Issue 15, 2024

https://doi.org/10.23939/sisn2024.15.023

УДК 004.9

РЕАЛІЗАЦІЯ НАДІЙНОЇ ТА ЕФЕКТИВНОЇ АВТЕНТИФІКАЦІЇ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ ШЛЯХОМ ВИКОРИСТАННЯ МЕТОДІВ ВІЗУАЛЬНОЇ БІОМЕТРИКИ

Тарас Батюк[1], Дмитро Досин[2]

Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж, Львів, Україна
[1] E-mail: taras.m.batiuk@lpnu.ua, ORCID: 0000-0001-5797-594X
[2] E-mail: dmytro.h.dosyn@lpnu.ua, ORCID: 0000-0003-4040-4467

Основна мета цієї статті – розгляд аспектів забезпечення безпеки та підвищення ефективності процесу автентифікації в інтелектуальних системах за допомогою візуальної біометрики. Дослідження спрямоване на розроблення та вдосконалення систем автентифікації з використанням передових методів біометричної ідентифікації. Створено інтелектуальну систему, яка з використанням сіамської нейронної мережі забезпечує безпечну автентифікацію користувачів поточної системи. Окрім реалізації базових засобів захисту у вигляді хешування і збереження користувацьких логіну і пароля, в наш час важлива реалізація двофакторної автентифікації, яка істотно посилює захист користувацьких даних і унеможливлює більшість сучасних способів злому та викрадення даних користувачів. Двофакторну автентифікацію реалізовано у вигляді технології пошуку, розпізнавання та порівняння обличчя користувачів системи, оскільки візуальна біометрика безпечніша за інші види двофакторної автентифікації. Розглянуто різні варіанти реалізації сіамської нейронної мережі за допомогою функцій Contrastive loss function та Triplet loss function і, відповідно, реалізовано та навчено нейронну мережу із використанням функції Triplet loss. Після навчання та перевірки правильності роботи нейронної мережі її було інтегровано до інтелектуальної системи, завдяки чому створено ефективний спосіб розпізнавання обличчя користувача системи, збереження отриманої інформації в базі даних та подальшого порівняння поточного користувача зі збереженим обличчям під час автентифікації. В результаті було створено надійну та захищену інтелектуальну систему, що мінімізує ризик несанкціонованого доступу до користувацького акаунту і використовує ефективний та сучасний спосіб автентифікації користувачів.

Ключові слова: двофакторна автентифікація; сіамська нейронна мережа; Triplet Loss Function; візуальна біометрика; технології розпізнавання обличчя.

Вступ

У зв'язку зі стрімким розвитком та впровадженням інтелектуальних систем аспекти безпеки та ефективності процесу автентифікації стають особливо актуальними та важливими завданнями. Стаття спрямована на вирішення цих проблем за допомогою розроблення та вдосконалення систем автентифікації із використанням передових методів візуальної біометрики та сучасних підходів до мережевого навчання. Ключовою метою цієї роботи є створення інтелектуальної системи, основаної на сіамській нейронній мережі, для забезпечення безпечної автентифікації користувачів. Окрім застосування базових

методів захисту, таких як хешування та зберігання логінів та паролів, необхідно розглянути та реалізувати двофакторну автентифікацію з використанням технології розпізнавання обличчя. Це істотно підвищує рівень безпеки та унеможливлює застосування багатьох сучасних методів злому.

Мета роботи – вдосконалення систем автентифікації в інтелектуальних системах за допомогою візуальної біометрики. Розглянуто та реалізовано передові методи автентифікації, зокрема, двофакторну систему з використанням технології розпізнавання обличчя на основі сіамської нейронної мережі. Робота націлена на створення надійної, безпечної та ефективної інтелектуальної системи, яка мінімізує ризик несанкціонованого доступу та забезпечує високий рівень захисту користувацьких акаунтів. Розуміючи загалом, що саме необхідно, в межах роботи здійснено поділ мети на декілька основних завдань. Основне завдання – створення та навчання моделі для розпізнавання обличчя за допомогою технології сіамської нейронної мережі. Насамперед варто обґрунтувати вибір сіамської нейронної мережі. Нейронну мережу використовують завдяки її здатності ефективно порівнювати два об'єкти та створювати векторні подання для порівняння. Це особливо важливо для завдань біометричної ідентифікації. Архітектурно сіамська нейронна мережа складається із двох гілок мережі, які спільно навчаються, приймають два вхідні зображення та генерують векторні представлення обличчя користувача системи. Функція втрат Triplet Loss дає змогу навчати мережу так, щоб векторні подання для одного користувача були близькими, а для різних користувачів – віддаленими.

Навчання та оптимізація теж відіграють важливу роль у використанні набору даних, що містить пари зображень обличчя для тренування та тестування, які необхідно оптимізувати для адаптації ваг моделі під час навчання. Отримавши навчену модель, необхідно використати окремий набір даних для валідації її ефективності та визначення точності розпізнавання обличчя та якості отриманих векторних представлень. Для успішної імплементації двофакторної автентифікації, зосереджуючись на технології пошуку, розпізнавання та порівняння обличчя користувачів, потрібно врахувати кілька ключових етапів та деталей. Необхідно визначити конкретні вимоги до безпеки та швидкості системи, вибрати технологію розпізнавання обличчя для реалізації другого етапу двофакторної автентифікації. Знаючи вибрану технологію, варто створити механізм пошуку, розпізнавання та порівняння обличчя, інтегруючи його із розробленою сіамською нейронною мережею. Важлива частина роботи – реалізація двофакторної автентифікації, де перший фактор – логін та пароль поточного користувача системи, а другий – розпізнавання обличчя.

Об'єктом дослідження в цій роботі є комплексний процес автентифікації в інтелектуальних системах із використанням візуальної біометрики, зокрема розпізнавання обличчя, та імплементації сіамської нейронної мережі. Виконано аналіз та розроблення методів, спрямованих на забезпечення безпеки та підвищення ефективності автентифікаційного процесу. Предметом дослідження є також двофакторна автентифікація, яка використовує технологію пошуку, розпізнавання та порівняння облич користувачів системи. Детально розглянуто використання візуальної біометрики як безпечнішого методу порівняно з іншими видами двофакторної автентифікації. Предметом дослідження є також сама сіамська нейронна мережа, зокрема варіації її реалізації за допомогою функцій Contrastive Loss та Triplet Loss. Основну увагу приділено розробленню, навчанню та інтеграції цієї мережі в інтелектуальну систему для забезпечення надійної автентифікації користувачів.

