Улічев Олександр Сергійович, кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.

Oleksandr Ulichev, candidate of technical sciences, senior lecturer of the department of cyber security and software of the Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.
E-mail: askin79@gmail.com.
Orcid ID: 0000-0003-3736-9613.

Яровий Роман Олександрович, кандидат технічних наук, доцент кафедри КНПІ, декан ФІСТ, Європейський університет, Київ, Україна.

Roman Yarovy, candidate of technical sciences, associate professor of the Department of National Institute of Scientific Research, dean of FIST, European University, Kyiv, Ukraine.
E-mail: roman.yaroviy@e-u.edu.ua.
Orcid ID: 0000-0001-8978-8137.

Задорожний Костянтин Олександрович, студент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.

Kostyantyn Zadorozhny, student of the Department of Cyber Security and Software at the Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.
E-mail: kostazadoroznij9@gmail.com.
Orcid ID: 0000-0002-5278-9627.

DOI: 10.18372/2410-7840.26.18831
УДК 004.932.2

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ КОНКАТЕНОВАНИХ ВЕКТОРІВ ВИЗНАЧЕННЯ ОСОБИ

Денис Ханін, Віктор Отенко

У епоху цифрової автентифікації системи верифікації особи за обличчям стали ключовим елементом безпеки у різних застосуваннях. Це дослідження розглядає синергію ефективності конкатенованих векторів для покращення точності біометричної автентифікації. З використанням набору даних «Celebrities in Frontal-Profile dataset» (CFP) ми досліджуємо, чи може злиття векторів, згенерованих такими моделями, як VGG-Face, Facenet, OpenFace, ArcFace та SFace, призвести до більш надійного процесу автентифікації. Методика включає обчислення відстані L2 між нормалізованими конкатенованими векторами вхідного образу обличчя та якоря, тим самим визначаючи справжність особи. Експерименти розроблені для порівняння ефективності векторів окремих моделей проти конкатенованих векторів, використовуючи такі метрики, як точність, рівень помилкових допусків (FAR) та рівень помилкових відмов (FRR). Висновки цього дослідження можуть істотно сприяти розвитку більш безпечних і надійних систем верифікації особи за допомогою використання декількох існуючих моделей без необхідності нових досліджень архітектур, їхнього проектування та навчання.

***Ключові слова**: верифікація обличчя, біометрична автентифікація, нейронні мережі, конкатеновані вектори.*

ВСТУП

У сучасному цифровому ландшафті системи верифікації обличчя [1] стали ключовими у забезпеченні безпеки та автентичності індивідуальних ідентичностей у різних застосуваннях, від безпеки мобільних пристроїв до контролю доступу в чутливих середовищах. Впровадження технології розпізнавання облич стимульоване її нетравматичністю та унікальними, важко-імітуваними характеристиками людського обличчя, що позиціонує її як лідера серед методів біометричної автентифікації.

Це дослідження розглядає потенціал покращення точності верифікації обличчя за допомогою конкатенованих векторів з декількох моделей нейронних мереж [2]. Використовуючи набір даних CFP [3], ми прагнемо визначити, чи може інтеграція векторів різних моделей створити більш надійну та безпечну систему біометричної автентифікації. Досліджуючи синергію ефективності цих конкатенованих векторів у порівнянні з векторами окремих моделей, це дослідження прагне сприяти розробці більш передових і надійних технік верифікації обличчя з використанням існуючого набору моделей для верифікації обличчя.

Еволюція технологій біометричної автентифікації значною мірою зумовлена прогресом у галузі машинного навчання та глибокого навчання [4], зокрема у сфері розпізнавання облич. Моделі нейронних мереж, такі як VGG-Face, Facenet, OpenFace, ArcFace та SFace, становлять передові напрямки досліджень та розробок у цій галузі. Ці моделі призначені для витягування та аналізу рис обличчя [5] із зображень, перетворюючи їх у числові представлення, відомі як вектори. Ці векто-

ри захоплюють унікальні аспекти структури обличчя людини, дозволяючи системам виконувати завдання верифікації з високим ступенем точності. Успіх цих моделей залежить від їхньої здатності вчитися складним візерункам та варіаціям рис обличчя в різноманітних наборах даних, у різних умовах освітлення, пози та виразів обличчя.

У технології верифікації обличчя використання лише однієї моделі нейронної мережі має певні обмеження. Різні моделі мають перевагу у різних аспектах, таких як точність, швидкість обробки, а також їхня здатність адаптуватися до змін в освітленні чи рисах обличчя [6]. Прагнення до кращої ефективності та надійності цих систем часто вимагає великих і різноманітних наборів даних для навчання, що може коштувати багато ресурсів. Крім того, існує постійна потреба розробляти та тестувати нові архітектури моделей, які могли б ефективно перетворювати зображення облич в корисні числові дані, відомі як вектори. Такий сценарій створює гіпотезу, що комбінація кількох моделей нейронних мереж може запропонувати більш ефективне рішення. Використовуючи унікальні переваги кількох моделей, такий підхід може потенційно подолати загальні виклики у верифікації обличчя. Це закладає основу для дослідження того, як інтеграція результатів різних моделей може призвести до покращення ефективності системи.

Гіпотеза, яка лежить в основі цього дослідження, виникає з критичного виклику в сфері систем верифікації облич: обмеження використання архітектур на основі однієї моделі для досягнення постійно високої точності в різноманітних умовах [7]. Це підкреслює необхідність дослідження альтернативних стратегій, які могли б використовувати сильні сторони існуючих технологій без необхідності постійного перенавчання моделей, оновлення наборів даних чи розробки нових архітектур.

