

СТВОРЕННЯ ПІДРОБНИХ ЗОБРАЖЕНЬ ЛЮДСЬКОГО ОБЛИЧЧЯ ЗА ДОПОМОГОЮ АЛГОРИТМІВ ГЕНЕРАТИВНИХ КОНКУРУЮЧИХ МЕРЕЖ

Г. О. Цикало^{1, а}

¹Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Фізико-технічний інститут

Анотація

Стаття присвячена створенню нового методу забезпечення анонімності при реєстрації в мережі інтернет за допомогою генеративних моделей, а саме – генеративні конкуруючі нейромережі. На основі StyleGAN, генератора зображень було протестовано його здатність до створення зображень людських облич. Результати експерименту дозволили стверджувати можливість підміни фотографії реального обличчя підробкою, яка не ідентифікується людським оком.

Ключові слова: людське обличчя, StyleGAN, алгоритм генеративних конкуруючих мереж, зображення

Вступ

З кожним роком збільшується кількість електронних пристроїв серед населення, а також покращується якість з'єднання в мережі інтернет. Все більша кількість людей користується різноманітними додатками й сайтами, але багато з них вимагають реєстрації. Процес реєстрації по достовірним даним не є складністю, але часом ми хочемо забезпечити свою анонімність в межах додатку. Як же вирішити цю проблему? Для ідентифікації по електронній пошті чи телефонному номеру ми використовуємо їх тимчасовий аналог, що ж робити якщо нам стало необхідне зображення людського обличчя, в цій статті ми спробуємо відповісти на дане запитання.

1. Огляд алгоритму генеративних конкуруючих мереж

Перспективи глибокого навчання полягають в застосування алгоритмів і здатності електронно – обчислювальних машин навчатись на минулих ітераціях робочого циклу для отримання досвіду, так як ми використовуємо оброблені ітерації то для нас не ймовірно важливо збільшення об'єму оброблюваних даних, також із збільшенням якості апаратних й програмних рішень відбуваються стрибки складності задач, які науковці здатні вирішити.

Принципальною новинкою для глибокого навчання стала праця Ian'a Goodfellow'a та інших людей з дослідницького університету Монреаля, вони в 2014 році представили свою ідею використання методології змагання двох нейронних мереж [1]. Неодмінною перевагою в цьому випадку є можливість мережі наслідування різних варіантів розподілення нашого data set. Характерною особливістю GAN (Generative adversarial networks) архітектури є наявність двох

нейронних мереж, налаштованих таким чином, щоб конкурувати в ефективності одна залежно від іншої. Для прикладу розглянемо ситуацію, створення нового продукту й процес запровадження його до продажу в магазини. Дана модель буде складатись з двох частин виробника продукту й контролюючого органу, який буде оцінювати якість продукту. Зрозуміло, що на початку діяльності виробник, створює продукцію, не здатну до конкуренції на ринку й контроль якості не пропускає продукт до участі у продажу. З іншого боку, пройшовши певний набір ітерацій – невдалих спроб створення продукції, виробник зробить продукцію здатну пройти контроль якості. Досягнувши бажаного результату, виробник не зупиняється й продовжує удосконалювати свою продукцію, але ринок товарів й послуг не стоїть на місці, тож змінюються й умови критерію якості. Ось така взаємодія: покращення продукту й зміна критерію якості і є головною ідеєю, яка лежить в основі Generative adversarial networks. Ми маємо ідею описану словами й поняттями, наступним кроком перетворимо нашу ідею в математичну модель. Далі закріпимо за нашим виробником продукту, який проходить критерій якості, назву generator(G), в свою чергу контролюючому органу присвоїмо назву discriminator(D), ми маємо якусь кількість інших товарів, які вже знаходяться на ринку й проходять контроль якості стабільно, позначимо її за X , контролюючий орган буде робити свій висновок ставлячи число в межах від 0 до 1, це число – відображає впевненість контролюючого органу, в якості продукту, котрий проходить перевірку. Оскільки наш виробник продукту, символізує нейронну мережу, йому необхідна певна кількість вхідних даних, які він буде трансформувати у готовий продукт, нехай це певний набір ресурсів Y – (їх змістовність у даному випадку не є важливою). Зрозуміло що задача, яка стоїть перед виробником, максимізація виразу $D(G(y))$, зробити так щоб ма-

