Исследование метода подмены лиц в видео при помощи глубокого обучения

А.С. Черномырдина[1]

[1]*Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34а, Самара, Россия, 443086*

Аннотация

В данной работе был изучен ряд научных статей на исследуемую тему, были проведены анализ и структуризация изученной информации. Были изучены имеющиеся реализации данной технологии и проведен сравнительный анализ. В результате работы была написана данная обзорная статья, сочетающая в себе структурированную информацию из разных источников, как российских, так и зарубежных. Так же был разработан программный модуль, показывающий свою эффективность в процессе работы. Этот модуль далее будет использован в дальнейших этапах разработки программы. Эффективность данной работы заключается в изучении и обобщение большого количества зарубежного материала, т.к. в российской науке данная тема пока мало изучена и существует лишь небольшое количество соответствующего теме научного материала.

Ключевые слова

Подмена лиц, DeepFake, глубокое обучение

1. Введение

Технология DeepFake[1] (конкатенация слов «глубинное обучение» (англ. Deeplearning) и «подделка» (англ. Fake)) – методика создания видеоконтента, которая подразумевает замену лица человека на исходном видеоматериале при помощи алгоритмов глубокого обучения. Алгоритмы, заложенные в основу этой технологии, позволяют легко создавать реалистичные видеоролики, в которых практически невозможно распознать подделку невооруженным глазом.

2. Этапы создания поддельных видео

Процесс создания поддельных видео включает в себя три основных шага:

1. Извлечение: порезать видео на кадры, найти лица в каждом кадре, вывести хорошо выровненные и тщательно обрезанные изображения каждого лица.
2. Обучение: использовать полученные изображения для обучения генеративно-состязательной нейросети, состоящей из генератора-автоэнкодера и дискриминатора.
3. Конвертирование: применить модель, обученную на предыдущем шаге, на кадрах из целевого видео, смешивание лиц в соответствии с маской, для идеального наложение, применение цветокоррекции, чтобы выдать дипфейк. После обучения модели её можно будет применять к любому видео, на котором присутствуют те люди, на лицах которых она обучалась.

3. Принцип работы метода подмены лиц

Понимание метода подмены лиц на изображениях заключается в необходимости использования двух наборов энкодеров-декодеров с общими весами. Когда мы хотим заменить одно лицо на другое мы пропускаем его через энкодер и декодируем его, используя декодер другой сети. Также следует отметить, что невозможно обучение обоих автоэнкодеров по отдельности, ведь в таком случае они будут несовместимы друг с другом.

После тренировки автоэнкодеров, скрытые представления лица, сгенерированного из исходного объекта, можно передавать в сеть декодеров, обученную на лицах объекта, который мы хотим вставить вместо исходного на видеопоследовательности. Декодер, обученный восстанавливать изображение целевого лица, попытается восстановить его из информации, содержащейся в скрытом представлении, сгенерированном энкодером исходного лица, полученной из кадров видеопоследовательности.

Для улучшения качества получаемых результатов автоэнкодер включается в генеративную сеть (GAN) в качестве генератора. Таким образом сеть из автоэнкодера и дискриминатора будет состязаться в состязательных отношениях. Автоэнкодер будет заменять лица, а дискриминатор будет пытаться отловить подделку. Это будет заставлять автоэнкодер создавать более реалистичные изображения, хорошо имитирующие реальность. Этот процесс затруднит борьбу с поддельными видео, так как система генерации лиц будет постоянно развиваться.

4. Анализ реализаций технологии

Таблица 1
Результаты работы различных реализаций алгоритмов подмены лиц в видеопоследовательности

Target	Source	DeepFaceLab	FaceSwap	Nirkin et al
[1]	[2]	[3]	[4]	[5]
				
				

5. Заключение

В результате работы, был проведен анализ каждой составляющей конвейера разработки DeepFake. Для каждого этапа была собрана информация о различных имеющихся реализациях и подходов решения необходимой задачи. Поиск и обзор литературы показал, что несмотря на практически повсеместное распространение технологии подмены лиц крайне существует крайне мало русскоязычных источников. Исходя из этого, можно сделать вывод, что данная тематика не получила достаточного развития в отечественной науке.

6. Литература

[1] Zucconi, A. Understanding the Technology Behind DeepFakes //Understanding Deepfakes. – 2019. – Vol. 6.
[2] Naruniec, J. High-Resolution Neural Face Swapping for Visual Effects // Computer Graphics Forum. – 2020. – Vol. 39(4). – P. 173-184.
[3] Petrov, I. DeepFaceLab: A simple, flexible and extensible face swapping framework // ArXiv preprint: 2005.05535. – 2020.
[4] Deepfakes [Electronic resource]. – Access mode: https://github.com/deepfakes/faceswap.
[5] Nirkin, Y. On face segmentation, face swapping, and face perception / Y. Nirkin, I. Masi, A.T. Tran, T. Hassner, G. Medioni // IEEE Conference on Automatic Face and Gesture Recognition, 2018.