Сучасні системи верифікації облич часто покладаються на одну нейронну мережу, яка може ефективно працювати в певних умовах, але не в інших. Така залежність становить значну проблему, оскільки вимагає постійних оновлень моделі та її базового набору даних для вирішення нових викликів та підтримки ефективності системи. Такий ітераційний цикл розробки є ресурсомістким, вимагаючи значних інвестицій в збір даних, їх обробку та обчислювальну потужність. Крім того, створення нових архітектур моделей для покращення вилучення ознак та точності класифікації додатково ускладнює процес, роблячи його непридатним у довгостроковій перспективі. Гіпотеза, представлена в цьому дослідженні, виникає з цих викликів, пропонуючи використання конкатенованих векторів [8] з декількох моделей як засіб обходу обмежень залежності від однієї моделі. Цей підхід має на меті дослідити, чи може інтеграція різноманітних можливостей встановлених моделей запропонувати більш надійне та точне рішення для верифікації облич, таким чином вирішуючи основні проблеми, пов'язані з поточними методологіями.

ПОСТАНОВКА ЗАВДАННЯ

Це дослідження зосереджене на ключових цілях, які мають на меті дослідити можливі покращення в системах верифікації облич:

- створити систему для тестування як індивідуальних, так і комбінованих векторів з моделей, таких як VGG-Face, Facenet, OpenFace, ArcFace та SFace, використовуючи набір даних CFP для всебічного аналізу;
- виміряти ефективність кожної моделі та їхніх комбінацій, використовуючи точність, рівень помилкових прийомів (FAR) та рівень помилкових відмов (FRR) [9];
- проаналізувати ефективність системи за допомогою індивідуальних та комбінованих векторів моделей для визначення найефективніших стратегій верифікації облич;
- видобути гіпотези для потенційних покращень системи та виявити будь-які виклики з багатомодельними векторами.

ОСНОВНА ЧАСТИНА

Набір даних та його роль у дослідженні

Набір даних CFP відіграє ключову роль у нашому дослідженні, пропонуючи детальне вивчення верифікації облич за різних поз та умов освітлення. Його структура та характеристики наступні:

- розмір та об'єм: набір даних складається з зображень 500 осіб, на кожну з яких припадає 10 фронтальних зображень;
- роздільна здатність та якість: включаючи суміш роздільних здатностей та якостей, набір даних відображає мінливість, яку можна зустріти в реальних застосуваннях, від високоякісних до зображень нижчої якості, що ставлять виклик адаптації систем верифікації до зображень різної роздільної здатності;
- різноманітність умов: він охоплює широкий спектр реальних умов – різні сценарії освітлення від природного денного світла до штучного та слабкого освітлення, різноманітні фони від простих до переповнених сцен, а також широкий

діапазон виразів облич та поз, особливо зосереджуючись на екстремальних профільних видах, які становлять значний виклик для сучасних алгоритмів;

- джерело: зображення отримані з інтернету, що відображає умови «в реальному житті», включаючи збалансоване представлення гендерів, етнічностей та професій. Цей підхід забезпечує відображення складності та різноманітності обличчя та виразів у повсякденному житті.

Приклади з набору даних CFP показані нижче: 4 випадкові зображення обличь для кожної з трьох осіб з набору даних (рис. 1).

Рис. 1. Приклади зображень облич особистостей з набору даних CFP

Моделі нейронних мереж

Дослідження використовує різні моделі нейронних мереж, кожна з унікальними архітектурами та характеристиками, щоб визначити, як їхня унікальність впливає на ефективність конкатенованих систем. Ось короткий огляд кожної моделі:

- VGG-Face [10] базується на архітектурі VGG-16, відомій своїми глибокими згортковими шарами. Модель відрізняється тим, що була спеціально навчена на великому наборі зображень облич, оптимізуючи свої можливості для завдань розпізнавання облич. Її глибина та використання малих (3x3) згорткових фільтрів дозволяють захоплювати дрібні деталі облич, роблячи її сильним кандидатом для точної верифікації облич;
- Facenet [11] використовує функцію втрати триплетів для оптимізації векторів безпосередньо, а не для класифікації зображень. Вона відома створенням компактних 128-вимірних векторів облич, навчаючись на основі функції втрати триплетів. Цей підхід зосереджений на зменшенні відстані між якорем та позитивним зразком (та сама особа), одночасно збільшуючи відстань між якорем та негативним зразком (інша особа), таким чином ефективно підвищуючи точність верифікації;
- Facenet512 є розширенням оригінального Facenet, виробляє вектори вищої розмірності (512 вимірів), намагаючись захопити більш тонкі риси облич для покращення ефективності верифікації. Збільшення розміру векторів має на меті надати багатший опис рис облич, потенційно сприяючи кращій дискримінації між різними обличчями;
- OpenFace [12] використовує легку модель нейронної мережі, що забезпечує розпізнавання облич та верифікацію в реальному часі. Вона призначена для практичного використання, забезпечуючи баланс між точністю та обчислювальною ефективністю. OpenFace відома своєю здатністю працювати на скромному обладнанні, все ще забезпечуючи високоякісні вектори облич, що робить її придатною для застосувань в реальному часі;
- ArcFace [13] вводить додаткову кутову маржу втрат до softmax втрат, підвищуючи дискримінаційну потужність векторів. Ця модель особливо зосереджена на покращенні геометричної точності простору ознак, тим самим значно підвищуючи ефективність верифікації облич. Її інноваційний підхід до управління маржею між класами робить її надзвичайно ефективною у розрізненні різних осіб;
- SFace [14], створена дослідниками університету Бейхан, вирішує виклик розпізнавання облич на широкому діапазоні розмірів у зображеннях високої роздільної здатності. Використовуючи нейронну мережу Xception-39, вона генерує 128-вимірні вектори для ефективного вирішення проблем масштабування облич. SFace вирізняється своєю вправністю у вирішенні питань масштабу, демонструючи помітну ефективність та точність. На наборі даних 4K-Face вона показує перспективні результати, а на наборі даних WIDER FACE обробляє близько 50 кадрів за секунду з точністю 80%. Це підкреслює здатність SFace швидко та точно розпізнавати вирази облич у різноманітних умовах.

