УДК 004.093

ПРО ПРОЦЕСИ КОМП'ЮТЕРНОЇ ФАЛЬСИФІКАЦІЇ І ГЕНЕРАЦІЇ МЕДІА КОНТЕНТУ

Білоцерківська В.А.
Науковий керівник – к.т.н., асист. Кобилін І.О.
Харківський національний університет радіоелектроніки, каф. ІНФ,
м. Харків, Україна
e-mail: viktoriia.bilotserkivska@nure.ua

This work explores the ethical considerations surrounding the use of face-swapping technology in photography. It highlights the importance of photographers taking steps to protect the privacy of their clients, such as by replacing faces in photographs that are published publicly. Additionally, the work stresses the need for responsible application of the technology, ensuring that the altered images maintain the original artistic expression and integrity of the photographs. The work also discusses the potential benefits of face-swapping technology, such as its ability to protect personal data and preserve the quality and artistic expression of photographs.

Проблема фальсифікації в інформаційному просторі являє собою важливий виклик для суспільства бізнесу та політики. За останні роки швидкі та легкодоступні технології, такі як штучний інтелект, глибоке навчання та інші інновації в області обробки зображень, дозволяють створювати реалістичні фальшиві медіа, які важко відрізнити від реальних.

Фальсифіковані фотографії, відео, аудіозаписи та інші медіа можуть бути використані для розповсюдження дезінформації, маніпулювання громадською думкою, а також для шахрайства та інших злочинних дій.

Незважаючи на те, що фальсифікація медіа та зловживання штучно створеними медіа викликають серйозні занепокоєння і можуть вести до величезних проблем у суспільстві, важливо визнати, що ті самі технології можуть бути використані і для добрих цілей [1].

Важливо розуміти, що ці технології також мають потенціал для розв'язання суспільних проблем, покращення якості життя людей.

Однією з таких технологій є технологія підміни обличчя (рис. 1).

Така обробка створена за допомогою бібліотеки InsightFace. Бібліотека InsightFace використовує технологію глибокого навчання для заміни обличь. Ця технологія включає в себе застосування нейронних мереж і алгоритмів машинного навчання для аналізу і трансформації обличь людей на зображеннях. Це дозволяє виконувати операції, такі як розпізнавання обличь, зміна атрибутів обличь (таких як вирази обличчя, зачіски, вік тощо) та інші форми маніпуляцій з обличчями на зображеннях [2]. Саме ця технологія дозволяє замінити обличчя з іншої фотокартки, як наприклад в нашому випадку взято обличчя актриси Енн Хетеуей (рис. 2).

Рисунок 1 – Оригінальне фото та змінене фото

Рисунок 2 – Фото актриси Енн Хетеуей

Однією з ключових формул, яку можна використовувати для опису роботи нейромережі в бібліотеці InsightFace, є формула обчислення косинусної схожості між двома векторами вкладень:

$$cos\_sim(f(x_1), f(x_2)) = \frac{f(x_1) \cdot f(x_2)}{\|f(x_1)\|_2 \cdot \|f(x_2)\|_2},$$

де x_1 – перше зображення обличчя; x_2 – друге зображення обличчя; $f(x_1)$ – вектор вкладень, отриманний для першого зображення; $f(x_2)$ – вектор вкладень, отриманний для другого зображення.

Ця формула дозволяє вимірювати схожість між обличчями на основі їх векторів вкладень, де більше значення вказує на більшу схожість. Функція втрат ArcFace виглядає наступним чином:

$$L = -\frac{1}{N}\sum_{i=1}^{N}\log\frac{e^{s(\cos(m\cdot\theta_{y_i,i})-m)}}{e^{s(\cos(m\cdot\theta_{y_i,i})-m)}+\sum\limits_{\substack{j=1,\\ j\neq y_i}}^{n} e^{s\cdot\cos(\theta_{j,i})}},$$

де N – кількість прикладів у поточному міні-пакеті; s – параметр масштабування (scaling parameter); m – гіперпараметр, зазвичай називається "margin", який регулює розмір межі між класами; $\theta_{j,i}$ – кут між векторами вкладень (embeddings) зображень i та j; y_i – справжній клас для зображення i.

Після проведення обробки програмою, на сфальсифікованому фото у дівчини буде обличчя Енн. Так як фотографи часто стикаються з ситуаціями, коли клієнти не бажають, щоб їхні обличчя були видимими на фотографіях, що публікуються відкрито, фотографи мають подбати про безпеку своїх клієнтів в інформаційному просторі. А шляхом заміни обличчя на фотографії можна забезпечити захист особистих даних клієнтів, зберігши при цьому якість та художній вираз фотографій.

Коли ви в наступний раз будете завантажувати дані чи документи, давати використовувати ваші фото, будь-яку персональну інформацію, фінанси – друзям, колегам чи не перевіреним джерелам, пам'ятайте, ваші дані в інтернеті завжди можуть мати деяку цінність для тих чи інших структур, через що потрібно використовувати збалансовану стратегію розвитку та використання технологій обробки та фальсифікації медіа даних, яка б враховувала як їхні потенційно можливі ризики та загрози, так і користь яку вони можуть принести.

Список використаних джерел:

1. Bodyanskiy, Y., Vynokurova, O., Kobylin, I., & Kobylin, O. (2016). Adaptive fuzzy clustering of short time series with unevenly distributed observations in Data Stream Mining tasks. Information Technology and Management Science, 19(1), 23–28.

2. Bodyanskiy, Y., Kobylin, I., Rashkevych, Y., Vynokurova, O., & Peleshko, D. (2018, February). Hybrid fuzzy-clustering algorithm of unevenly and asynchronously spaced time series in computer engineering. In 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) (pp. 930–935). IEEE