Issue 15, 2024

https://doi.org/10.23939/sisn2024.15.001

УДК 004.439

МЕТОД ІДЕНТИФІКАЦІЇ ВІДБИТКІВ ПАЛЬЦІВ НА ОСНОВІ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Юрій Мишковський[1], Марія Назаркевич[2]

[1, 2] Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж, Львів, Україна,
[1] E-mail: yurii.i.myshkovskyi@lpnu.ua, ORCID: 0009-0004-0051-026X
[2] E-mail: mariia.a.nazarkevych@lpnu.ua, ORCID: 0000-0002-6528-9867

Запропоновано передовий метод ідентифікації відбитків пальців, оснований на технології згорткових нейронних мереж (CNN). У роботі детально описано процес розроблення та впровадження спеціалізованої архітектури CNN для виявлення і верифікації автентичності відбитків пальців. Використання комплексного набору даних Socofing дало змогу глибоко проаналізувати здатність моделі розрізняти справжні та імітовані відбитки пальців. Точність моделі вражає – до 98,964 %. Особливу увагу звернено на аналіз помилок, зокрема відсоток помилкового виявлення та пропускання, що вказує на потенційні напрями подальшого удосконалення. Окрім висвітлення технічних аспектів і високої точності ідентифікації, у статті також розглянуто потенційні виклики та обмеження, з якими можна зіткнутися, використовуючи метод. Це проблеми, пов'язані з незбалансованістю та різноманітністю даних у наборі Socofing, а також обмеження, пов'язані з обчислювальними ресурсами під час навчання глибоких нейронних мереж. Висвітлено потенційні способи оптимізації моделі, зокрема, зосереджено увагу на зменшенні відсотка помилкового пропускання, що може покращити досвід користувача під час автентифікації. У завершальній частині статті наголошено на важливості поданої роботи для сфери безпеки, де критично потрібна точна аутентифікація зображень відбитків пальців. Отримані результати можна вважати міцним підґрунтям для майбутніх наукових розробок у цьому напрямі. Також звернено увагу на необхідність систематичного оновлення та модифікації моделі з метою її адаптації до постійно вдосконалюваних методик імітації, що забезпечить її довгострокову релевантність та ефективність.

Ключові слова: відбитки пальців; згорткові нейронні мережі (CNN); біометрична аутентифікація; підробки.

Вступ та постановка проблеми

Біометричні технології сьогодні є ключовими засобами безпеки, що активно впроваджуються у різноманітні сфери життя. Завдяки високій надійності та зручності методи біометричної аутентифікації стали невід'ємною частиною сучасних систем контролю доступу. Однак, попри значні зусилля, спрямовані на розроблення та вдосконалення цих методів, стабільність та надійність систем ідентифікації залишаються недостатніми для відповіді на усі виклики сучасного світу. Особливу увагу привертають системи ідентифікації за відбитками пальців, які, незважаючи на унікальність біометричних даних, вразливі до атак і підробок.

Об'єктом дослідження є процес ідентифікації особи за відбитками пальців у системах біометричної аутентифікації. Це явище передбачає взаємодію між технологіями визначення відбитків

пальців і потенційними викликами безпеки, які виникають через можливість підробки або імітації відбитків. Отже, об'єкт дослідження охоплює ширший контекст використання біометричних технологій для ідентифікації осіб, виявляючи проблемну ситуацію, пов'язану із необхідністю забезпечення високого рівня точності та безпеки в цих системах.

Предметом дослідження є вивчення способів підвищення точності та безпеки ідентифікації осіб за допомогою згорткових нейронних мереж (CNN) у контексті біометричних систем аутентифікації на основі відбитків пальців. Конкретно предмет охоплює аналіз та вдосконалення методів глибокого навчання для ефективної ідентифікації відбитків пальців, здатних відрізняти достовірні відбитки від імітацій. Це передбачає розроблення архітектури нейронної мережі, вибір оптимальних параметрів для обробки зображень відбитків, оцінювання продуктивності моделі на основі стандартних метрик та порівняльний аналіз із іншими методами.

Основні цілі цього дослідження – розроблення та навчання моделі CNN, оцінювання її продуктивності за допомогою стандартних метрик, дослідження стійкості моделі проти різних типів спроб підробки, а також порівняння точності CNN з іншими моделями машинного та глибокого навчання.

Наукова новизна дослідження полягає у розробленні унікальної архітектури нейронної мережі, яка демонструє високу точність у класифікації відбитків пальців. Ця розробка відкриває нові перспективи для підвищення безпеки біометричних систем ідентифікації та пропонує ефективні рішення для протидії сучасним викликам у сфері біометричної аутентифікації.

Аналіз останніх досліджень та публікацій

Методи біометричної ідентифікації [2] забезпечують надійний захист. Біометрична аутентифікація користувача – це метод, який ідентифікує користувача та підтверджує його особистість на основі вимірювання його унікальних фізіологічних ознак або поведінкових характеристик. Фізіологічними біометричними даними є відбитки пальців, розпізнавання особи, сканування райдужки, геометрія руки, сканування сітківки. Поведінковими біометричними даними [3] є розпізнавання голосу, сканування натиску клавіш та сканування підпису. Багато ноутбуків оснащено сканерами відбитків пальців, також доступні USB-накопичувачі, які зчитують відбитки пальців. Біометрична аутентифікація широко використовується завдяки високій надійності: вона звільняє користувача від важкого завдання відновлення паролів; біометричні дані є унікальними та простими; дуже важко відтворити біометричні характеристики, їх неможливо втратити; сканування відбитків пальців [4] швидке та недороге; сканування очей дає змогу точно визначити користувача.

Зі збільшенням залежності від біометричної аутентифікації в системах безпеки [5] важливість розпізнавання відбитків пальців істотно зросла. Системи на основі відбитків пальців використовують у безлічі застосувань, починаючи від смартфонів і закінчуючи перевірками громадян, які іммігрують, в аеропортах. Однак, як і всі системи безпеки, системи розпізнавання відбитків пальців [6] не є повністю захищеними. Роблять спроби подавати підроблені або сфабриковані відбитки пальців, що зумовлює потребу в ефективних механізмах виявлення достовірності. Виявлення достовірності забезпечено у джерелі [4], де наведено біометричні дані.