Конкатенація та метрики оцінки системи

Конкатенація моделей

Система конкатенації формує ключовий компонент нашої методології, розробленої для використання колективних сил кількох моделей розпізнавання облич. Цей підхід покликаний підвищити надійність та точність верифікації облич за допомогою використання різноманітних представлень ознак, вилучених різними моделями. Процес включає кілька ключових кроків, кожен з яких сприяє формуванню всебічного набору ознак, який використовується для верифікації облич:

1. Вибір моделі: перший крок полягає у виборі набору моделей нейронних мереж, таких як VGG-Face, Facenet, OpenFace, ArcFace та SFace, кожна з яких відома своїм унікальним підходом

до захоплення ознак облич. Це різноманіття є вирішальним для збирання широкого набору ознак;

2. Отримання вектору: для кожної моделі ми витягуємо вихідні вектори, які представляють ознаки облич, ідентифіковані цією моделлю. Ці вектори є високовимірними векторами, які укладають інтерпретацію моделі ознак облич;

3. Нормалізація Z-оцінки [15]: для стандартизації векторів з різних моделей ми застосовуємо нормалізацію Z-оцінки до кожного вектора виводу. Цей процес нормалізації налаштовує вектори так, щоб вони мали середнє значення 0 та стандартне відхилення 1. Цей крок важливий для зменшення розбіжностей у масштабі та розподілі векторів між різними моделями, забезпечуючи, щоб вивід жодної моделі не впливав надмірно на конкатенований вектор ознак;

4. Конкатенація: після нормалізації вектори з усіх обраних моделей об'єднуються в єдиний, всебічний вектор ознак. Цей конкатенований вектор представляє синтез різноманітних ознак облич, визнаних індивідуальними моделями, захоплюючи ширший спектр характеристик облич, ніж могла б будь-яка окрема модель;

5. Нормалізація L2 [16]: конкатенований вектор ознак проходить нормалізацію L2, яка масштабує вектор так, щоб він мав одиничну норму. Цей крок нормалізації критично важливий для підготовки вектора ознак до обчислень схожості, забезпечуючи, що величина вектора не впливає на вимірювання відстаней;

6. Визначення EER: після обчислення відстаней L2 між парами зображень облич ми визначаємо рівну помилкову ставку (EER), точку, де збігаються FAR та FRR. Визначення EER є важливим кроком, оскільки воно представляє оптимальну точку балансу для порогу рішень системи, мінімізуючи як хибні позитиви, так і хибні негативи.

Цей оптимальний поріг використовується для розрізнення між збігами та невідповідностями по всьому набору даних, дозволяючи правильно вимірювати метрики верифікації, такі як точність, FAR та FRR.

Метрики оцінки

Для аналізу ефективності наших систем верифікації облич, включаючи як окремі, так і комбіновані моделі, ми використовуємо три основні метрики: точність, рівень помилкових прийомів (FAR) та рівень помилкових відмов (FRR). Ці метрики допомагають нам зрозуміти ефективність систем для автентифікації облич.

1. Рівень помилкових допусків (FAR): FAR вимірює ймовірність того, що система неправильно верифікує імпостера як справжнього користувача. Це критично важливо для оцінки аспекту безпеки системи верифікації облич, де нижчі значення вказують на вищу безпеку. FAR розраховується як:

$$FAR = \frac{FP}{(FP+TN)}, \quad (1)$$

де FP – кількість хибнопозитивних результатів, а TN – кількість справжньонегативних результатів;

2. Рівень помилкових відмов (FRR): FRR оцінює частоту, з якою система помилково відкидає справжню відповідність. Ця метрика важлива для розуміння зручності використання системи, оскільки високий FRR може призвести до фрустрації користувачів. Бажані нижчі значення FRR, що вказують на кращу ефективність. FRR розраховується як:

$$FRR = \frac{FN}{(TP+FN)}, \quad (2)$$

де FN – кількість хибнонегативних результатів, а TP – кількість справжньопозитивних результатів;

3. Точність: ця метрика вимірює загальну ефективність системи верифікації облич. Вона розраховується як відношення правильно ідентифікованих випадків (як справжньопозитивних, так і справжньонегативних) до загальної кількості випадків. Висока точність вказує на те, що система ефективно верифікує обличчя. Формула для розрахунку точності виглядає так:

$$Accuracy = \frac{TP+TN}{(TP+TN+FP+FN)}. \quad (3)$$

Ці метрики разом забезпечують всебічний огляд ефективності системи, надаючи інсайти щодо її точності, безпеки та зручності використання. Оцінюючи ці метрики, ми можемо приймати обґрунтовані рішення щодо оптимізації конфігурацій моделей та покращення систем верифікації облич.