Предметом дослідження є система автентифікації в інтелектуальних системах, спрямована на захист інформації та забезпечення високої ефективності користувачів. У межах статті конкретизовано дослідження методів автентифікації, зокрема використання візуальної біометрики, такої як розпізнавання обличчя, та сіамської нейронної мережі для досягнення двофакторної автентифікації. Об'єкт дослідження розширено на розроблення та оптимізацію інтелектуальної системи, яка охоплює етапи опрацювання та збереження користувацьких даних, розпізнавання обличчя з використанням сіамської нейронної мережі, впровадження двофакторної автентифікації через технологію пошуку та порівняння облич користувачів. Об'єктом дослідження є ефективність та безпека цієї системи,

зокрема застосування функцій Contrastive Loss та Triplet Loss для реалізації сіамської нейронної мережі, а також оцінка впливу цієї системи на мінімізацію ризику несанкціонованого доступу до користувацького акаунту.

Інтелектуальна система, реалізована в цій науковій роботі, імплементує наукову новизну через вдосконалення та поєднання передових методів біометричної ідентифікації та машинного навчання. Однією з ключових інновацій є використання сіамської нейронної мережі для розпізнавання обличчя. Цей підхід дає змогу враховувати унікальні риси кожного користувача, забезпечуючи високу точність ідентифікації. Реалізація та тренування нейронної мережі з використанням Triplet Loss Function є інноваційним кроком у напрямі вдосконалення біометричних методів. Інтеграція технології пошуку, розпізнавання та порівняння облич як складової двофакторної автентифікації є додатковим нововведенням. У науковій роботі також приділено увагу оптимізації методів біометричної ідентифікації з використанням передових алгоритмів та методів, що сприяє підвищенню точності та ефективності розпізнавання обличчя. Інтеграція всіх етапів, ураховуючи розроблення нейронної мережі, імплементацію двофакторної автентифікації, оптимізацію біометричної ідентифікації та інші, в єдину інтелектуальну систему – новаторський підхід до вирішення проблем безпеки та автентифікації в інтелектуальних системах. Цей комплексний науковий підхід спрямований на створення ефективної та надійної системи, яка може мінімізувати ризик несанкціонованого доступу та забезпечити високий рівень безпеки користувачів.

Аналіз останніх досліджень та публікацій

У статті [1] зроблено важливий внесок у сферу кібербезпеки та автоматизованого виявлення вразливостей. Автори пропонують використовувати графові нейронні мережі для автоматичного присвоєння ідентифікаторів Common Weakness Enumeration вразливостей. Однією з ключових переваг статті є застосування графових нейронних мереж, що дає змогу моделі ефективно аналізувати взаємозв'язки між різними вразливостями та їх характеристиками. Використання графових структур може покращити якість ідентифікації та класифікації вразливостей. Добре викладений огляд різних методів виявлення вразливостей та присвоєння ідентифікаторів CWE свідчить про глибоке розуміння предметної області авторів. Пропозиція використання графових нейронних мереж у контексті цього завдання є оригінальною та перспективною. Однак бажано докладніше обговорити обмеження та можливі ризики використання запропонованого підходу. Додаткові деталі щодо вибраних параметрів графових нейронних мереж, методів навчання та валідації також покращать розуміння читача щодо стабільності та надійності моделі. Стаття представляє інноваційний підхід до проблеми виявлення вразливостей та автоматизованого присвоєння ідентифікаторів CWE.

В роботі [2] запропоновано новаторський підхід до розроблення інтелектуальної системи для соціалізації з урахуванням особистих інтересів на основі технологій SEO та методів машинного навчання. Позитивними аспектами статті є впровадження ідеї використання SEO технологій у контексті соціальної платформи для взаємодії користувачів між собою. Використання методів машинного навчання для аналізу та рекомендацій стосовно особистих інтересів також свідчить про високий рівень технічної компетентності авторів. Ілюстративний огляд проблем та визначення бази для розроблення інтелектуальної системи розширюють можливість використання SEO технологій.

Автори в статті [3] описали застосування Siamese Trackers на основі глибоких ознак для завдання візуального відстеження. Дослідники висвітлюють важливі аспекти використання глибоких ознак та моделей Siamese для підвищення точності та ефективності відстеження об'єктів у відеопотоці. Переваги статті – чітке формулювання проблеми та доцільність вибору Siamese Trackers для вирішення завдань візуального відстеження. Особливу увагу потрібно звернути на обґрунтування використання глибоких ознак, що дають змогу досягти високої точності відстеження об'єктів у варіативних умовах. Автори ретельно розглядають різні аспекти реалізації Siamese Trackers, такі як архітектура глибоких мереж, функції втрат та методи оновлення моделі. Це робить статтю корисною для дослідників та практиків, які цікавляться удосконаленням технологій візуального відстеження об'єктів. Насамкінець зазначимо, що стаття може стати ще ціннішою, якщо подальші дослідження будуть спрямовані на порівняння Siamese

Trackers [4] із сучасними методами візуального відстеження та їх ефективності у різних умовах. Ця робота є вагомим внеском у сферу візуального відстеження, де використання Siamese Trackers та глибоких ознак може покращити результати в реальних умовах відстеження об'єктів.

У статті [5] розглянуто важливий аспект використання сіамських нейронних мереж у завданнях регресії та кількісного визначення невизначеності. Автори пропонують новий підхід до підвищення ефективності сіамських нейронних мереж із використанням парування на основі схожості. Однією з ключових переваг цієї роботи є вдале використання ідеї подібності для підвищення точності та надійності сіамських нейронних мереж у завданнях регресії. Автори проаналізували вплив різних методів парування на результати та продемонстрували, що подібність-основане парування сприяє підвищенню ефективності нейронних мереж. Додатковою перевагою є те, що автори вивчають використання сіамських нейронних мереж для кількісного визначення невизначеності, що є актуальним напрямом дослідження. Вони подають цікаві результати і вказують на можливості використання подібності для підвищення надійності оцінювання невизначеності в регресійних задачах. Стаття пропонує нові підходи розвитку методології використання сіамських нейронних мереж у задачах регресії та кількісного визначення невизначеності, а подібність-основане парування представляє ефективний підхід до збільшення їх ефективності.

Автори статті [6] запропонували інноваційний підхід до виявлення клонів у Java-коді, використовуючи сіамську нейронну мережу на основі байт-коду. Автори ретельно досліджують проблему виявлення клонів у програмному забезпеченні, що є актуальним завданням у галузі розроблення програмного забезпечення та обслуговування. Однією з ключових переваг цієї роботи є використання байт-коду для представлення Java-коду та застосування сіамської нейронної мережі для визначення схожості між частинами коду. Це дає змогу враховувати структурні та семантичні аспекти клонів, що може збільшити точність виявлення. Додатковою перевагою є впровадження методу сіамських нейронних мереж для порівняння байт-коду, що може допомогти в ідентифікації складніших форм клонів, таких як змінені клони, які нелегко виявити за допомогою традиційних методів. Робота також надає докладний огляд сучасних методів виявлення клонів, порівняння їх переваг та недоліків, що робить її корисною для читачів, які орієнтуються в цьому полі. Загальна структура та подання матеріалу в роботі є чіткими та логічними, що покращує розуміння реалізованої методології. Чітко визначені етапи експерименту та отримані результати додають вагомості доведенням ефективності запропонованого методу. Стаття [7] висвітлює перспективний підхід до виявлення клонів у Java-коді, використовуючи сіамські нейронні мережі на основі байт-коду, і є важливим внеском у галузь аналізу програмного забезпечення.

