РОЗПІЗНАВАННЯ DEEPFAKE ЗОБРАЖЕНЬ НА МОБІЛЬНИХ ПРИСТРОЯХ

Долганенко О.Д., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна

Із появою технології ефективної заміни обличчя на фото відео (deepfake), функціонал біометричної автентифікації та підтвердження особистості користувача стає під загрозою [1], особливо в додатках державного та фінансового призначення. Створення швидкого, надійного та захищеного автоматизованого рішення розпізнавання deepfake на мобільному пристрої є актуальною проблемою, яка потребує ретельного дослідження.

Метою доповіді є аналіз предметної області створення та розпізнавання на мобільному пристрої зображень та відео, над якими було здійснено маніпуляцію deepfake. У доповіді наводяться методи створення deepfake: здебільшого це досягається за допомогою глибоких нейронних мереж у поєднанні з методами заміни обличчя та Generative Adversarial Networks (GAN). Також, перераховуються та аналізуються методи розпізнавання deepfake зображень, до яких належать: методи що базуються на статистичних вимірюваннях, методи машинного навчання та глибокого навчання [2]. У результаті порівняння та аналізу існуючих досліджень виявлено оптимальний метод для вирішення цієї задачі – метод глибокого навчання. Наводяться методи створення моделі та аналізуються доступні набори даних, таких як FaceForensics, DFD, Celeb-A та інші.

У доповіді наводяться методи застосування моделей глибокого навчання на мобільних пристроях. Піднімається питання оптимізації моделі шляхом її зменшення, що досягається операцією трасування. Розглядається статистика порівняння точності моделі до та після застосування трасування. Також порівнюються технології PyTorch Mobile та TensorFlow Lite для взаємодії із моделлю на мобільному пристрої. У висновку зазначаються результати дослідження, що включають обрані технології та підходи до розпізнавання deepfake зображень на мобільному пристрої, їх переваги, недоліки та обмеження.

Список літератури

1. Zainab Zahid, Ammar Haider, Nosheen Sabahat, Asim Tanwir . Vulnerabilities in Biometric Authentication of Smartphones. *2020 IEEE 23rd International Multitopic Conference (INMIC)*. 2020. DOI: https://doi.org/10.1109/inmic50486.2020.9318094

2. Hady A. Khalil;Shady A. Maged; (2021). Deepfakes Creation and Detection Using Deep Learning. *International Mobile, Intelligent, and Ubiquitous Computing Conference.* 2021. DOI: https://doi.org/10.1109/MIUCC52538.2021.9447642