Технічне середовище та попередня обробка даних

Технічне середовище

Експерименти проводилися в рамках визначеної технічної структури, що включає специфічні компоненти апаратного та програмного забезпечення:

1. Конфігурація апаратного забезпечення: MacBook Pro 16 з процесором M1 Pro та 16 ГБ оперативної пам'яті, що забезпечує достатньо обчислювальної потужності для обробки операцій з нейронними мережами;

2. Конфігурація програмного забезпечення:

- Python 3.11: вибраний за його широку підтримку задач аналізу даних та машинного навчання;
- Tensorflow-metal 1.1.0: оптимізований для M1 Pro, покращує швидкості обчислень машинного навчання;
- OpenCV-python 4.9.0: використовується для завдань обробки зображень, таких як завантаження, зміна розміру та обрізка;
- Deepface 0.0.83: бібліотека, яка забезпечує доступ до ваг моделей розпізнавання облич (VGG-Face, Facenet, OpenFace, ArcFace, SFace) та їхніх функціональних можливостей, спрощуючи екстракцію векторів.

Попередня обробка даних

Попередня обробка даних є критично важливою початковою фазою нашого експерименту, що забезпечує належну підготовку зображень облич для аналізу різними моделями нейронних мереж. Ось короткий огляд кроків попередньої обробки, які були виконані:

- завантаження зображень: зображення спочатку завантажуються в кольоровому просторі rgb, зберігаючи їхню основну кольорову інформацію, яка є важливою для точного аналізу рис облич;
- масштабування значень пікселів: для стандартизації зображень значення пікселів кожного кольорового каналу масштабуються до діапазону від 0 до 255;
- нормалізація специфічна для моделі: залежно від вимог кожної моделі до даних зображення застосовуються специфічні техніки нормалізації, щоб відповідати умовам, за яких моделі були натреновані [17].

Для моделі Facenet:

$$img = \frac{img - mean(img)}{std(img)}, \quad (4)$$

де mean та std – середнє значення та стандартне відхилення значень пікселів зображення відповідно.

Для моделей Facenet512 та ArcFace:

$$img = \frac{img}{127} - 1. \quad (5)$$

Для моделі VGGFace:

$$img = img - \begin{bmatrix} 93.5940 \\ 104.7624 \\ 129.18633 \end{bmatrix}. \quad (6)$$

Ця формула представляє віднімання середніх значень для кожного кольорового каналу (R, G, B) на основі навчальних даних VGGFace1.

Для моделей OpenFace та SFace:

$$img = \frac{img}{255}. \quad (7)$$

Оцінка систем з однією та багатьма моделями

1. Система з однією моделлю.

На етапі оцінювання наших експериментів кожна модель нейронної мережі оцінювалася окремо для встановлення її ефективності на наборі даних CFP. Критичною частиною цієї оцінки було визначення EER для кожної моделі, який надає поріг, при якому рівень помилкових прийомів дорівнює рівню помилкових відмов.

Процес розпочався з обчислення відстаней між векторами облич для пар справжніх та імпосторів. Після цього ми обчислили EER для кожної моделі, який потім слугував основою для визначення відповідної точності в точці EER та найкращої загальної точності, досягнутої моделлю. Ці метрики дають нам уявлення про можливості моделей у завданнях верифікації облич за різноманітних умов, представлених у наборі даних CFP. Результати оцінок окремих моделей підсумовані (табл. 1).

Таблиця 1

Метрики систем з однією моделі на наборі даних CFP

Модель	EER(%)	EER точність(%)	Найвища точність(%)
VGG-Face	4.7	95.28	95.28
Facenet	3.4	96.62	**97.45**
Facenet512	**3.15**	**96.85**	97.37
OpenFace	18.3	81.70	81.72
ArcFace	5.95	94.07	94.65
SFace	18.5	81.42	81.80

Аналізуючи результати, ми спостерігаємо широкий діапазон ефективності між різними моделями. Моделі, такі як Facenet та Facenet512, показують обнадійливі значення EER та високу точність, що вказує на їх стійкість у завданнях верифікації облич. Навпаки, моделі, такі як OpenFace та SFace, демонструють виклики досягнення високої точності в різноманітних умовах набору даних CFP.

2. Системи з багатьма моделями.

Дослідження конкатенованих кластерів є невід'ємною частиною дослідження, метою якого є використання колективних сил кількох моделей нейронних мереж для підвищення точності верифікації облич. Цей розділ обговорює оцінку кластерів, сформованих усіма можливими комбінаціями шести різних моделей: VGG-Face, Facenet, Facenet512, OpenFace, ArcFace та SFace. Ко-

жен кластер ідентифікований унікальним ID для зручності посилання та порівняльного аналізу.

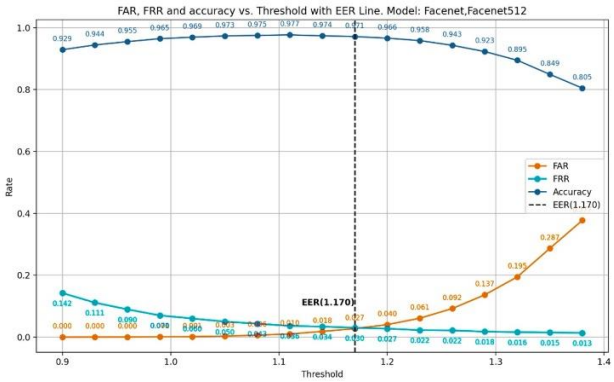

Рис. 2. Візуальний аналіз показників ефективності для кластера Facenet та Facenet512 (ID кластера 5)

Методологія оцінки розпочалася з визначення EER для кожного кластера. EER служить важливою метрикою для оцінки балансу між безпекою та зручністю користувача.