Уже розроблено достатньо технік та методологій для встановлення достовірності відбитків пальців, проте існує потреба в надійних та стабільних методах, оскільки зловживання стають усе підступнішими. З розвитком глибокого навчання CNN [7] продемонструвало значний потенціал у різних задачах комп'ютерного зору. Метою цього дослідження є вивчення стійкості CNN для встановлення достовірності відбитків. Al-Wajih et al. [19] зосередили своє дослідження на класифікації типів відбитків пальців за допомогою глибоких згорткових нейронних мереж, підкреслюючи значні можливості CNN у підвищенні точності та ефективності біометричної ідентифікації. Такий підхід демонструє, як глибоке навчання може сприяти кращому розумінню та класифікації складних візу-

альних ознак відбитків пальців, що є критично важливим для розвитку надійних систем безпеки. З іншого боку, робота Zong, Xu, і Yuan [20] пропонує застосування CNN для розпізнавання радіочастотних відбитків, відкриваючи нові можливості для застосування цих технологій у бездротових комунікаціях та інших сферах, де біометрична ідентифікація може слугувати додатковим засобом забезпечення безпеки. Це дослідження наголошує на універсальності та адаптивності CNN до різних типів біометричних даних, підтверджуючи істотний потенціал глибокого навчання в ідентифікації осіб.

Дуже часто розпізнавання відбитків пальців зводиться до вирішення завдання класифікації, що полягає у створенні навчального набору розмічених зображень. Інша складність полягає у підключенні великих обчислювальних ресурсів, щоб завершити процес навчання за короткий відрізок часу. Метод, описаний у [8], дає змогу використовувати попередньо навчені моделі даних для побудови класифікатора зображень. Трансферне навчання [9] дає можливість повторно натренувати останній шар мережі, з використанням власного набору зображень, не змінюючи ваг інших шарів та досягаючи необхідної точності моделі. Зокрема у Residual Network [10] описана згорткова нейронна мережа. Основним елементом Residual Network є залишковий блок зі швидким з'єднанням, що являє собою декілька згорткових шарів із активаціями. Мережа складається з 101 шару, тому можна апроксимувати складніші залежності між вхідними та вихідними даними.

Ідентифікація відбитків пальців на основі CNN [11] – це метод біометричної ідентифікації. CNN – це тип нейронної мережі, який добре підходить для розпізнавання зображень, оскільки може виявляти візуальні особливості, такі як крапки, лінії та дуги, характерні для відбитків пальців.

Метод ідентифікації відбитків пальців CNN працює так:

1. Спочатку відбиток пальця сканують та перетворюють на цифрове зображення.
2. Потім зображення відбитка пальця подають у CNN.
3. CNN навчається виявляти візуальні особливості відбитка пальця.
4. Коли новий відбиток пальця подано в CNN, мережа використовує свої знання про візуальні особливості, щоб визначити, чи належить він відомій особі.

Моделі на основі глибокого навчання дуже успішні в комп'ютерному зорі [12]. Ці моделі застосовують для вирішення проблем біометричного розпізнавання, застосування якого постійно зростає. Моделі на основі глибокого навчання все частіше використовують для підвищення точності різних біометричних даних систем розпізнавання.

У [13] запропоновано модель часткової ідентифікації відбитків пальців на основі модуля уваги під назвою APFI. По-перше, алгоритм використовує залишкову мережу (ResNet) для вилучення дескриптора ознак, який генерує представлення просторової інформації на зображенні відбитків пальців. Модуль уваги каналу вставляють у запропоновану модель для отримання точнішої інформації про відбитки пальців із залишкового блока. Потім, щоб підвищити точність ідентифікації часткових відбитків пальців, кутову відстань між ознаками використовують для обчислення подібності відбитків пальців. Нарешті, запропонована модель тренується та перевіряється на саморобному наборі даних зображень часткових відбитків пальців. Експерименти на саморобних наборах даних відбитків пальців і наборах даних NIST-SD4 показали, що метод часткової ідентифікації відбитків пальців, запропонований у цій статті, забезпечує вищу точність ідентифікації, ніж інші сучасні методи.

Розроблено систему ідентифікації відбитків пальців на основі згорткової нейронної мережі та систему інтерпретації результатів класифікації, що дає змогу задавати співвідношення помилок першого і другого роду та вибирати поріг детектування на основі цього співвідношення. На відміну від стандартного рішення, система не використовує критерій максимальної правдоподібності, що дає змогу отримувати більше інформації від класифікатора та знизити рівень помилок системи. Вихідні дані для дослідження – тисяча фотографій, на яких зображені автори статті. Розроблений метод є інноваційним і дає змогу поліпшити комплексні захисні системи.

Класифікація зображення полягає у використанні комп'ютерного зору, де комп'ютер може імітувати здатність людини розуміти дані на зображенні [14]. Процес класифікації зображення може виконуватись із глибоким навчанням, він подібний до роботи мозку під час мислення та спроб відтворювати частину своїх функцій за допомогою нейронів. Згорткова нейронна мережа є одним із видів глибокого навчання. У цьому дослідженні розроблено класифікацію статі на основі методу відбитків пальців. Результати цього дослідження буде використано як модель CNN з рівнем точності 99,9667 %.

Аналіз цих досліджень у контексті нашого власного дослідження підкреслює актуальність застосування новітніх методів глибокого навчання для вирішення наявних та потенційних викликів у біометричній ідентифікації. Вони свідчать про необхідність подальших досліджень та розробок у цій сфері з метою розширення меж можливого та підвищення точності та надійності біометричних систем. Наше дослідження спирається на ці фундаментальні знахідки та пропонує інноваційний підхід до розроблення біометричних систем ідентифікації, що відповідає сучасним вимогам безпеки. Метод ідентифікації відбитків пальців на основі згорткових нейронних мереж має переваги порівняно з традиційними методами ідентифікації відбитків пальців. Він точніший, оскільки може виявляти дрібніші деталі. Він також швидший, оскільки може обробляти зображення за частки секунди.