У статті [8] проаналізовано проблему візуального відстеження об'єктів та запропоновано ефективний і легкий метод, на основі використання підходу диференційованого пошуку нейроархітектури. Робота зосереджена на досягненні високої ефективності відстеження за обмежених обчислювальних ресурсів. Однією з ключових переваг цієї роботи є використання методу DNAS із метою автоматичного пошуку оптимальної нейроархітектури для завдання візуального відстеження. Це дає змогу автоматизувати процес вибору оптимальної моделі, що важливо для досягнення високої ефективності за обмежених ресурсів. Стаття [9] детально описує процес диференційованого пошуку нейроархітектури та підходи до забезпечення легкості моделі для забезпечення високої швидкодії в реальному часі. Автори впроваджують ефективні механізми для зменшення обсягу та обчислювальної складності моделі, що робить її придатною для використання в змінних умовах. Досягнуті результати вказують на високий рівень ефективності та швидкодії пропонованого методу порівняно з іншими підходами візуального відстеження. Експерименти додатково підтверджують конкурентоспроможність розробленої моделі.

Автори статті [10] описали розроблення ефективної системи рекомендацій з урахуванням взаємності та популярності. Автори пропонують використання Siamese Bi-Directional Gated Recurrent Units network для досягнення цієї мети. Однією з ключових переваг цієї роботи є використання Siamese Bi-GRU network для моделювання взаємності між користувачами та об'єктами, враховуючи їхні взаємодії в часі. Це дає змогу враховувати динаміку відносин між користувачами та об'єктами, що важливо у

контексті рекомендаційних систем. Стаття містить чітке описання використаних методів та моделей, зокрема, Siamese Bi-GRU network, що полегшує розуміння читачеві. Детальний аналіз результатів експериментів та порівняння з іншими підходами підтверджують ефективність запропонованої моделі в умовах рекомендаційних систем. Окрім того, у роботі розглянуто урахування популярності об'єктів під час надання рекомендацій, що підвищує реалізм та актуальність рекомендаційної системи.

У статті [11] розглянуто проблему виявлення різноманітних патернів дихання на основі неперервних сигналів дихання людини за допомогою одновимірної штучної нейронної мережі та методу класифікації для кожного типу дихання. Автори пропонують новий підхід, спрямований на розширення можливостей виявлення та класифікації різноманітних зразків дихання. Одна із суттєвих переваг статті полягає у використанні одновимірної штучної нейронної мережі, що може ефективно обробляти послідовності сигналів дихання. Упровадження класифікаційного методу для різних типів дихання дає змогу отримати деталізовану інформацію та підвищити точність визначення конкретного патерна. Експериментальні результати вказують на високу точність виявлення та класифікації різних патернів дихання. Автори також детально обґрунтовують [12] використані методи та алгоритми, що сприяє загальному зрозумінню механізму роботи системи.

Формулювання цілі статті

У ході роботи необхідно вибрати основну функцію підрахунку втрат, базовим варіантом використання є функція контрастних втрат (Contrastive Loss Function) [14], яку в сіамській нейронній мережі застосовують для навчання моделі на парах вхідних зразків. Основна мета полягає в тому, щоб зближувати векторні представлення подібних зразків і віддаляти векторні представлення відмінних зразків. Функція контрастних втрат визначає втрати для пар зображень у такий спосіб, щоб вони були мінімізовані, якщо зображення подібні, і максимізувалися, якщо відмінні. Зазвичай вона використовує поняття "позитивних" та "негативних" пар, де позитивні пари складаються з однакових або подібних зразків, а негативні пари – із відмінних. Функцію контрастних втрат можна визначити різними способами, але один із популярних варіантів – використання евклідової відстані між векторними представленнями зображень [15]. Зазвичай втрати для позитивних пар намагаються зробити евклідову відстань якнайменшою, а для негативних пар – якнайбільшою, забезпечуючи цим ефективне навчання для векторних представлень. Функцію контрастних втрат визначають за формулою (1), де D_w визначають як евклідову відстань між виходами суміжних нейронних мереж, яку підраховують за (2):

$$Loss\ (P,N) = (1-Y)\frac{1}{2}(D_w)^2 + (Y)\frac{1}{2}\{\max(0, m - D_w)\}^2, \quad (1)$$

$$D_w = \sqrt{\{G_w(X_1) - G_w(X_2)\}^2}. \quad (2)$$

Функція контрастних втрат має деякі недоліки, які варто врахувати. Це чутливість до гіперпараметрів, тобто ефективність функції контрастних втрат може залежати від гіперпараметрів, таких як відстань між позитивними та негативними зразками, яка потребує уважного налаштування. Для ефективного навчання функції контрастних втрат необхідний деякий баланс між позитивними та негативними парами, що іноді складно забезпечити в реальних даних. Результати функції контрастних втрат може істотно змінити якість векторних представлень, які надає модель. Якщо модель неефективно вивчає корисні ознаки, то і результати функції втрат можуть бути неадекватними. У разі великої кількості класів важко підібрати ефективні пари для порівняння, що може призвести до менш ефективного навчання. Отже, для ефективної роботи варто використовувати сучаснішу функцію, таку як триплетна функція втрат (*Triplet loss function* [16]) – це один із видів функцій втрат, який часто використовують у сіамських нейронних мережах для навчання моделей порівнянню об'єктів у векторному просторі. Основна ідея триплетної втрати полягає в тому, щоб забезпечити розташування векторних представлень схожих об'єктів близько один до одного, тоді як векторні представлення різних об'єктів мають бути відокремлені в просторі.

Функція втрати має три зразки: як позитивний, так і негативний зразок для конкретного об'єкта, а також негативний зразок для іншого об'єкта (тривіально негативний). Мета полягає в тому, щоб зменшити відстань між векторними представленнями позитивного та якірного (тривіаль-

но негативного) зразка і, водночас, збільшити відстань між векторними представленнями якірного та складного негативного зразка. На рис. 1 зображено концептуальну модель роботи триплетної функції втрат, яка містить ключовий ввід [17] (якірний), а також позитивний і негативний об'єкти на вході. На рис. 2 подано модель сіамської нейронної мережі з доданою триплетною функцією втрат.