Використовуючи цей поріг, ми отримали точність на основі EER та найкращу можливу точність у ряді порогів, тим самим кількісно оцінюючи можливості верифікації моделей. Показані графіки метрик та приклад аналізу діапазону порогів (рис. 2).

Після графічного аналізу представлені результати ефективності кожного кластера (табл. 2). Ця таблиця розташовує точність EER та найкращу спостережувану точність для кожного кластера в 57 комбінаціях.

Таблиця 2

Метрики систем з багатьма моделями на наборі даних CFP

ID кластера	Моделі	EER точність(%)	Найвища точність(%)
0	VGG-Face, Facenet	95.63	95.63
1	VGG-Face, Facenet512	95.97	96.18
2	VGG-Face, OpenFace	95.33	95.33
3	VGG-Face, ArcFace	95.88	95.88
4	VGG-Face, SFace	95.55	95.55
5	Facenet, Facenet512	**97.13**	**97.68**
6	Facenet, OpenFace	95.25	95.53
7	Facenet, ArcFace	95.25	96.35
8	Facenet, SFace	95.57	96.13
9	Facenet512, OpenFace	96.87	97.28
10	Facenet512, ArcFace	96.65	97.43
11	Facenet512, SFace	**97.2**	97.33
12	OpenFace, ArcFace	93.53	94.83
13	OpenFace, SFace	85.83	86.13
14	ArcFace, SFace	93.67	94.62
15	VGG-Face, Facenet, Facenet512	96.13	96.35
16	VGG-Face, Facenet, OpenFace	95.57	95.63
17	VGG-Face, Facenet, ArcFace	95.93	96.03
18	VGG-Face, Facenet, SFace	95.67	95.67
19	VGG-Face, Facenet512, OpenFace	95.9	96.25
20	VGG-Face, Facenet512, ArcFace	96.13	96.52
21	VGG-Face, Facenet512, SFace	95.92	96.23
22	VGG-Face, OpenFace, ArcFace	95.68	95.98
23	VGG-Face, OpenFace, SFace	95.35	95.35
24	VGG-Face, ArcFace, SFace	95.82	95.92
25	Facenet, Facenet512, OpenFace	96.68	**97.55**
26	Facenet, Facenet512, ArcFace	96.65	**97.53**
27	Facenet, Facenet512, SFace	**97.3**	**97.57**
28	Facenet, OpenFace, ArcFace	94.9	96.13
29	Facenet, OpenFace, SFace	94.38	94.62
30	Facenet, ArcFace, SFace	95.98	96.15
31	Facenet512, OpenFace, ArcFace	96.8	97.23
32	Facenet512, OpenFace, SFace	96.57	97.23
33	Facenet512, ArcFace, SFace	96.55	97.3
34	OpenFace, ArcFace, SFace	93.53	94.37

35	VGG-Face, Facenet, Facenet512, OpenFace	95.97	96.52
36	VGG-Face, Facenet, Facenet512, ArcFace	96.2	96.72
37	VGG-Face, Facenet, Facenet512, SFace	96.12	96.47
38	VGG-Face, Facenet, OpenFace, ArcFace	95.77	96.07
39	VGG-Face, Facenet, OpenFace, SFace	95.47	95.7
40	VGG-Face, Facenet, ArcFace, SFace	95.97	96.03
41	VGG-Face, Facenet512, OpenFace ,ArcFace	96.08	96.55
42	VGG-Face, Facenet512, OpenFace, SFace	95.97	96.32
43	VGG-Face, Facenet512, ArcFace, SFace	96.1	96.63
44	VGG-Face, OpenFace, ArcFace, SFace	95.63	95.88
45	Facenet, Facenet512, OpenFace, ArcFace	**96.92**	97.35
46	Facenet, Facenet512, OpenFace, SFace	96.78	97.43
47	Facenet, Facenet512, ArcFace, SFace	96.57	97.43
48	Facenet, OpenFace, ArcFace, SFace	94.93	95.88
49	Facenet512, OpenFace, ArcFace, SFace	96.8	97.1
50	VGG-Face, Facenet, Facenet512, OpenFace, ArcFace	96.12	96.72
51	VGG-Face, Facenet, Facenet512, OpenFace, SFace	95.98	96.53
52	VGG-Face, Facenet, Facenet512, ArcFace, SFace	96.13	96.75
53	VGG-Face, Facenet, OpenFace, ArcFace, SFace	95.73	96.07
54	VGG-Face, Facenet512, OpenFace, ArcFace, SFace	96.07	96.55
55	Facenet, Facenet512, OpenFace, ArcFace, SFace	**96.95**	97.35
56	VGG-Face,Facenet,Facenet512,OpenFace,ArcFace,SFace	96.08	96.67

Під час оцінки конкатенованих кластерів наші дані вказують, що обрані кластери досягають незначного підвищення точності порівняно з найкращою індивідуальною моделлю, Facenet-512. Зокрема, кластери 5, 9, 11, 25, 26, 27, 45 та 55 демонструють несуттєве поліпшення, покращуючи точність найкращої окремої моделі приблизно на 0.23%. Хоча це покращення демонструє потенційні переваги конкатенації моделей, важливо враховувати обчислювальні потреби, пов'язані з такою стратегією.