Формулювання цілі статті та постановка задачі

Центральною метою нашого дослідження є розроблення та валідація моделі згорткової нейронної мережі (CNN), оптимізованої для ідентифікації відбитків пальців, з метою істотного покращення точності та надійності біометричних систем ідентифікації. Ми прагнемо вивчити, як глибоке навчання впливатиме на здатність системи розпізнавати складні візуальні шаблони відбитків пальців, зокрема, розрізняючи достовірні зразки від імітацій. Для досягнення цієї мети, ми поставили перед собою такі завдання:

1. Аналіз відомих методів ідентифікації відбитків пальців та визначення обмежень поточних підходів.
2. Розроблення архітектури CNN, яка ефективно обробляє зображення відбитків пальців, забезпечуючи високу точність розпізнавання.
3. Навчання та тестування моделі із використанням розгорнутого набору даних, що містить як достовірні, так і імітовані відбитки пальців.
4. Оцінювання ефективності моделі через аналіз метрик точності, відсотка помилкового виявлення (ВПВ) та відсотка помилкового пропускання (ВПП).
5. Порівняння результатів використання пропонованої моделі з наявними методами та визначення її переваг.

Очікуємо, що наша модель CNN не лише забезпечить вищу точність порівняно з традиційними методами ідентифікації відбитків пальців, але й зможе ефективно протистояти спробам підробки, тим самим підвищуючи загальний рівень безпеки в системах біометричної ідентифікації. Результати цього дослідження мають на меті сприяти подальшому розвитку та оптимізації біометричних систем ідентифікації на основі глибокого навчання.

Виклад основного матеріалу

Відомі такі метрики розпізнавання образів [15], за результатами яких можна зробити висновки про ефективність алгоритму або системи в розпізнаванні об'єктів, патернів чи зразків на зображеннях. Ці метрики допомагають визначити, наскільки точно і надійно виконується завдання розпізнавання. Ось деякі загальні метрики для оцінювання роботи систем розпізнавання образів:

1. Точність (Accuracy). Це відношення кількості правильно розпізнаних об'єктів до загальної кількості об'єктів. Точність можна використати для визначення загальної ефективності системи.

$$T = \frac{TP + TN}{TP + TN + FP + FN},$$

де *TP* – істинно позитивне; *TN* – істинно негативне; *FP* – хибно позитивне; *FN* – хибно негативне. Точність використовують як статистичний показник або ж це частка правильних прогнозів серед загальної кількості досліджених випадків. Так порівнюють імовірності до і після класифікації.

2. Матриця помилок (confusion matrix)

Матриця помилок надає інформацію про те, де ми помилились, у вигляді умовної таблиці розподілу – *ij*-та позиція матриці дорівнює кількості об'єктів *j*-го класу, яким алгоритм присвоїв мітку *i*-го класу.

	Справжній стан	
Прогнозований стан	істинно позитивний	хибно позитивний, помилка першого роду
	хибно негативний, помилка другого роду	істинно негативний

3. Точність класифікації (Precision). Визначає, наскільки точно система знайшла позитивні приклади серед усіх прикладів, які вона визнала позитивними:

$$Precision = \frac{TP}{TP+FP},$$

Precision можна інтерпретувати як частку об'єктів, які класифікатор назвав позитивними і які справді є позитивними, а відкликання вказує, яку частку об'єктів позитивного класу з усіх об'єктів позитивного класу знайшов алгоритм.

4. Recall (повнота) відома також як чутливість, є часткою загальної кількості позитивних зразків, яку було справді знайдено. Повнота є мірою того, наскільки добре модель виявляє всі позитивні зразки.

$$Recall = \frac{TP}{TP + FN},$$

5. F-міра є комбінованою мірою точності та повноти. F-міра зважує точність та повноту, щоб отримати єдине число, яке відображає загальну продуктивність моделі. Визначається як залежність від повноти за фіксованої точності й позначається формулою:

$$F_\beta = (1 + \beta^2)\frac{Precision \times Recall}{\beta^2(Precision + Recall)},$$

де β визначає вагу точності в усередненій (агрегованій) метриці.

Набір даних Socofing

Дослідження ґрунтується на наборі даних Socofing [1], доступному на Kaggle. Socofing – це великий набір даних зображень відбитків, розроблений, щоб сприяти дослідженню виявлення справжності відбитків пальців. Він містить комбінацію справжніх та підроблених відбитків пальців, що робить його ідеальним для нашого аналізу.

Набір даних Socofing створила BiDA-Lab (Лабораторія біометрії Америки) при Universidad de las Fuerzas Armadas ESPE. Його мета – надати надійне порівняння для алгоритмів, що повинні відрізняти справжні та підроблені відбитки пальців [1]. Кожне зображення у наборі даних відрізняється за роздільною здатністю, відтворюючи відбитки з багатьма деталями. Зображення відбитків пальців у наборі даних Socofing отримані з різних пристроїв і надають різноманітні дані для імітації реальних сценаріїв. Перед введенням даних у модель виконано кілька етапів попереднього оброблення кожного зображення, зокрема нормалізацію, зміну розміру та аугментацію, щоб підвищити здатність моделі до узагальнення.

Приклади набору даних SocoFing відображено на рис. 1: достовірні відбитки пальців у першому рядку, незначно модифіковані відбитки пальців у другому та суттєво модифіковані відбитки пальців у третьому рядку.

Рис. 1. Приклади з набору даних SocoFing

Архітектура моделі CNN

Основна модель, проаналізована в цьому дослідженні, – згорткова нейромережа (CNN), відома своєю здатністю обробляти зображення (див. рис. 2).

.

