УДК 519.688

АНОНИМИЗАЦИЯ ЛИЦ НА ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ

Мосяев А.Е. (Национальный исследовательский университет ИТМО), **Деева И.Ю.** (Национальный исследовательский университет ИТМО)
Научный руководитель –к.т.н., доцент каф. ВПВ Калюжная А.В.
(Национальный исследовательский университет ИТМО)

Разработка системы для анонимизации лиц на изображениях с применением генерирующих нейронных сетей. Преобразование изображения не должно сопровождаться изменением семантики, помимо анонимизируемого объекта с высоким качеством изображений после анонимизации.

Основная проблематика, которую затрагивает данный проект – постоянно растущее информационное пространство, с которым ежедневно взаимодействуют миллионы людей. В связи с этим возрастает необходимость контролирования информационных потоков с целью защиты персональных данных.
На данный момент в задачах синтетической генерации графических данных, наилучшим образом зарекомендовали себя, так называемые, генеративно-состязательные сети (ГСС). На их основе существует уже десятки, различной степени утилитарных, архитектур, что позволяет оптимально подобрать подходящие для генерации изображений лиц, с высоким качеством генерируемых данных.

Для использования данной системы в сферах, где необходимо сохранение общего смысла изображения (видео) без привязки к действующему лицу, важным условием является минимизация, а в лучшем случае отсутствие изменения семантики исходного изображения. То есть, по мере возможности, никакие объекты изображения, кроме лица человека, не должны быть изменены в ходе анонимизации. Для выделения лиц на изображении используется предобученная система обнаружения лиц.

Проектируемую систему можно разбить на две подсистемы: система генерирующая контент и система анонимизации. Последняя основана на геометрических свойствах многомерных векторов. На фотографии выделяется лицо человека и происходит преобразование изображения лица в 128-мерный вектор. Данный вектор имеет свое положение среди остальных изображений лиц, на основе которых происходит анонимизация. Используя методы кластеризации данных, в частности метод k-ближайших соседей, можно сформировать новый многомерный вектор для анонимизируемого объекта. Далее на основе полученного векторного представления происходит генерация (анонимизация) посредством генеративно-состязательных сетей. В данной сети основными элементами являются: генератор и дискриминатор. Они, в свою очередь, являются многослойными нейронными сетями, с разными типами выполняемых преобразований.

В рамках своей работы мы сформировали несколько подходов к использованию многомерного векторного представления изображения лица человека, которое необходимо анонимизировать:

1. Передавать вектор на вход генератора в ГСС. То есть генератор будет производить преобразование вектор – изображение.
2. Встраивать векторное представление в один из слоев используемых нейронных сетей. В таком случае генератор будет производить преобразование типа изображение – изображение. Данный вариант является наиболее часто встречающимся, чем упомянутый в пункте 1. Это позволит использовать уже существующие архитектуры ГСС с минимальными изменениями.

В результате мы планируем получить систему производящую преобразование исходного изображения с высоким качеством генерации графического контента. Данная система анонимизации может использоваться: в оперативной деятельности спецслужб, где личность свидетеля необходимо скрыть; в медицинских учреждениях при проведении операций, для скрытия личности пациента; в системах «умного» дома; для генерации синтетических наборов данных.

Мосяев А.Е. /_____/

Деева И.Ю. /_____/

Калюжная А.В. /_____/