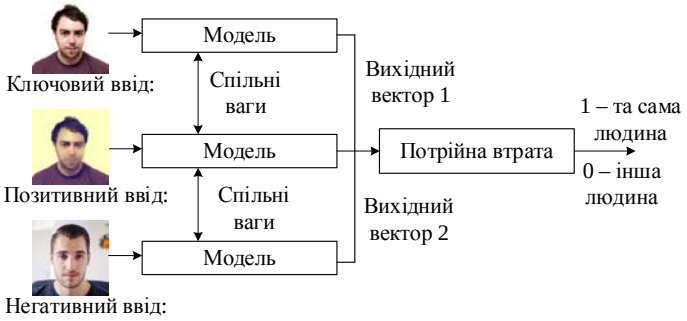

Рис. 1. Концептуальна модель роботи триплетної функції втрат

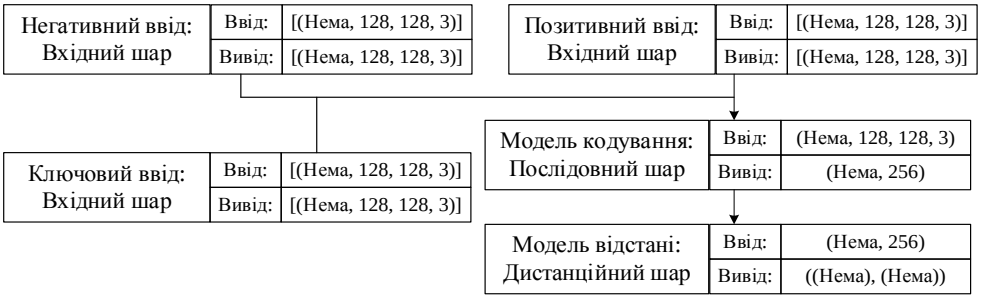

Рис. 2. Модель сіамської нейронної мережі з доданою триплетною функцією втрат

Отримані вектори передаються на рівень відстані, де обчислюється відстань між парами (прив'язка, додатний) та (прив'язка, від'ємний). У цьому контексті ми використовуємо спеціальний шар для обчислення відстані між поточними векторами ознак [18]. Цей шар враховує відстань між векторами та генерує відповідь, яка стає основою для подальших кроків, таких як навчання моделі для забезпечення ефективного порівняння об'єктів. Підрахунок векторів негативного і позитивного зразків наведено у формулах (3) та (4), у формулі (5) – обчислення триплетної функції втрат.

$$n = \|f_i^a - f_i^n\|_2^2, \tag{3}$$

$$p = \left\|f_i^a - f_i^p\right\|_2^2, \tag{4}$$

$$Loss\,(A,P,N) = \max(\|f(A) - f(P)\|^2 - \|f(A) - f(N)\|^2 + \alpha, 0), \tag{5}$$

де A – якірний (позитивний) зразок; P – позитивний зразок (той самий клас, що і A); N – негативний зразок (інший клас); f – функція, яка визначає векторне подання об'єкта; α – параметр, який визначає мінімальну відстань між позитивним та негативним зразками; розміри кожного шару і вхідні параметри сіамської нейронної мережі з триплетною функцією втрат наведено в табл. 1.

Сіамська нейронна мережа з триплетною функцією втрат має велику кількість переваг, а саме ефективність у взаємодії з обмеженими даними, тобто в умовах обмежених навчальних даних, оскільки вони використовують три зображення для навчання, а не пари. Модель [19] може навчатися узагальнювати ознаки, важливі для відокремлення різних класів або екземплярів вхідних даних. Триплетна функція втрат допомагає у вирішенні проблеми схожості та відмінності в просторі векторів ознак, зменшуючи відстань між позитивними парами та збільшуючи відстань між негативними парами. Модель можна використовувати для різноманітних завдань, таких як розпізнавання обличчя, виокремлення об'єктів чи розпізнавання патернів, що якраз необхідно в нашій

ситуації, оскільки там потрібен один кінцевий формат роботи з фотографіями користувачів і виокремлення облич користувачів.

Таблиця 1

План моделі сіамської нейронної мережі

Шар	Розмір	Параметри
Згортка	96×11×11	Кроки = 1
Об'єднання	128×2×2	α = 10–5, β = 0,7
Відкидання	–	k = 2, n = 2
Згортка	256×5×5	Кроки = 2
Об'єднання	96×2×2	Кроки = 1, прикладні ряди = 2
Відкидання	–	α = 10–5, β = 0,8, k = 2, n = 2
Згортка	384×3×3	Кроки = 2, прикладні ряди = 2
Об'єднання	64×2×2	Кроки = 2, p = 0.35
Відкидання	–	α = 10–5, β = 0,9, k = 2, n = 2
Повністю завантажений 1	1024	p = 0,45
Повністю завантажений 2	128	p = 0,55
Прихований вбудований	128	Кроки = 1

У сіамської нейронної мережі з триплетною функцією втрат є і певні недоліки, а саме: модель може бути чутливою до вибору гіперпараметрів, таких як розмір трійок та параметрів триплетної функції втрат, що іноді потребує додаткового налаштування, але це некритично в межах створюваної інтелектуальної системи, оскільки оброблятимуться фотографії, зведені до одного типу, який і буде початково налаштованим. За великого обсягу даних може виникнути проблема підбору ефективних трійок для навчання, а також збільшитися обчислювальна складність, що також не відіграє великої ролі в межах поточної системи, оскільки для одного користувача в момент часу будуть оброблятися лише дві фотографії – поточна фотографія користувача з використанням вебкамери та збережена в базі даних світлина. У випадку неправильного підбору триплетів для навчання може виникнути проблема, коли модель навчається недостатньо ефективно і навпаки, як і багато інших моделей, сіамські нейронні мережі можуть бути схильними до перенавчання, особливо за обмежених даних, що потрібно врахувати під час реалізації сіамської нейронної мережі та вибору датасету для навчання моделі. На рис. 3 наведено деталізовану структуру сіамської нейронної мережі з триплетною функцією втрат, розмір кожного шару та його вхідні параметри.