РЕЗУЛЬТАТИ АНАЛІЗУ ТА ВИСНОВКИ

Ключові висновки

Дослідження ефективності моделей верифікації облич, як окремо, так і в комбінованих кластерах, виявило кілька ключових висновків:

- вплив комбінування моделей на ефективність системи: наші результати підкреслюють помітну тенденцію, де кластери, що комбінують моделі з нижчою початковою точністю, відчувають значне збільшення ефективності. Наприклад, поєднання OpenFace з SFace (ID кластера 13) призвело до збільшення точності на 4.33%, досягнувши показника в 86.13%. Це контрастує з кластерами високоефективних моделей, які в середньому показують лише приблизно 0.5% покращення в точності. Це спостереження свідчить, що стратегічне парування, особливо з використанням моделей з різними сильними сторонами, може ефективно компенсувати індивідуальні слабкості;
- не систематичні результати від кластерів змішаних моделей: не всі комбінації моделей призводять до позитивних результатів. У деяких випадках, як у кластері Facenet і VGG-Face (ID кластера 0), результуюча точність була трохи нижчою, ніж у моделі Facenet. Це вказує на складність взаємодії моделей у кластерах і показує, що комбінування моделей не гарантує підвищення ефективності і може, фактично, призвести до субоптимальних результатів у певних конфігураціях;
- проблеми обчислювальної ефективності: хоча деякі кластери моделей досягають невеликих покращень в точності, як Facenet з Facenet512 (ID кластера 5) з збільшенням на 0.23%, необхідні обчислювальні ресурси значно зростають. Це свідчить про потенційні негативні співвідношення витрат і користі від використання конкатенованих моделей, особливо коли здобутки в ефективності невеликі порівняно з доданим обчислювальною потребою;
- дотримання високої точності та безпеки: варто відзначити, що як індивідуальні, так і кластеровані моделі, які досягають найвищої ефективності, змогли зберегти свою точність без будь-яких помилкових прийомів на наборі даних CFP. Це демонструє їх потенціал у сценаріях, що вимагають високої безпеки, де збереження точності без компромісів щодо рівня помилкових прийомів є критично важливим;
- стратегічний склад кластерів для оптимальної ефективності: аналіз додатково виявляє, що

найуспішніші кластери часто включають комбінацію двох найкращих моделей разом з однією з менш ефективних. Такий склад свідчить, що різноманітні можливості розпізнавання ознак комбінованих моделей сприяють більш всебічному аналізу і можуть підвищити загальну ефективність системи.

Виклики

Протягом проведення цього дослідження ми зіткнулися з декількома викликами, які вплинули на реалізацію наших експериментів та аналіз результатів:

- нормалізація вхідних даних: для ефективної роботи кожна модель нейронної мережі вимагає, щоб вхідні дані були нормалізовані відповідно до специфічних тренувальних даних, з якими вона була розроблена. Цей процес нормалізації включав коригування кольорового простору та масштабування каналів для кожної моделі, щоб відповідати її умовам тренування;
- Z-оцінкова нормалізація вихідних векторів: враховуючи розбіжність у розподілі векторів між різними моделями, значним викликом була стандартизація цих векторів для спільного аналізу. Застосування Z-оцінкової нормалізації до кожного вектора дозволило відрегулювати вектори так, що їх середнє значення стало 0, а стандартне відхилення – 1. Цей критичний крок дозволив зменшити розбіжності у виходах кожної моделі;
- значний час на обчислення без потужних серверних ресурсів: обчислення, необхідні для генерації векторів для 57 кластерів разом з оцінкою окремих моделей, були значними. Для оптимізації ми впровадили механізм кешування [18] для векторів після налаштування системи. Стратегія дозволила повторно використовувати вектори у різних кластерах та експериментах з окремими моделями, економлячи десятки годин обчислювального часу;
- нижча за очікувану точність для моделей OpenFace та SFace: нижча, ніж очікувалося, точність для моделей OpenFace та SFace викликала занепокоєння. Це могло бути викликано неточною інформацією нормалізації або відхиленнями від стандартних тренувальних даних, які використовувались у цих моделях. Хоча ця стаття не фокусувалась безпосередньо на покращеннях точності цих моделей, ідентифікація потенційних причин відкриває шлях для майбутніх покращень;
- роздільна здатність набору даних: хоча набір даних CFP був достатньо всебічним для наших експериментальних цілей, його розмір та різноманітність даних були обмеженими. Більший та різноманітний набір даних міг би виявити інсайти та проблеми, які не спостерігалися з використаним у дослідженні набором даних CFP. Для майбутніх напрямків дослідження рекомендовано дослідити більші набори даних для глибшого аналізу.

Рекомендації та майбутні дослідження

Висновки з наших експериментів надають цінне розуміння про синергію ефективності систем біометричної автентифікації облич при використанні конкатенованих кластерів моделей нейронних мереж.

На основі нашого аналізу надаються наступні рекомендації:

- ефективність проти невеликих покращень: поточна експериментальна система демонструє, що хоча декілька кластерів досягли поступового покращення в точності, необхідне збільшення обчислювальних ресурсів було надмірно великим. Враховуючи це, для застосувань, де обчислювальна ефективність є пріоритетом, використання окремих моделей, таких як Facenet або Facenet512, є більш рекомендоване. Ці моделі забезпечують достатньо високу точність без значного обчислювального навантаження, пов'язаного з кластерами моделей;
- застосування без обмежень в обчислювальних ресурсах: у випадках, де система верифікації може дозволити собі збільшений час висновків та має доступ до значних обчислювальних потужностей, використання кластерів моделей може бути корисним. Зокрема, кластер, що поєднує Facenet і Facenet512 (ID кластера 5), представляє найкращий варіант, оскільки він перевершує точність моделі Facenet на 0.23%, досягаючи точності 97.68%. Це невелике покращення може виправдати додаткові обчислювальні ресурси в сценаріях, де максимізація точності має вирішальне значення;
- балансування швидкості та точності в системах з обмеженими ресурсами: для систем верифікації, які обмежені обчислювальними можливостями та часовими обмеженнями, але прагнуть покращити точність, яку надають швидкі моделі, як OpenFace, формування кластерів з іншими швидкодіючими моделями пропонує стратегічне рішення. Наприклад, парування OpenFace з SFace призвело до значного збільшення точності на 4.33% порівняно з окремою моделлю OpenFace, досягаючи точності 86.13%. Ця стратегія дозволяє збалансовано покращити точність, зберігаючи при цьому необхідні можливості

швидких обчислень, що підходить для застосувань, де цінуються як ефективність, так і точність.