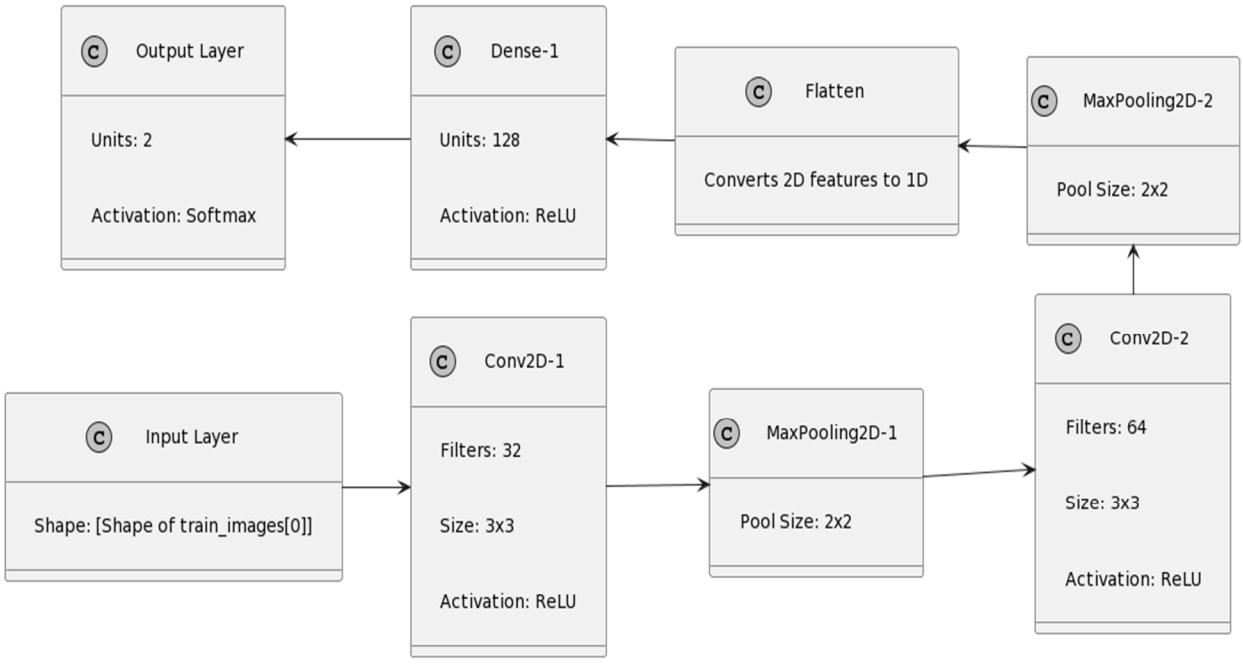

Рис. 2. Архітектура згорткової нейронної мережі для виявлення достовірності відбитків пальців

В архітектуру входять такі шари:

1. Вхідний шар приймає вхідні піксельні значення зображення як вхід. Форма: відповідає роздільній здатності зображень відбитків пальців, які обробляються. Для RGB (кольорових) зображень характерні розміри (висота, ширина) отримують через три кольорові канали (Червоний, Зелений, Синій). Якщо зображення в градаціях сірого, розміри (висота, ширина, 1) представляютьи один канал градацій сірого.

2. Конволюційний шар (Conv2D) сканує вхідне зображення за допомогою фільтрів/ядер, допомагаючи моделі вивчати локальні шаблони.

Кількість фільтрів: 32.

Розмір фільтра: 3×3.

Функція активації ReLU (Rectified Linear Unit) вводить нелінійність у модель, даючи їй змогу вчитися на помилках та вносити корективи, що важливо для вивчення складних шаблонів.

3. Шар максимального пулінгу (MaxPooling2D).

Для зниження просторових розмірностей вихідного об'єму. Використовується для зниження обчислювальної складності, даючи мережі змогу зосередитися на релевантніших шаблонах/ознаках.

Розмір пулу: 2×2.

4. Конволюційний шар (Conv2D) – це інша згорткова операція для видобування вищих ознак.

Кількість фільтрів: 64.

Розмір фільтра: 3×3.

Функція активації: ReLU.

5. Шар максимального пулінгу (MaxPooling2D). Зниження просторових розмірностей.

Розмір пулу: 2×2.

6. Шар стиснення (Flatten) сплющує виведення попередніх шарів у один довгий вектор. Це необхідно, тому що повністю з'єднані шари (щільні шари) очікують на 1D вхідний вектор.

7. Повністю з'єднаний шар (Dense). Інтерпретація особливостей та шаблонів, вивчених попередніми шарами.

Блоки (нейрони): 128.

Функція активації: ReLU.

8. Вихідний шар (Dense) передбачає виведення розподілу ймовірностей за класами (достовірним або імітаційним, як у нашому випадку).

Блоки (нейрони): 2, котрі відповідають двом класам: достовірному та імітаційному.

Функція активації Softmax. Ця функція активації повертає розподіл ймовірностей за класами, тобто кожен нейрон буде виводити значення між 0 та 1, що представляє ймовірність того, що вхідне зображення належить до його відповідного класу

Компіляція моделі

Оптимізатор Adam є алгоритмом оптимізації з адаптивною швидкістю навчання [16], який виявився ефективним у роботі з градієнтами на завданнях з шумом. Він поєднує переваги двох інших розширень стохастичного градієнтного спуску: AdaGrad і RMSProp.

Функція втрат – розріджена категоріальна крос-ентропія. Таку функцію втрат використовують для задач класифікації з багатьма класами, де мітки є цілими числами (на відміну від векторів, закодованих методом one-hot). Вона обчислює крос-ентропійні втрати між справжніми та передбаченими мітками.

Експеримент та результати

Для цього дослідження ми намагалися оцінити, наскільки ефективно нейронна мережа CNN розрізняє справжні та фальшиві відбитки пальців, за допомогою набору даних Socofing (див. табл. 1).

Таблиця 1

Метрики точності навчання та перевірки моделі для кожної епохи.

