УДК 316.4

Т. О. Савчук
В. В. Філіпов

НЕЙРОПІДХІД ДО АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНТЕРАКТИВНИХ ДОДАТКІВ

Вінницький національний технічний університет

Анотація

Запропоновано підхід до автентифікації користувачів інтерактивних додатків, що базується на використанні фронтальної камери смартфона або іншого пристрою, та нейромережевих засобів розпізнавання облич. Це забезпечить підвищений захист даних за рахунок використання біометрії користувача при необмеженому рості точності розпізнавання обличчя користувача за рахунок використання багатошарових згорткових нейронних мереж. Розбиття зображення на різноформатні фрейми з однотипними ознаками забезпечить зниження часу розпізнавання та навантаження на центральний та графічний процесори пристрою.

Ключові слова: біометрична ідентифікація, нейромережеві засоби, згорткова нейронна мережа, розпізнавання облич, фрейми, інтерактивні додатки.

Abstract

The approach to authenticating users of interactive applications based on the use of the front camera of a smartphone or other device and neural network face recognition devices is proposed. This will provide enhanced data protection through the use of user biometrics with unlimited increase in the accuracy of the user's face recognition due to the use of multilayer convolutional neural networks. Splitting an image into a variety of frames of the same type will reduce the recognition time and load on the central and graphic processors of the device.

Keywords: biometric identification, neural network resources, convolutional neural network, facial recognition, frames, interactive applications.

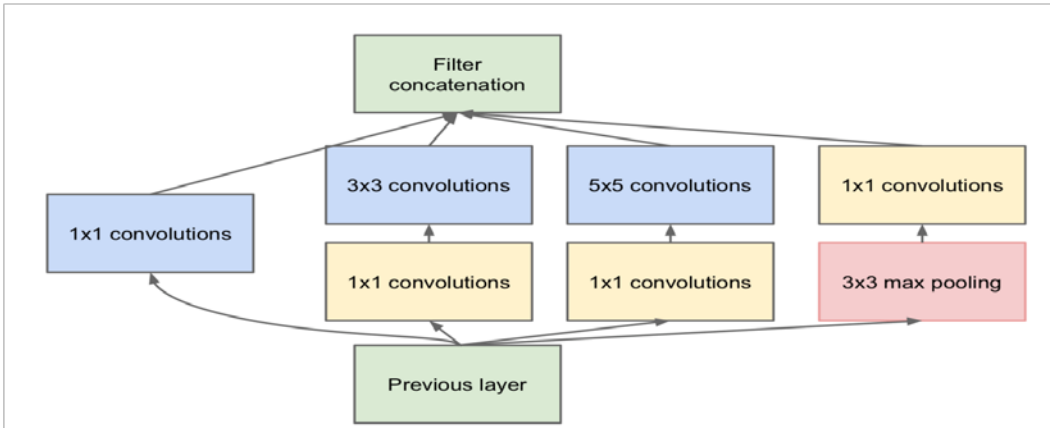
Двадцять перше століття ознаменувало небачений донині ріст інформаційних технологій і багатокористувацьких сервісів, що базуються на них. Більшість нашого часу ми проводимо в різних додатках, що використовують наші персональні дані, які не можна розголошувати. Тому для забезпечення конфіденційності ми використовуємо величезні паролі, які не завжди можна запам’ятати, а тому потрібно записувати чи зберігати в якийсь інший спосіб, що є небезпечно, адже підвищує ризик інформаційної небезпеки.

В сучасних операційних системах є можливість на апаратному рівні використовувати фронтальні камери, які направлені на користувача, що не залежить від апаратних та програмних особливостей конкретного пристрою – будь-який смартфон має фронтальну камеру. Для автентифікації користувачів замість введення паролів повсякчас доцільніше використовувати фронтальну камеру мобільного пристрою та нейронні мережі. Дана функція відсутня в нативному, базовому, виконанні в сучасних операційних системах. Виключенням є лише iOS від 11 версії [1], але лише для пристроїв, де доступний набір точкових проекторів та сканерів Face ID [2]. Даний спосіб має потенціал та можливість стати кросплатформною реалізацією біометричного захисту даних користувачів.