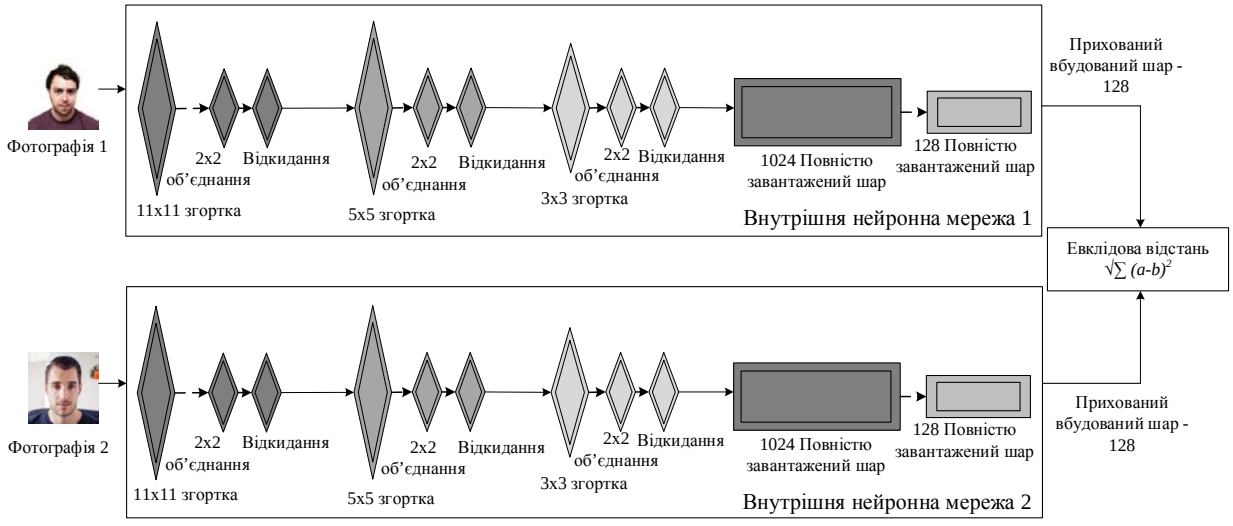

Рис. 3. Деталізована структура сіамської нейронної мережі

На рис. 4 подано блок-схему роботи функціоналу ініціалізації двофакторної автентифікації користувача в інтелектуальній системі за допомогою фотографування, пошуку обличчя та подальшого збереження медіаключа в базі даних.

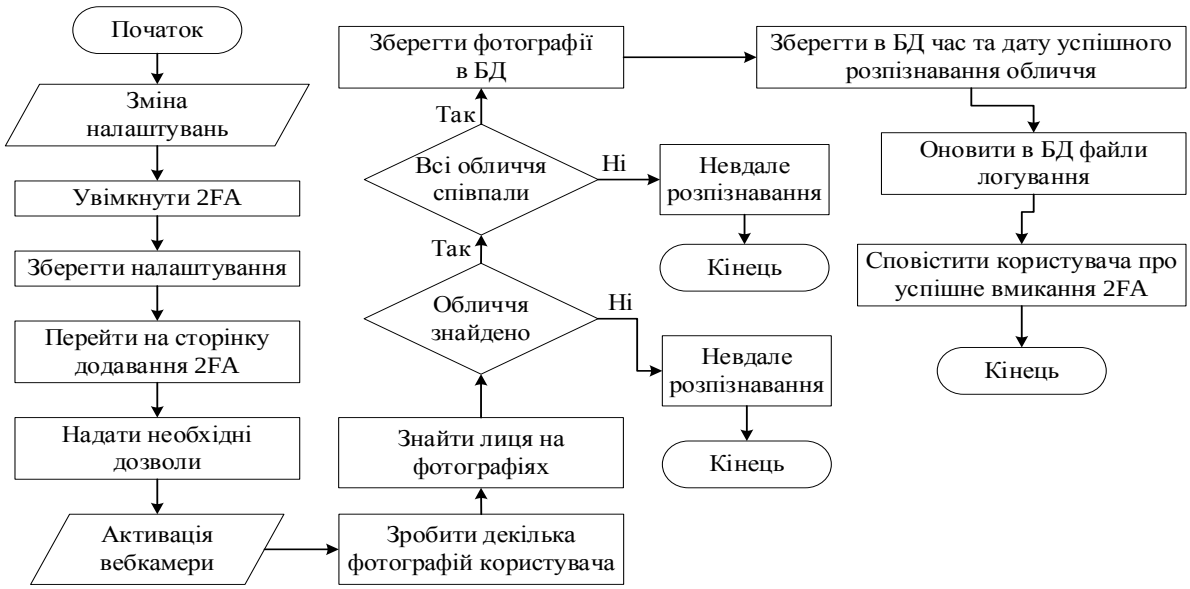

Рис. 4. Ініціалізація двофакторної автентифікації користувача в інтелектуальній системі

На рис. 5 наведено блок-схему процесу автентифікації користувача, а саме валідації введених логіну та пароля, збереження в localstorage фотографії користувача, зробленої за допомогою вебкамери та порівняння поточної фотографії з вже наявною в базі даних, що містить обличчя користувача. Якщо ознаки збігаються, користувач інтелектуальної системи отримує доступ до наявного функціоналу.

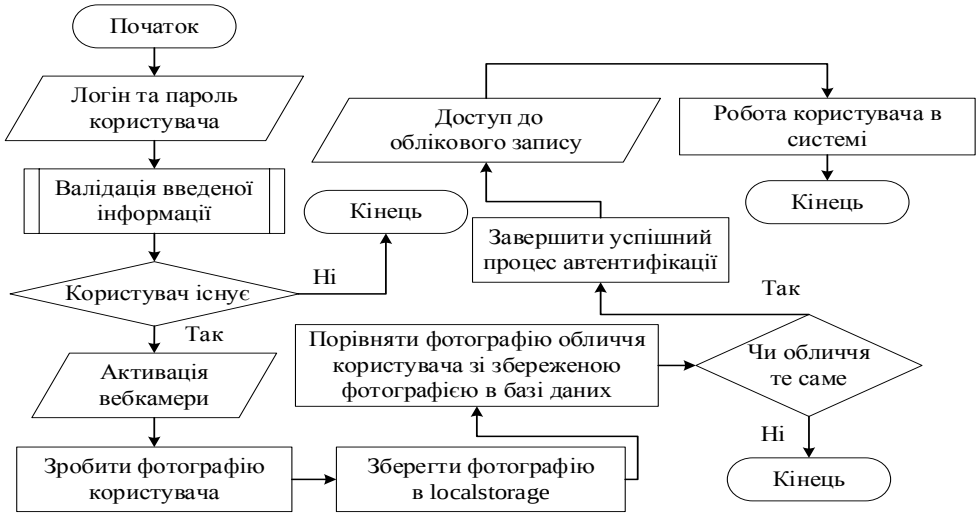

Рис. 5. Процес автентифікації користувача

На рис. 6 подано діаграму послідовності в інтелектуальній системі, яка містить три основні сутності, а саме користувача, сервер та базу даних, які взаємодіють між собою за допомогою http-запитів. Кожен запит має власний контекст відповідно до свого типу і властивостей синхронізації та виконується в певній послідовності.