Епоха	Втрати	Точність	Втрати перевірки	Точність перевірки
1	0,1742	0,9260	0,1342	0,9378
2	0,0751	0,9694	0,0650	0,9761
3	0,0482	0,9813	0,0634	0,9755
4	0,0348	0,9866	0,0375	0,9860
5	0,0260	0,9905	0,0267	0,9910
6	0,0189	0,9931	0,0350	0,9869
7	0,0162	0,9940	0,0246	0,9919
8	0,0131	0,9952	0,0252	0,9935
9	0,0116	0,9958	0,0321	0,9923
10	0,0116	0,9959	0,0368	0,9896

Перед подаванням даних на CNN відбитка пальця виконували стандартні етапи попередньої обробки кожного зображення, які передбачали зміну розміру до узгодженого роздільної здатності, нормалізацію для масштабування значень пікселів між 0 та 1 і доповнення даних (наприклад, випадкові повороти та перевороти), щоб підвищити стійкість моделі [17, 18].

Вибрано архітектуру CNN, котра складалася з кількох згорткових, пулінгових та щільних шарів. Модель ініціалізовано з випадковими вагами.

Навчання здійснювалося з розміром пакета 2764 та протягом 10 епох. Ми виконували розбиття 80 % для навчання та 20 % для перевірки з набору даних. Використано оптимізатор Adam зі швидкістю навчання 0.001 та функцією втрат категоріальної крос-ентропії.

Протягом навчання ми спостерігали як за втратами навчання та перевірки, так і за точністю.

Збіжність кривих навчання та перевірки свідчить про мінімальне перенавчання. Модель добре узагальнює дані, які не брали участі в навчанні (див. рис. 3).

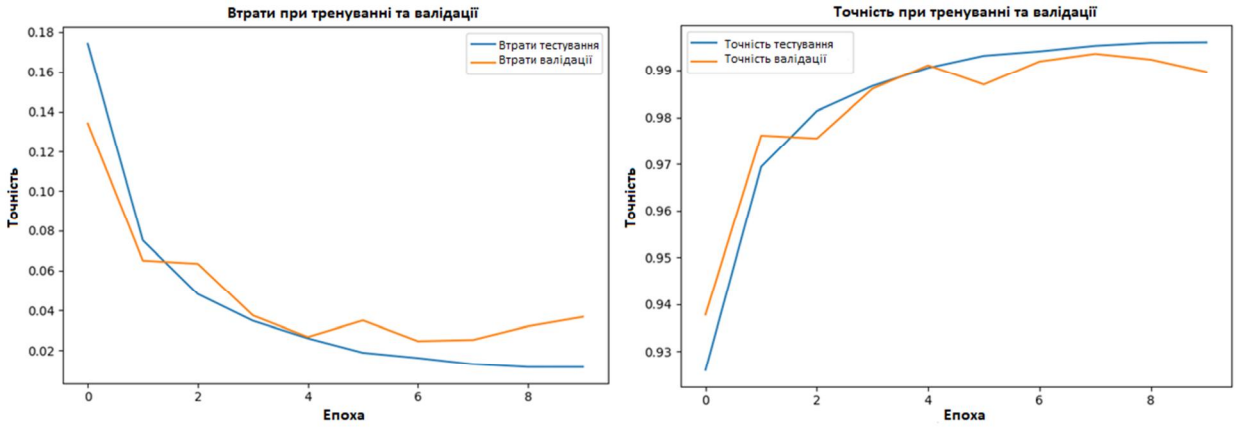

Рис. 3. Криві точності та втрат при навчанні та перевірці

Після завершення процесу навчання модель оцінено на тестовому наборі даних для вимірювання її ефективності:

- Точність (Accuracy): 98,964 %.
- Відсоток помилкового виявлення (ВПВ): 0,215 %.
- Відсоток помилкового пропускання (ВПП): 7,251 %.

Модель демонструє високий рівень точності, що свідчить про її здатність розрізняти справжні та симуляційні відбитки пальців. Однак ВПП свідчить про необхідність подальших оптимізацій, оскільки деякі справжні відбитки пальців класифіковано неправильно.

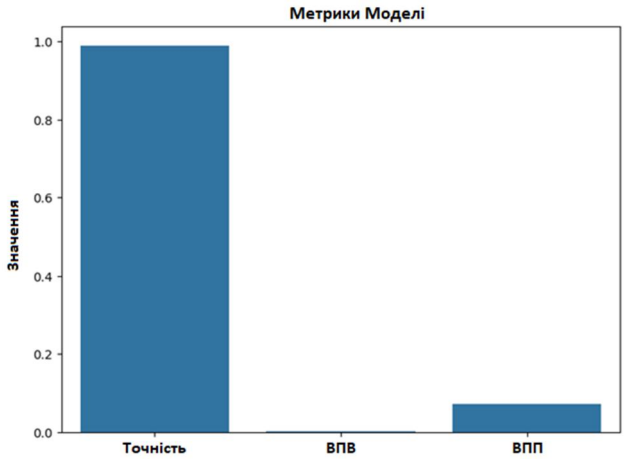

Рис. 4. Показники ефективності моделі виявлення справжності відбитків пальців, що демонструють точність (Accuracy), відсоток помилкового виявлення (ВПВ) та відсоток помилкового пропускання (ВПП)

Аналіз матриці помилок

На основі оцінки тестового набору даних матриця помилок була такою:

- Істинно позитивний (TP) – 2392.
- Хибно позитивний (TN) – 42.
- Істинно негативний (FP) – 19487.
- Хибно негативний (FN) – 187.

Хоча модель показала високий рівень істинних позитивів та істинних негативів, що свідчить про правильну класифікацію, були випадки як хибних позитивів, так і хибних негативів, які підкреслюють сфери для потенційного удосконалення моделі (рис.5).