Рішення про використання окремих моделей чи конкатенованих кластерів повинно керуватися конкретними вимогами та обмеженнями конкретної системи верифікації облич.

Дослідження конкатенованих кластерів моделей у верифікації облич створює численні можливості для майбутніх досліджень. Наше дослідження визначило кілька ключових областей, які можуть значно покращити ефективність і ефективність систем верифікації облич:

- аналіз впливу ознак вихідних векторів моделей: перспективним напрямком є аналіз конкретних ознак у векторах кожної моделі, які найбільше впливають на рішення про верифікацію. Шляхом ідентифікації та пріоритизації цих впливових ознак можливо відфільтрувати менш релевантні або шумові ознаки з векторів моделей [19]. Цей підхід має потенціал не тільки для систем з окремими моделями, але й може значно покращити продуктивність систем кластеризованих моделей, зосереджуючись на комбінації найважливіших ознак для розрахунку відстані L2;
- альтернативні метрики відстані: поточне дослідження використовує відстань L2 для оцінки схожості між векторами облич. Майбутні дослідження можуть вивчати ефективність альтернативних метрик відстані, таких як косинусна [20] і L1 відстані. Ці метрики можуть створити різні розподіли, пороги та в кінцевому підсумку точності для кластерів моделей, надаючи нове розуміння про оптимізацію систем верифікації;
- продуктивність на більших, високоякісних наборах даних: переваги кластеризованих систем можуть стати більш помітними, коли вони застосовуються до більших наборів даних з вищою роздільною здатністю та якістю зображень. Додаткові дослідження можуть оцінити, як ці системи масштабуються та працюють у ще більш різноманітних умовах, потенційно виявляючи переваги, які не спостерігалися в поточному наборі даних;
- інтеграція специфічного для моделі вирівнювання: враховуючи, що певні моделі сильно залежать від вирівнювання облич, інтеграція динамічних технік вирівнювання, адаптованих до кожної моделі в кластері, може покращити точність. Цей персоналізований підхід до вирівнювання облич може оптимізувати продуктивність внеску кожної моделі в кластері;
- комбінації моделей, зосереджені на ефективності: початковий успіх комбінації моделей з нижчою продуктивністю, але швидшим обрахунком, слугує сильною базою для стратегії розробки ефективних систем верифікації, придатних для вбудованих систем. Майбутня робота може зосередитися на ідентифікації та тестуванні комбінацій ефективних, швидких моделей для створення системи верифікації, яка балансує точність з необхідною обчислювальною швидкістю для застосувань в реальному часі в обмежених умовах.

ЛІТЕРАТУРА

[1]. G. Alfarsi, J. Jabbar, R. M. Tawafak, A. Alsidiri and M. Alsinani, "Techniques for Face Verification: Literature Review," 2019 International Arab Conference on Information Technology (ACIT), Al Ain, United Arab Emirates, 2019, pp. 107-112, doi: 10.1109/ACIT47987.2019.8990975.

[2]. M. Zulfiqar, F. Syed, M. J. Khan and K. Khurshid, "Deep Face Recognition for Biometric Authentication," 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Swat, Pakistan, 2019, pp. 1-6, doi: 10.1109/ICECCE47252.2019.8940725.

[3]. S. Sengupta, J.C. Cheng, C.D. Castillo, V.M. Patel, R. Chellappa, D.W. Jacobs, Frontal to Profile Face Verification in the Wild, IEEE Conference on Applications of Computer Vision, 2016.

[4]. LeCun, Y., Bengio, Y. & Hinton, G. Deep learning. Nature 521, pp. 436-444 (2015). (https://doi.org/10.1038/nature14539).

[5]. C. Ding and D. Tao, "Robust Face Recognition via Multimodal Deep Face Representation," in IEEE Transactions on Multimedia, vol. 17, no. 11, pp. 2049-2058, Nov. 2015, doi: 10.1109 / TMM.2015.2477042.

[6]. M. Egmont-Petersen, D. de Ridder, H. Handels, Image processing with neural networks: a review, Pattern Recognition, Volume 35, Issue 10, 2002, pp. 2279-2301, ISSN 0031-3203. (https: // doi.org/10.1016/S0031-3203(01)00178-9).

[7]. Neoklis Polyzotis, Sudip Roy, Steven Euijong Whang, and Martin Zinkevich. 2018. Data Lifecycle Challenges in Production Machine Learning: A Survey. SIGMOD Rec. 47, 2 (June 2018), pp. 17-28. (https://doi.org/10.1145/3299887.3299891).

[8]. Wang, X., Jiang, Y., Bach, N., Wang, T., Huang, Z., Huang, F., & Tu, K. (2021). Automated Concatenation of Embeddings for Structured Prediction. In Zong, C., Xia, F., Li, W., & Navigli, R. (Eds.), Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)(pp. 2643-2660). DOI: 10.18653/v1/2021.acl-long.206.