^аrealsydak@gmail.com

ксимальна кількість продуктів, пройшла контроль якості. В той же самий час, перед контролюючим органом стоїть задача не тільки оцінки якості, але й ідентифікація неякісної продукції. Його ціль ставити 0 неякісній продукції й число максимально близьке до 1 високоякісній продукції, здатній до конкуренції. Тож це буде задача максимізації даного виразу $D(x)(1 - D(y))$. Працювати з множенням не зручно тож, даний вираз ми спокійно перетворюємо в суму шляхом логарифмування.

Тож дана задача перетворюється в задачу максимізації по ролям:

- Для виробника

$$\log(D(D(y)))$$

- Для органу контролю [2]

$$\log(D(x) + \log(1 - D(y)))$$

2. Особливості роботи StyleGAN

Для формування зображення обличчя, ми користувались неймережами від NVIDIA а точніше StyleGAN, адже в мережі існує натренована архітектура, яка знаходиться на GitHub та в онлайні. На сьогоднішній день не існує повністю прозорої теорії, яка б досконало пояснила нам механізм навчання, проте в новій методології від NVIDIA науковці пропонують підхід використання прихованого вхідного кодування в тимчасове приховане представлення. Якщо ж говорити про це простими аналогіями, то ми ділимо фактори з яких складається обличчя на дві групи:

- Фундаментальні (до них відносять орієнтація в просторі об'єктів, генетичні особливості)
- Псевдовипадкові (довжина волосся, форма зачіски, родимки й т.д.)

Так як неймережа генератор здатний змінювати атрибути зображення частково, це дозволяє нам створювати нові зображення обличчя, не затрачуючи багато ресурсів.

3. Аналіз результатів роботи алгоритму

Для тесту спроможності генерації було використано два датасети FFHQ, CelebA – HQ, які містять набір зображень людських облич. Також були проведені тести для замірів ефективності StyleGAN в порівнянні з іншими класичними GAN архітектурами по класичним метрикам, такі як роздільність, Frechet Inception Distance(FID), Perceptual path – для кожної метрики мінімальне значення найкраще (табл. 1,2).

Висновки

У цій статті було розглянуто метод генерування зображень на основі генеративних конкуруючих мереж. Він був протестований на двох датасетах CelebA – HQ та FFHQ класичних для задач генерації зображень обличчя. Запропонований метод ефективно справляється із поставленою задачею (рис. 1). Також був проведений аналіз, для розрахунку ефективності даної архітектури при генерації зображень в

Табл. 1. Порівняння ефективності [3]

Method	Separability	Pl(full)	Pl(end)	FID
B Traditional	10.78	412.0	415.3	5.25
0 Z				
Traditional 8	170.29	896.2	902.0	4.87
Z				
Traditional 8	6.52	324.5	212.2	4.87
W				
Style-based 0	9.88	283.5	285.5	5.06
Z				
Style-based 1	6.81	219.9	209.4	4.60
W				
Style-based 2	6.25	217.8	199.9	4.43
W				
F Style-based	3.79	234.0	195.9	4.40
8 W				

Табл. 2. Порівняння ефективності [3]

Method	Separability	Pl(full)	Pl(end)
B			
Traditional	10.78	412.0	415.3
generator Z			
D			
Style-based	3.61	446.2	376.6
generator W			
E +Add			
noise inputs	3.54	200.5	160.6
W			
+Mixing 0.5	3.51	231.5	182.1
W			
F +Mixing	3.79	234.0	195.9
0.9 W			



Рис. 1. Створені обличчя

порівнянні з класичною, він показав переваги даного метода за класичними метриками.

Перелік використаних джерел

1. Generative Adversarial Networks Ian J. Goodfellow, Jean Pouget – Abadie, Mehdi Mirza, Bing Xu, David Warde – Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio
2. Разбираемся с войной нейронных сетей (GAN) <https://habr.com/ru/post/278425/>
3. StyleGAN для генерации новых лиц опубликована в открытом доступе <https://neurohive.io/ru/papers/stylegan-open-source/>