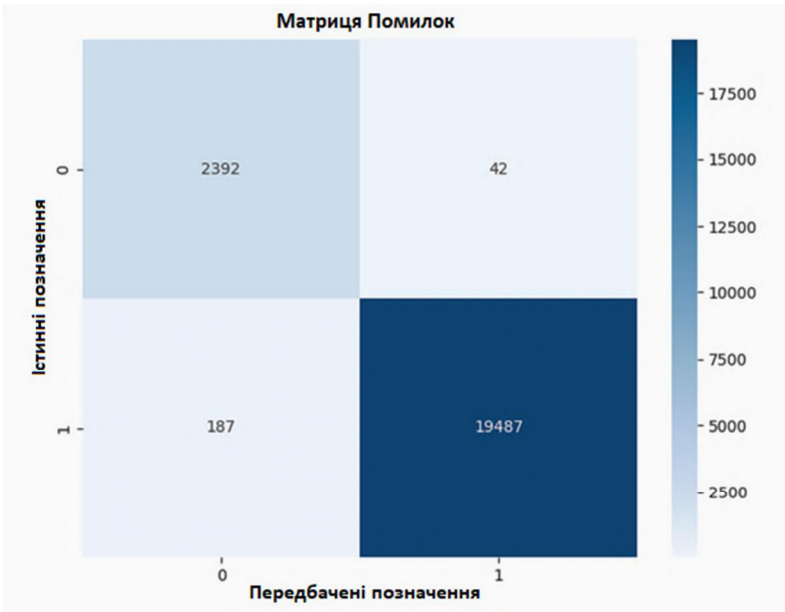

Рис. 5. Матриця помилок

У майбутніх дослідженнях необхідно розробляти:

- Гібридні моделі для комбінування переваг різних архітектур, наприклад, інтеграція особливостей з рекурентними нейронними мережами або автоенкодерів з CNN, можуть запропонувати покращену роботу.
- Використання попередньо навчених моделей на більших наборах даних для виявлення активності відбитків пальців.
- Такі техніки, як GAN, можуть генерувати синтетичні відбитки пальців для розширення набору даних та потенційного підвищення стійкості моделі.

Дискусія

Порівняно із роботою Al-Wajih et al. (2022)[19], де зосереджено увагу на класифікації типів відбитків пальців за допомогою CNN, наша модель показала здатність не лише класифікувати, але й ефективно відрізняти достовірні відбитки від імітованих із високою точністю. Це стало можливим завдяки глибшому навчанню та оптимізації мережі, зосереджених на виявленні тонких особливостей відбитків.

Порівняно з дослідженням Zong, Xu, і Yuan (2020)[20], яке використовує CNN для розпізнавання радіочастотних відбитків, наш підхід забезпечив ширший спектр застосування за рахунок адаптації до різноманітних сценаріїв ідентифікації. Важливо, що наша модель не тільки вдосконалює розпізнавання на основі візуальних даних, але й робить внесок у зростання загальної безпеки біометричних систем, підвищуючи стійкість до спроб обходу аутентифікації.

У висновках статті, яку опублікували Kothadiya et al. (2023) у Journal of Imaging[8], зазначено, що запропоноване дослідження використовує унікальний підхід на основі спрямування уваги на виявлення живості зображень відбитків пальців та їх розпізнавання як справжніх або фальшивих. Застосування архітектури ResNet50 з подвійною увагою досягло видатної точності на рівні 97,7 % на наборі даних LivDet для відбитків пальців, що демонструє вражаючі результати порівняно з іншими глибокими навчальними конволюційними моделями, такими як Xception, InceptionV3, VGG19, DenseNet121. Порівняно з результатами нашого експерименту, де ми досягли точності ідентифікації на рівні 98,964 %, результати Kothadiya et al. Підкреслюють значний потенціал глибокого навчання у вирішенні викликів, пов’язаних із виявленням живості відбитків пальців. Незважаючи на дещо нижчу точність порівняно з нашими результатами, запропонований підхід до виявлення достовірності з використанням подвійної уваги в архітектурі ResNet50 є новаторським та обіцяє значні переваги в точності та надійності систем біометричної ідентифікації. Обидва дослідження демонструють, як інноваційне застосування глибокого навчання та архітектур уваги може істотно покращити здатність біометричних систем точно визначати автентичність відбитків пальців, що відкриває нові можливості подальшого розвитку в цій галузі.

Висновки

У ході дослідження ми глибоко проаналізували методи біометричної ідентифікації особи за відбитками пальців та виявили потенційні напрями підвищення точності та безпеки цих систем. Важливою частиною роботи став огляд сучасних підходів і досліджень у цій сфері, що дало змогу визначити ключові проблеми та виклики, які постають перед науковою спільнотою.

Основним досягненням дослідження є розроблення та впровадження нової архітектури згорткової нейронної мережі (CNN), спеціально адаптованої для задачі ідентифікації відбитків пальців. Ця модель продемонструвала високу точність у виявленні достовірних та імітаційних

відбитків. Досягнуто 98,964 % точності на тестовому наборі даних, що значно перевершує результати більшості інших рішень.

На особливу увагу заслуговує низький відсоток помилкового виявлення (ВПВ) – 0,215 % та відсоток помилкового пропускання (ВПП) 7,251 %, що свідчить про високу специфічність та чутливість розробленої моделі. Матриця помилок додатково підтверджує здатність системи ефективно розрізняти достовірні та підроблені відбитки пальців, висвітлюючи потенціал її застосування у реальних системах безпеки.

Виконаний огляд різних підходів підкреслив значення упровадження інновацій у технології біометричної ідентифікації. Дослідження показало, що інтеграція глибокого навчання та розроблення спеціалізованих архітектур можуть істотно підвищити точність та безпеку біометричних систем. Використання згорткових нейронних мереж відкриває нові можливості для подолання викликів, пов'язаних із підробкою відбитків пальців, та забезпечує надійне рішення для ідентифікації особи.

Це дослідження становить важливий крок у розвитку біометричних технологій, пропонуючи ефективні інструменти для боротьби із потенційними загрозами безпеки. Продовження роботи в цьому напрямі обіцяє подальше вдосконалення систем аутентифікації, зробивши їх ще точнішими, безпечнішими та надійнішими.