Рис. 6. Діаграма послідовності в інтелектуальній системі

Виклад основного матеріалу

У ході роботи головне завдання – створити сіамську нейронну мережу, яка після тестування буде імплементована в інтелектуальну систему. Для реалізації машинного навчання використано мову програмування Python 3.10 і для написання коду вибрано IDE PyCharm. Першим кроком є завантаження датасету з фотографій та відповідних міток користувачів, що буде використовуватися для навчання та тестування нейронної мережі. Загалом датасет містить 5000 зображень і 50 унікальних елементів, тобто зображення облич 50 користувачів із різних ракурсів та з різними емоціями. Розмір кожного зображення – 128 на 128 пікселів, позаду користувацьких облич чорний фон, всі також зображення завантажені у кольорах відтінків сірого. Усі пікселі промасштабовані в інтервалі від 0 до 1, кожен користувач з датасету отримав відповідний ідентифікатор від 0 до 49. Вся ця інформація, а також інформація щодо оцінки точності навчання моделі подана на рис. 7.

```
Всього є  5000 зображень в датасеті        Оцінка точності: 0.93
Всього є 50 унікальних елементів в датасеті Середній бал точності, усереднений по всіх класах: 0.96
Розмір кожного зображення 128x128          Відстань: 0.96
Форма X: (500, 4096)                       Середня точність (AP): 1.0
Форма тренувального X: (250, 4096)         Середнє негативне (AN): 0.28
```

Рис. 7. Інформація про створену модель нейронної мережі

Наступний функціонал програми використано для відображення десяти зображень облич для кожного вказаного унікального ідентифікатора. Зображення виведено у вигляді сітки, де кожен рядок представляє одного користувача з датасету. Для кожного піддослідного виведено

десять його фотографій різного типу, на яких обличчя користувача по-різному зображене і відображає унікальні емоції (рис. 8).

Рис. 8. Унікальні зображення облич користувачів із датасету

Відтак виконано переформатування даних: кожне зображення з датасету перетворено на одновимірний масив розміру 4096×(128×128). Тренувальний і тестовий набори даних сформовано за допомогою розподілу зображень із початкового датасету. Крім того, створено DataFrame, який містить ідентифікатори суб'єктів для тренувального набору даних. DataFrame – це основна структура даних, яка використовується в бібліотеці pandas для опрацювання та аналізу даних. Вона створює двовимірний масив даних, схожий на таблицю чи аркуш даних, де дані організовано у рядки та колонки. Кожен рядок у DataFrame відповідає одному зразку в тренувальному наборі даних. Це відіграє важливу роль для подальшого вивчення та аналізу залежностей між ідентифікаторами суб'єктів та властивостями і показниками в нейронній мережі.

Наступний крок – створено триплети для використання у сіамській нейронній мережі. Написано функцію, що приймає три аргументи: шлях до директорії зображень, словник, де ключі – це папки (класи), а значення – кількість файлів у кожній папці, і максимальна кількість файлів, яку необхідно враховувати для кожної папки. Створено порожній список для зберігання триплетів та список усіх папок (класів) на основі ключів словника списку папок. Було реалізовано кортежі для якірного та позитивного зображення у поточній папці за вказаними індексами і проаналізовано змінну для папки негативного зображення, яка спочатку дорівнює поточній папці. Вибрано кортежі для позитивних та негативних зображень, усі триплети додано до загального списку. В кінці програмна функція повертає список усіх створених триплетів.

На рис. 9 подано графік проєкції обличчя людей на площину за допомогою методу аналізу головних компонент. Кожна точка на графіку відповідає одному обличчю людини. Дві осі графіка позначають перші дві головні компоненти, які визначають основні напрями варіації серед зображень обличчя. Вісь X відповідає першому головному компоненту, а вісь Y – другому головному компоненту. Кожна точка на графіку представляє обличчя однієї конкретної людини. Розташування точок вказує на те, як варіюються обличчя між людьми у вибірці. Близькі точки вказують на схожі обличчя, а віддалені точки – на різноманітні. Кожен колір відображає різних людей, ізольованих ідентифікаторами, що забезпечує чітку візуальну розмежованість різних осіб.

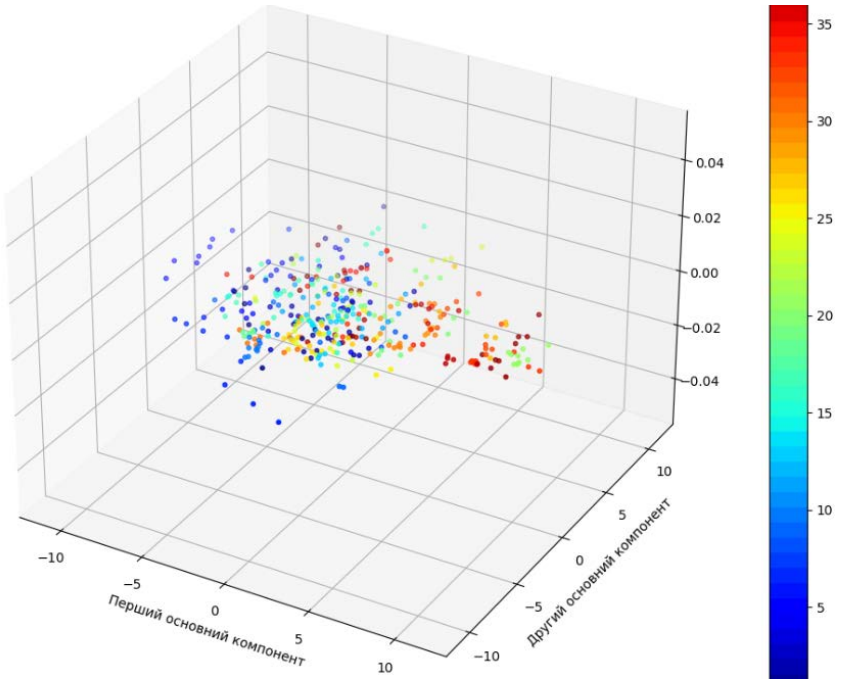

Рис. 9. Графік проєкції облич людей на площину

Далі необхідно визначити різні функції та моделі для реалізації сіамської нейронної мережі з триплетною функцією втрат. Було створено функцію для отримання партії триплетів зображень, що приймає список триплетів, кількість триплетів у кожній партії, булеве значення, вказано, чи потрібно попередньо опрацьовувати зображення. Виконано обчислення кількості кроків для отримання всіх партій триплетів, проініціалізовано списки для якірних, позитивних та негативних зображень у поточній партії та одержано якірне, позитивне та негативне зображення для поточного триплету. Зображення для кожної категорії (якірне, позитивне, негативне) додано до відповідного списку. Одержано партію триплетів у форматі (128, 128, 3), придатну для використання у нейронній мережі. Після написання функції для отримання моделі кодування зображень (екстрактора ознак) було імплементовано клас для обчислення відстаней між закодованими зображеннями.