Для розпізнавання облич користувачів доцільно використовувати багатошарові згорткові нейронні мережі [3], що забезпечують високий рівень розпізнавання об’єктів, у тому числі облич людей. Серед ключових особливостей даного підходу можна відзначити використання порівняно малої кількості попередньої обробки зображення, в порівнянні з іншими алгоритмами класифікації зображень. Це означає навчання мережі за допомогою фільтрів, що в традиційних алгоритмах розробляються вручну. Така незалежність у конструюванні ознак від апріорних знань та людських зусиль є великою перевагою. Точність даного підходу доказав в своїх дослідженнях підрозділ DeepDream компанії Google, який довів можливість зниження похибки розпізнавання об’єкту до 0.06656 [4]. Подальше використання даного типу нейронних мереж дає необмежену можливість для росту точності

розпізнавання, адже з кожним наступним запуском механізму розпізнавання мережа буде вичленювати ключові особливості обличчя користувача та спрацьовуватиме швидше.

Архітектура нейронної мережі для біометричної автентифікації користувачів побудована на різнорозмірних фільтрах зображень з розміром фрейму в 1×1, 3×3, 5×5 пікселів. Дана диференціація розмірів фільтрів обрана для підвищення ефективності розпізнавання користувача, адже забезпечить необхідну точність (рівень похибки складає не вище 0.08, в залежності від якості зображення). Паралельно з підвищенням точності, за рахунок диференціації сусідніх пікселів у групи, підвищена швидкість розпізнавання та навантаження на розрахункові потужності засобу. У вхідних шарах зкорельовані одиниці будуть концентруватися в локальних регіонах пам'яті. Це означає, що ми матимемо багато кластерів, зосереджених в одній області зображення, і вони можуть бути покриті шаром звивин 1×1 в наступному нейронному шарі. Запропонована архітектура являє собою комбінацію всіх цих шарів з їх вихідними наборами фільтрів, об'єднаних в один вихідний вектор, що подається на вхід нової ітерації нейронного фільтру[4]. Схема архітектурного рішення блоку



розпізнавання наведено на рисунку 1

Рисунок 1 – Архітектура блоку розпізнавання

Отже, запропонований підхід до автентифікації користувачів інтерактивних додатків забезпечить підвищений захист даних за рахунок використання біометрії користувача. Доцільним є використання багатошарових згорткових нейронних мереж для цієї задачі, через необмежений ріст точності розпізнавання обличчя користувача. Розбиття зображення на різноформатні фрейми з однотипними ознаками забезпечить зниження часу розпізнавання та навантаження на центральний та графічний процесори пристрою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.First Beta of iOS 11 Now Available for Developers [Електронний ресурс] – Режим доступу: https://www.macrumors.com/2017/06/05/first-beta-of-ios-11-now-available/

2.LocalAuthentication [Електронний ресурс] – Режим доступу: https://developer.apple.com/documentation/localauthentication

3.Convolutional Neural Networks (CNNs / ConvNets) [Електронний ресурс] – Режим доступу: https://cs231n.github.io/convolutional-networks/

4.Going Deeper with Convolutions [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/1409.4842

Савчук Тамара Олександрівна — PhD, професор кафедри комп'ютерних наук Вінницький національний технічний університет, м. Вінниця.

Філіпов Владислав Вікторович — студент групи 1кн-18м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Savchuk Tamara Oleksandrivna. — PhD, Professor of the Computer Sciences Chair, Vinnytsia National Technical University, Vinnytsia.

Filipov Vladislav — student of group 1cs-18m, Faculty of Information Technology and Computer Engineering.