Список літератури

1. Shehu, Y. I., Ruiz-Garcia, A., Palade, V., & James, A. (2018). Sokoto coventry fingerprint dataset. arXiv preprint. https://doi.org/10.48550/arXiv.1807.10609

2. Skoryk, Y., & Bezruk, V. (2023). Вибір переважного методу біометричної автентифікації. International Science Journal of Engineering & Agriculture, 2(4), 28–34. https://doi.org/10.46299/j.isjea.20230204

3. Салієва, О. В., Зоря, І. С., Бондаренко, І. О., & Берестенко, М. О. (2023). Підвищення достовірності автентифікації користувача на основі захищеного електронного ключа та поведінкової біометрії. Вісник Вінницького політехнічного інституту, (2), 102–111. https://doi.org/10.31649/1997-9266-2023-167-2-102-111

4. Пуріш, С. В., Яковенко, Р. О., & Годовиченко, М. А. (2023). Задача вибору біометричних ознак в системах біометричної ідентифікації людини. In Сучасні інформаційні технології –2023=Modern Information Technology–2023 (pp. 11–13). Retrieved from http://dspace.op.edu.ua/jspui/bitstream/123456789/14147/1/MIT2023-Пуріш.pdf

5. Цимбал, В. В. (2023). Використання біометричних методів аутентифікації для забезпечення високого рівня безпеки в телекомунікаційних системах. In Інформаційні моделюючі технології, системи та комплекси (ІМТСК-2023): IV міжнародна науково-практична конференція. Черкаси: Черкаський національний університет імені Богдана Хмельницького. Retrieved from https://fotius.cdu.edu.ua/wp-content/uploads/2023/06/Book_IMTCK_2023.pdf

6. Андрушків, В. В., & Порохняк, О. З. (2023). Розробка та дослідження автоматизованої системи ідентифікації особи по відбитках пальців (Master's thesis, Тернопіль, ТНТУ). Retrieved from https://elartu.tntu.edu.ua/handle/lib/43265

7. Alzubaidi, L., Zhang, J., Humaidi, A. J., et al. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data, 8, 53. https://doi.org/10.1186/s40537-021-00444-8

8. Kothadiya, D., Bhatt, C., Soni, D., Gadhe, K., Patel, S., Bruno, A., & Mazzeo, P. L. (2023). Enhancing fingerprint liveness detection accuracy using deep learning: A comprehensive study and novel approach. Journal of Imaging, 9(8), 158. https://doi.org/10.3390/jimaging9080158

9. Джаноянц, В. О. (2023). Спосіб розпізнавання емоційних станів у зображеннях людини. (Master's thesis, КПІ ім. Ігоря Сікорського). Retrieved from https://ela.kpi.ua/server/api/core/bitstreams/e5b27ff3-bcfc-418d-a3a3-3a15e545784d/content

10. Liu, J., Wang, X., Wu, S., Wan, L., & Xie, F. (2023). Wind turbine fault detection based on deep residual networks. Expert Systems with Applications, 213, 119102. https://doi.org/10.1016/j.eswa.2022.119102

11. Dong, Y., Jiang, Z., Tao, F., & Fu, Z. (2023). Multiple spatial residual network for object detection. Complex & Intelligent Systems, 9(2), 1347–1362. https://doi.org/10.1007/s40747-022-00859-7

12. Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. Artificial Intelligence Review. https://doi.org/10.48550/arXiv.1912.00271

13. Sun, Y., Tang, Y., & Chen, X. (2023). A neural network-based partial fingerprint image identification method for crime scenes. Applied Sciences, 13(2), 1188. https://doi.org/10.3390/app13021188

14. Яковенко, О. О., Кушніренко, Н. І., Дорофєєва, І. С., & Євтушенко, А. Р. (2019). Розробка системи розпізнавання осіб на основі згорткової нейронної мережі. Інформатика та математичні методи в моделюванні, 9(№ 1–2), 77–87. Retrieved from http://nbuv.gov.ua/UJRN/Itmm_2019_9_1-2_10

15. Milner, R. (1997). The definition of standard ML: revised. MIT Press. https://doi.org/10.7551/mitpress/2319.003.0001

16. Gustisyaf, A. I., & Sinaga, A. (2021). Implementation of convolutional neural network to classification gender based on fingerprint. International Journal of Modern Education & Computer Science, 13(4). DOI: 10.5815/ijmecs.2021.04.05

17. Nazarkevych, M., Logoyda, M., Dmytruk, S., & Voznyi, Y. (2019). Identification of biometric images using latent elements. CEUR Workshop Proceedings. Retrieved from https://ceur-ws.org/Vol-2488/paper8.pdf

18. Nazarkevych, M., & Nazarkevych, H. (2019). Ateb-Gabor filtering method in fingerprint recognition. Procedia Computer Science, 160, 30–37. https://doi.org/10.1016/j.procs.2019.09.440

19. Al-Wajih, Y., Hamanah, W. M., Abido, M. A., Al-Sunni, F., & Alwajih, F. (2022). Finger type classification with deep convolution neural networks. Retrieved from https://www.scitepress.org/PublishedPapers/2022/113271/113271.pdf

20. Zong, L., Xu, C., & Yuan, H. (2020). A RF fingerprint recognition method based on deeply convolutional neural network. In 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China (pp. 1778–1781). DOI: 10.1109/ITOEC49072.2020.9141877

References

1. Shehu, Y. I., Ruiz-Garcia, A., Palade, V., & James, A. (2018). Sokoto coventry fingerprint dataset. arXiv preprint. https://doi.org/10.48550/arXiv.1807.10609

2. Skoryk, Y., & Bezruk, V. (2023). Selection of the preferred method of biometric authentication. International Science Journal of Engineering & Agriculture, 2(4), 28–34. https://doi.org/10.46299/j.isjea.20230204

3. Salieva, O. V., Zorya, I. S., Bondarenko, I. O., & Berestenko, M. O. (2023). Enhancing the reliability of user authentication based on a secure electronic key and behavioral biometrics. Bulletin of Vinnytsia Polytechnic Institute, (2), 102–111. https://doi.org/10.31649/1997-9266-2023-167-2-102-111