Створивши функцію для отримання моделі кодування зображень, ми реалізували функцію для одержання сіамської нейронної мережі на основі моделі кодування та спеціального шару відстаней. Було отримано модель сіамської нейронної мережі та здійснено її тестування. На рис. 10 наведено графік, що являє собою матрицю невідповідностей для результатів класифікації за допомогою методу екстрактора ознак на основі відстаней між закодованими зображеннями. По горизонталі та вертикалі розташовані номери облич користувачів. Кожна клітина матриці вказує на кількість облич, які були правильно (по діагоналі) або неправильно (поза діагоналлю) класифіковані. Забарвлення кожної клітини відображає кількість облич, класифікованих для відповідної пари зображень (якірний клас, передбачений клас). Темніші кольори вказують на більшу кількість облич у відповідному класі. Ця матриця допомагає оцінити, наскільки добре модель класифікує обличчя для кожної особи.

Наступним кроком було оголошення класу моделі сіамської нейронної мережі, було створено відповідний клас, який успадковується від класу загальної моделі даних бібліотеки TensorFlow, та визначено методи для тренування та тестування моделі, обчислення втрат, ініціалізації параметрів. Маючи об’єкт класу моделі сіамської нейронної мережі, ми визначили оптимізатор з певними параметрами. Модель надалі була повноцінно зібрана з використанням зазначеного оптимізатора. Отримавши готову модель, ми визначили функцію тестування на триплетах, яка оцінює точність моделі на тестових триплетах, а саме виводиться точність на тестовому наборі триплетів та середні значення відстаней для правильних і неправильних пар. Здійснено зазначену кількість епох тренування, а саме 512

епох. Для кожної епохи виконано обчислення, виведено значення середніх втрат на тренувальному наборі триплетів. Модель протестовано на тестовому наборі триплетів і виведено метрики (точність, середні відстані та стандартні відхилення). Збережено ваги моделі, коли точність на тестовому наборі підвищилася, останній крок навчання – збережено фінальні ваги моделі після всіх епох. Загальною метою було тренування сіамської нейронної мережі за допомогою триплетної функції втрат для вирішення завдання порівняння обличчя користувача на двох фотографіях і визначення, позитивною чи негативною є відповідь у цьому контексті. Модель намагається мінімізувати втрати для правильних пар облич користувачів (якірні позитивні зображення) та максимізувати відстані для неправильних пар облич користувачів (якірні негативні зображення).

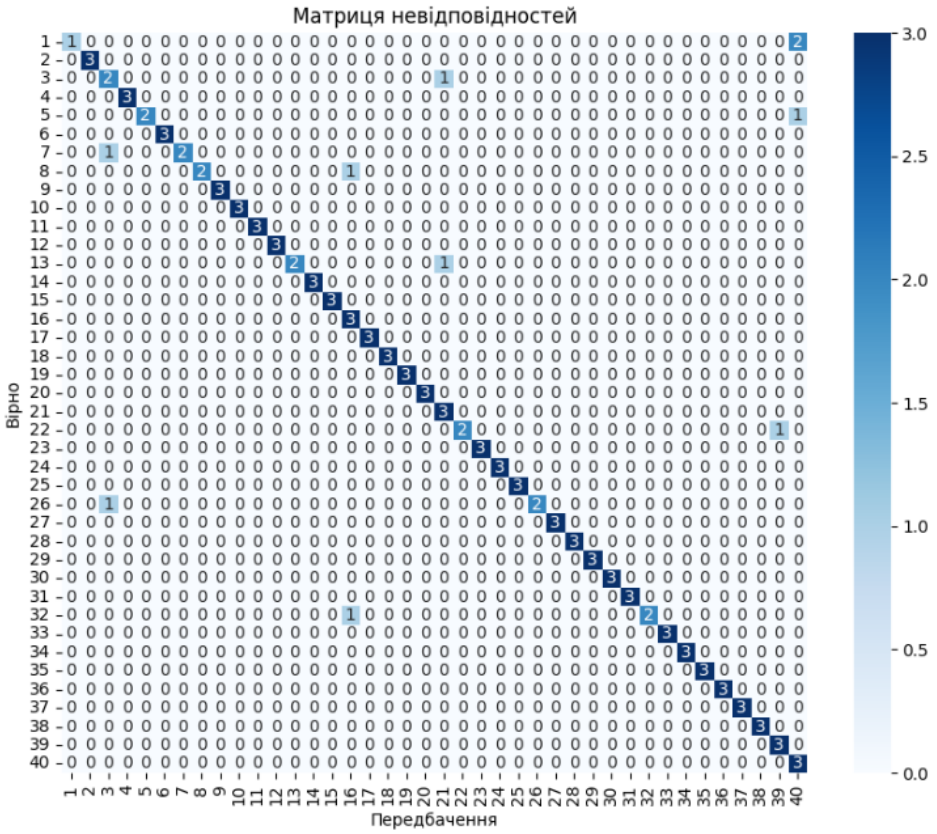

Рис. 10. Матриця невідповідностей для результатів класифікації

На рис. 11 наведено графік – криву, на осі X відображено повноту, на осі Y – точність. Кожна точка на цій кривій відповідає певному порогу вирішення для класифікаційної моделі. Точність визначає, яка частина вказаних моделлю позитивних випадків позначені правильно, а повнота показує, яку частину фактично позитивних випадків виявила модель. Крива точність-повнота відображає, як змінюються точність і повнота за різних порогів вирішення завдання. Область під цією кривою вказує на якість моделі: чим більше це значення, тим краще. На графіку також відзначена фіолетовим кольором область між кривою та віссю X, яка вказує на середню оцінку точності, усередненну за всіма класами. Це число дає змогу отримати узагальнену міру якості класифікації, об’єднуючи інформацію про точність та повноту для різних класів. Що більше значення середньої точності, то ефективніше працює модель.

Створено нову функцію кодування за архітектурою значень вихідного кодування. Пройшовши по шарах кодування вихідної моделі, ми скопіювали їх ваги до відповідних шарів нового шару кодування. Було збережено ваги отриманого закодованого файлу і виведено опис архітектури шару

кодування. Отримавши вбудовування для переданих списків зображень облич, ми обчислили квадрат відстані між вбудовуваннями облич та здійснили класифікацію на основі порогового значення, одержавши в результаті масив з прогнозами 0 або 1. Отримано два списки прогнозів (позитивні та негативні), які відповідають схожим і різним парам облич користувачів. Перевірено всі наявні пакети тестових триплетів і реалізовано функцію класифікації зображень для отримання прогнозів для позитивних (схожих) і негативних (різних) пар користувацьких обличь. Останній крок тестування – виклик функції метрик для оцінювання ефективності моделі.

