УДК 004.03

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ПОДМЕНЫ ЛИЦ НА ФОТО И ВИДЕО. СУЩЕСТВУЮЩИЕ МЕТОДЫ И ИХ НЕДОСТАТКИ

Роговой В. (Университет ИТМО),
Научный руководитель: к.т.н., доцент Коржук В.М. (ИТМО), к.т.н., ассистент Попов И.Ю. (Университет ИТМО)

В данной работе была исследована проблема, появившаяся в результате развития технологий машинного обучения, подделки лиц на фото и видео. Поскольку метода выявления манипуляций с цифровым контентом, удовлетворяющего необходимым условиям, не представлено, были рассмотрены существующие методы и их недостатки.

Введение. В последнее время количество фото и видео, изготовленных по технологии deepfake и FaceGAN, возросло в несколько раз. Известны случаи, когда данные материалы были использованы с целью шантажа или компрометации всех категорий граждан. Крупные международные компании, такие как Facebook, Amazon и Google, уже озаботились решением данной проблемы, предлагая вознаграждение за создание метода, который мог бы детектировать подделку фото или видео. Однако существующие методы детектирования, с учетом скорости развития технологии, могут очень быстро устареть и, помимо этого, имеют свои недостатки. В данной работе рассмотрена проблематика этой темы и представлен обзор существующих методов распознавания подделки лиц на фото и видео.

Основная часть. Среди всех существующих на данный момент методов детектирования подделки фото и видео, с использованием технологий машинного обучения, были выделены методы, которые показывают наилучший результат.

Метод анализа частотного спектра обеспечивает точность детектирования вплоть до 99.64%, однако может быть уязвим для постобработки, в результате которой происходит подавление дискретных пиков, появляющихся в результате искусственного увеличения количества образцов для обучения нейросети.

«MESONET» – нейросеть, используемая для детектирования подделки фото и видео, основана на процессе сжатия данных при создании дипфейков. Данный метод уязвим к восстановлению детализации контента.

Метод распознавания последовательности поз основан на ошибках связанных с недообучением или недостатком входных данных, при которых нейросеть не способна распознать направление взгляда человека относительно угла поворота головы, в связи с чем происходит рассогласование изображения.

Однако данный метод потенциально потеряет свою актуальность с увеличением обучающей выборки.

Также, при подмене лиц на видео, возникает проблема с моделированием процесса моргания человека, в связи с чем количество морганий в минуту может упасть с 34, до 4. На этом основан метод детектирования процесса моргания, который подсчитывает количество движений. Однако данный метод также потенциально теряет свою актуальность при увеличении обучающей выборки или при подключении специальных модулей, которые дополнительно будут обрабатывать данный процесс.

Выводы. В результате проделанной работы были рассмотрены существующие методы распознавания подделки фото и видео, изготовленных при помощи различных методов машинного обучения. Рассмотрение слабых сторон данных методов позволяет не только улучшить технологию подделки биометрических данных, но и говорит о том, что исследование методов детектирования дипфейков крайне актуально и востребовано, поскольку существующие методы имеют массу недостатков.

Роговой В. (автор) Подпись

Коржук В.М. (научный руководитель) Подпись

Попов И.Ю. (научный руководитель) Подпись