4. Purish, S. V., Yakovenko, R. O., & Godovychnenko, M. A. (2023). The task of selecting biometric characteristics in human biometric identification systems. In Modern Information Technologies–2023 (pp. 11–13). Retrieved from http://dspace.op.edu.ua/jspui/bitstream/123456789/14147/1/MIT2023-Пуріш.pdf

5. Tsymbal, V. V. (2023). Using biometric authentication methods to ensure a high level of security in telecommunications systems. In Information Modeling Technologies, Systems and Complexes (IMTSC-2023): IV International Scientific and Practical Conference. Cherkasy: Bohdan Khmelnytsky National University of Cherkasy. Retrieved from https://fotius.cdu.edu.ua/wp-content/uploads/2023/06/Book_IMTCK_2023.pdf

6. Andrushkiv, V. V., & Porokhniak, O. Z. (2023). Development and research of an automated system for personal identification by fingerprints (Master's thesis, Ternopil, TNTU). Retrieved from https://elartu.tntu.edu.ua/handle/lib/43265

7. Alzubaidi, L., Zhang, J., Humaidi, A. J., et al. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data, 8, 53. https://doi.org/10.1186/s40537-021-00444-8

8. Kothadiya, D., Bhatt, C., Soni, D., Gadhe, K., Patel, S., Bruno, A., & Mazzeo, P. L. (2023). Enhancing fingerprint liveness detection accuracy using deep learning: A comprehensive study and novel approach. Journal of Imaging, 9(8), 158. https://doi.org/10.3390/jimaging9080158

9. Dzhanoiants, V. O. (2023). A method for recognizing emotional states in human images (Master's thesis, Kyiv Polytechnic Institute named after Igor Sikorsky). Retrieved from https://ela.kpi.ua/server/api/core/bitstreams/e5b27ff3-bcfc-418d-a3a3-3a15e545784d/content

10. Liu, J., Wang, X., Wu, S., Wan, L., & Xie, F. (2023). Wind turbine fault detection based on deep residual networks. Expert Systems with Applications, 213, 119102. https://doi.org/10.1016/j.eswa.2022.119102

11. Dong, Y., Jiang, Z., Tao, F., & Fu, Z. (2023). Multiple spatial residual network for object detection. Complex & Intelligent Systems, 9(2), 1347–1362. https://doi.org/10.1007/s40747-022-00859-7

12. Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. Artificial Intelligence Review. https://doi.org/10.48550/arXiv.1912.00271

13. Sun, Y., Tang, Y., & Chen, X. (2023). A neural network-based partial fingerprint image identification method for crime scenes. Applied Sciences, 13(2), 1188. https://doi.org/10.3390/app13021188

14. Yakovenko, O. O., Kushnirenko, N. I., Dorofeieva, I. S., & Yevtushenko, A. R. (2019). Development of a face recognition system based on a convolutional neural network. Informatics and Mathematical Methods in Modeling, 9(№ 1-2), 77-87. Retrieved from http://nbuv.gov.ua/UJRN/Itmm_2019_9_1-2_10

15. Milner, R. (1997). The definition of standard ML: Revised. MIT Press. https://doi.org/10.7551/mitpress/2319.003.0001

16. Gustisyaf, A. I., & Sinaga, A. (2021). Implementation of convolutional neural network to classification gender based on fingerprint. International Journal of Modern Education & Computer Science, 13(4). DOI: 10.5815/ijmecs.2021.04.05

17. Nazarkevych, M., Logoyda, M., Dmytruk, S., & Voznyi, Y. (2019). Identification of biometric images using latent elements. CEUR Workshop Proceedings. Retrieved from https://ceur-ws.org/Vol-2488/paper8.pdf

18. Nazarkevych, M., & Nazarkevych, H. (2019). Ateb-Gabor filtering method in fingerprint recognition. Procedia Computer Science, 160, 30–37. https://doi.org/10.1016/j.procs.2019.09.440

19. Al-Wajih, Y., Hamanah, W. M., Abido, M. A., Al-Sunni, F., & Alwajih, F. (2022). Finger type classification with deep convolution neural networks. Retrieved from https://www.scitepress.org/PublishedPapers/2022/113271/113271.pdf

20. Zong, L., Xu, C., & Yuan, H. (2020). A RF fingerprint recognition method based on deeply convolutional neural network. In 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China (pp. 1778–1781). DOI: 10.1109/ITOEC49072.2020.9141877

FINGERPRINT IDENTIFICATION METHOD BASED ON CONVULSIONAL NEURAL NETWORKS

Yurii Myshkovskyi[1] and Mariia Nazarkevych[2]

[1, 2] Lviv Polytechnic National University,
Information Systems and Networks Department, Lviv, Ukraine,
[1] E-mail: yurii.i.myshkovskyi@lpnu.ua, ORCID: 0009-0004-0051-026X
[2] E-mail: mariia.a.nazarkevych@lpnu.ua, ORCID: 0000-0002-6528-9867

The article presents an advanced method of fingerprint identification based on convolutional neural network (CNN) technology. This work elaborately describes the development and implementation process of a specialized CNN architecture for detecting and verifying the authenticity of fingerprints. Utilizing the comprehensive Socofing dataset allowed for an in-depth analysis of the model's ability to distinguish between genuine and fabricated fingerprints, where the model demonstrated impressive accuracy – up to 98.964 %. Special attention is given to error analysis, including the false discovery and omission rates, pointing towards potential directions

for further improvement. Besides highlighting the technical aspects and high identification accuracy, the article also addresses potential challenges and limitations that the method might encounter. This includes issues related to the imbalance and diversity of data in the Socofing set, as well as limitations associated with computational resources when training deep neural networks. Potential pathways for model optimization are discussed, particularly focusing on reducing the false omission rate, which could improve user experience in authentication. The concluding section of the article emphasizes the importance of the presented work for the security sector, where precise authentication of fingerprint images is critically needed. The obtained results can be considered a solid foundation for future scientific developments in this direction. Additionally, the need for systematic updates and modifications of the model is highlighted to adapt it to continually improved imitation techniques, ensuring its long-term relevance and effectiveness.

Key words: fingerprints; convolutional neural networks (CNN); biometric authentication; forgeries.