены лица в видео получили большое распространение и стали доступными для широких масс. Они позволяют редактировать лица в видеозаписях с реалистичными результатами при минимальных усилиях. Несмотря на полезность этих инструментов во многих областях, довольно часто они используются злоумышленниками для оказания негативного влияния на общество (например, распространение поддельных новостей, обход биометрической идентификации). Одним из наиболее популярных каналов распространения информации являются социальные сети, которые направлены на потребление больших потоков данных — это означает, что конечные пользователи тратят меньше времени на проверку источников, достоверности увиденной инфорации. Следовательно, необходимость объективного определения того, подвергалось ли лицо на видеозаписи каким-либо изменениям, является задачей первостепенной важности.

Детектирование подмены личности в социальных сетях усложняется тем, что видеофайлы подвергаются сжатию и постобработке, что усложняет процесс анализа нейросетями, так как таким образом количество аномалий в данных возрастает. Цель работы – определить необходимую и достаточную структуру нейросети, которая с высокой точностью сможет выявлять поддельные видеозаписи с учетом основных алгоритмов сжатия и наложения постобработки, применяемых социальными сетями.

Основная часть. Выполнение поставленной задачи включает в себя построение архитектуры нейросети с её последующей реализацией для детектирования подмены лица на видеозаписи, а также создание набора данных (датасета), на котором будет проведена оценка эффективности её работы. При тренировке не будут использоваться техники, призванные повысить точность обучения нейросети, так как поставлена задача определить минимально простую архитектуру, которая будет показывать высокую точность работы на тестовых данных.

Выводы. Разработанная архитектура при своей простоте реализации позволяет с достаточно высокой точностью выявлять подмену лица на видеозаписях в социальных сетях, что делает в свою очередь её доступной для внедрения в проекты в короткие сроки и использования в качестве готовые компонента по методу Transfer Learning.

Баулин Г.А. Подпись

Попов И. Ю. Подпись