УДК 004.056.53

ИССЛЕДОВАНИЕ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ КЛАССА GAN

Афендин К.З. (федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»)

Научный руководитель – к.т.н, доцент ФБИТ, Волошина Н.В.

(федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»)

В работе приведены современные методы биометрической аутентификации, а также актуальные угрозы для существующих систем из-за развития нейронных сетей, в частности, генеративно-состязательных сетей (GAN).

Введение. Алгоритмы глубокого машинного обучения за последние годы принесли огромное развитие и успех во многих приложениях. Данное направление развивалось очень активно и нашло применение во многих традиционных для этого областях. При развитии были предложены различные методы, основанные на различных способах обучения, в частности, обучение с учителем, полу-контролируемое обучение, а также неконтролируемое обучение. Результаты экспериментов имеют современный уровень производительности в сравнении с традиционными подходами к машинному обучению в различных областях, например, компьютерное зрение, распознавание речи, робототехника, управление, обработка естественного языка, кибербезопасность, обработка изображений. За всё время были разработаны разные подходы к построению нейронных сетей, начиная с глубоких нейронных сетей (DNN) и продолжая сверточными нейронными сетями (CNN), рекуррентными нейронными сетями (RNN), сетями долгой краткосрочной памяти (LSTM), управляемыми рекуррентными блоками (GRU), автоэнкодерами (AE), сетями глубокого доверия (DBN), глубоким обучением с подкреплением (DRL), а также генеративно-состязательными сетями (GAN).

В последнее время генеративные модели на основе глубокого обучения, такие как автоэнкодеры и генеративно-состязательные сети, широко применяются для создания фотореалистичных частей или же полных изображений или видео. Более того, недавние модификации GAN, такие как PGGAN и BigGAN использовались для синтеза фотореалистичных изображений и видео высокого разрешения, которые человек не может отличить от настоящих за ограниченное время. Поэтому с появлением такого рода технологий возникла острая необходимость в эффективном методе обнаружения поддельного контента.

Основная часть. Описание современных методов биометрической аутентификации с использованием нейронных сетей и существующих угроз безопасности с появлением GAN. Приведен анализ существующих методов распознавания поддельного контента.

Выводы. На основе проведённого разбора доступных методов сформированы актуальные направления развития защиты систем биометрической аутентификации.

Афендин К.З. (автор) Подпись

Волошина Н.В. (научный руководитель) Подпись