[9]. Roberto Tronci, Giorgio Giacinto, Fabio Roli, Designing multiple biometric systems: Measures of ensemble effectiveness, Engineering Applications of Artificial Intelligence, Volume 22, Issue 1, 2009, pp.

66-78, ISSN 0952-1976. (https: //doi.org/10.1016/j.engappai.2008.04.007).
[10]. Q. Cao, L. Shen, W. Xie, O. M. Parkhi and A. Zisserman, "VGGFace2: A Dataset for Recognising Faces across Pose and Age," 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, China, 2018, pp. 67-74, doi: 10.1109/FG.2018.00020.
[11]. F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682.
[12]. T. Baltrušaitis, P. Robinson and L. P. Morency, "OpenFace: An open-source facial behavior analysis toolkit," 2016 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Placid, NY, USA, 2016, pp. 1-10, doi: 10.1109 / WACV. 2016. 7477553.
[13]. J. Deng, J. Guo, J. Yang, N. Xue, I. Kotsia and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 10, pp. 5962-5979, 1 Oct. 2022, doi: 10.1109/TPAMI.2021.3087709.
[14]. Wang, J., Yuan, Y., Li, B., Yu, G., & Jian, S. (2018). SFace: An Efficient Network for Face Detection in Large Scale Variations. ArXiv, abs/1804.06559.
[15]. Anil Jain, Karthik Nandakumar, Arun Ross, Score normalization in multimodal biometric systems, Pattern Recognition, Volume 38, Issue 12, 2005, Pages 2270-2285, ISSN 0031-3203. (https: // doi.org /10.1016/j.patcog.2005.01.012).
[16]. Perlibakas, V. (2004). Distance measures for PCA-based face recognition. Pattern Recognit. Lett., 25, pp. 711-724. (https://doi.org/10.1016/j.patrec.2004.01.011).
[17]. Günther, F., & Fritsch, S. (2010). neuralnet: Training of Neural Networks. R J., 2, 30. (https: // doi.org/10.32614/RJ-2010-006).
[18]. Fasnacht, L. (2018). mmappickle: Python 3 module to store memory-mapped numpy array in pickle format. J. Open Source Softw., 3, 651. (https://doi.org/10.21105/JOSS.00651).
[19]. Ye, H., Li, X., Yao, Y., & Tong, H. (2022). Towards Robust Neural Graph Collaborative Filtering via Structure Denoising and Embedding Perturbation. ACM Transactions on Information Systems, 41, pp. 1-28. (https://doi.org/10.1145/3568396).
[20]. Nguyen, H., & Bai, L. (2010). Cosine Similarity Metric Learning for Face Verification., pp. 709-720. (https://doi.org/10.1007/978-3-642-19309-5_55).

RESEARCH ON THE EFFICIENCY OF COMBINED EMBEDDINGS FOR FACIAL VERIFICATION

In the era of digital authentication, facial verification systems have become a cornerstone of security protocols across various applications. This study explores the performance synergy from concatenated embeddings in enhancing biometric authentication accuracy. By leveraging the Celebrities in Frontal-Profile dataset (CFP), we investigate whether the fusion of embeddings generated by models such as VGG-Face, Facenet, OpenFace, ArcFace, and SFace can result in a more robust authentication process. The approach involves computing the L2 distance between normalized concatenated embeddings of an input face image and an anchor, thereby determining the authenticity of the individual. Experiments are designed to compare the performance of singular model embeddings against concatenated embeddings, employing metrics such as accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR). The findings of this research could significantly contribute to the development of more secure and reliable facial verification systems by using multiple existing models without the need for new model research, designing, and training.

Keywords: Facial Verification, Biometric Authentication, Neural Networks, Concatenated Embeddings.

Ханін Денис Олегович, асистент кафедри захисту інформації Національного університету «Львівська політехніка».
Denys Khanin, Assistant at the Department of Information Security, National University "Lviv Polytechnic".
E-mail: denys.o.khanin@lpnu.ua.
Orcid ID: 0009-0001-4009-0202.

Отенко Віктор Іванович, к.т.н., доцент кафедри захисту інформації Національного університету «Львівська політехніка».
Viktor Otenko, PhD, Associate Professor at the Department of Information Security, National University "Lviv Polytechnic".
E-mail: viktor.i.otenko@lpnu.ua.
Orcid ID: 0000-0003-4781-7766.

DOI: 10.18372/2410-7840.26.18832
УДК 004.422.4:005.3:004.4

МУЛЬТИАСПЕКТНІСТЬ ТА СТРАТЕГІЧНЕ ПЛАНУВАННЯ ПРИ СТВОРЕНІ БАГАТОЦІЛЬОВИХ МОДЕЛЕЙ ОЦІНКИ ЯКОСТІ ПРОГРАМНИХ СИСТЕМ

Антон Шантир, Ольга Зінченко, Максим Фесенко, Віктор Вишнівський

У сучасному інформаційному суспільстві проблема оцінювання якості програмних систем (ПС) є однією з ключових. Мета даної статті полягає в ретельному розгляді особливостей процесу оцінювання якості ПС з використанням принципів мультиаспектності та стратегічного планування. Для досягнення поставленої мети визначені чотири основні цілі. По-перше, стаття пропонує докладно розглянути основні етапи принципу мультиаспектності в підході до оцінювання якості ПС при створенні багатоцільових моделей якості. По-друге, здійснюється спроба надати математичні пояснення щодо того, як може бути представлена му-