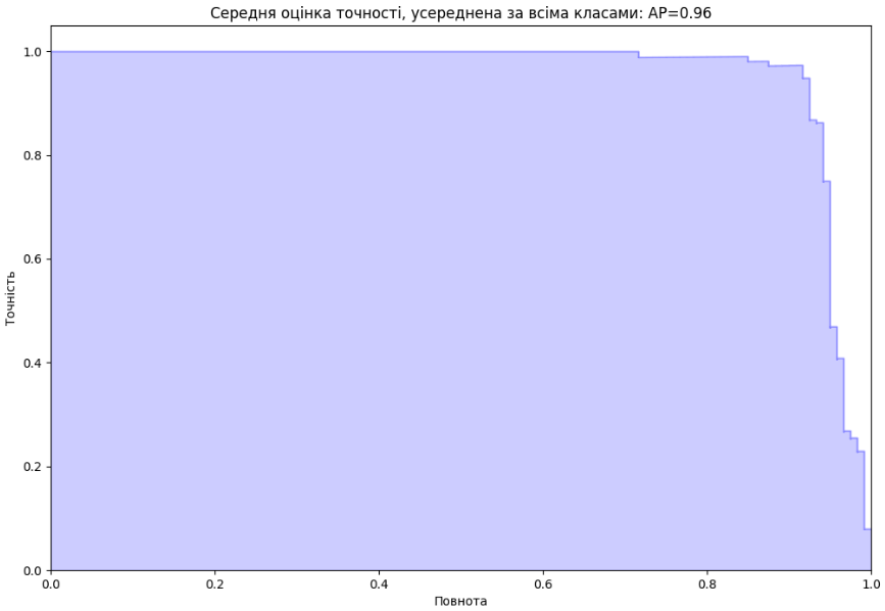

Рис. 11. Графік зміни точності та повноти за різних порогів розв'язання задачі

На рис. 12 наведено приклад порівняння якірного зображення та поданого на вхід функції для перевірки схожості. Як видно з графіка, це дві фотографії того самого користувача, а отже, прогноз є позитивним. Подано вміст та структуру першого та другого зображень та зображення, що показує абсолютну відмінність між першою і другою фотографіями, використовуючи кольоровий мапінг. У цьому вікні кожний піксель представлений відтінком згідно з різницею між відповідними пікселями перших двох зображень. Темніші області вказують на меншу різницю, світліші – на більшу. В результаті визначено, чи відображають фотографії ту саму особу.

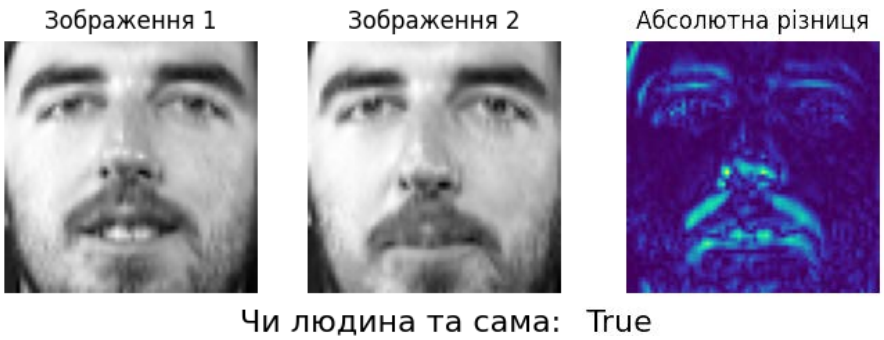

Рис. 12. Визначення, чи та сама особа на обох фотографіях

Графік на рис. 13 відображає залежність тренувальних втрат від кількості ітерацій під час навчання моделі. Кожна точка на графіку відображає втрати на конкретній ітерації. На горизонтальній осі

розташовані ітерації, тобто кількість кроків або епох тренування моделі. На вертикальній осі – значення втрат на кожній ітерації. Втрати представляють помилки моделі під час навчання. Графік відображає спеціально вибрану функцію втрати, яка може змінюватися від ітерації до ітерації. У цьому випадку застосовано гіперболічний спад втрат на початкових ітераціях (до досягнення плато), після чого втрати залишаються на стабільному рівні. Цей графік допомагає ефективно проаналізувати динаміку втрат під час навчання моделі та визначити ефективність процесу навчання.

Графік на рис. 14 відображає основні метрики для моделі розпізнавання користувацького обличчя. Середня точність – це показник того, наскільки добре модель розпізнає позитивні пари, які повинні бути схожими. Високе значення AP (середня точність) свідчить про ефективність моделі в розпізнаванні подібних облич. AN (середнє негативне значення) – вказує на ступінь схожості для негативних пар, які повинні бути різними. Низьке значення AN свідчить про ефективність моделі в розпізнаванні різних обличь.

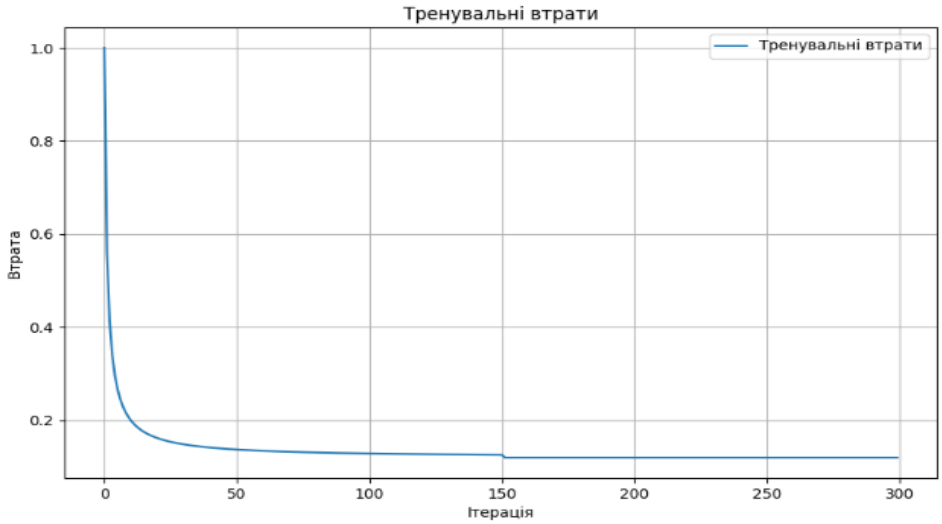

Рис. 13. Графік залежності тренувальних втрат від кількості ітерацій під час навчання моделі

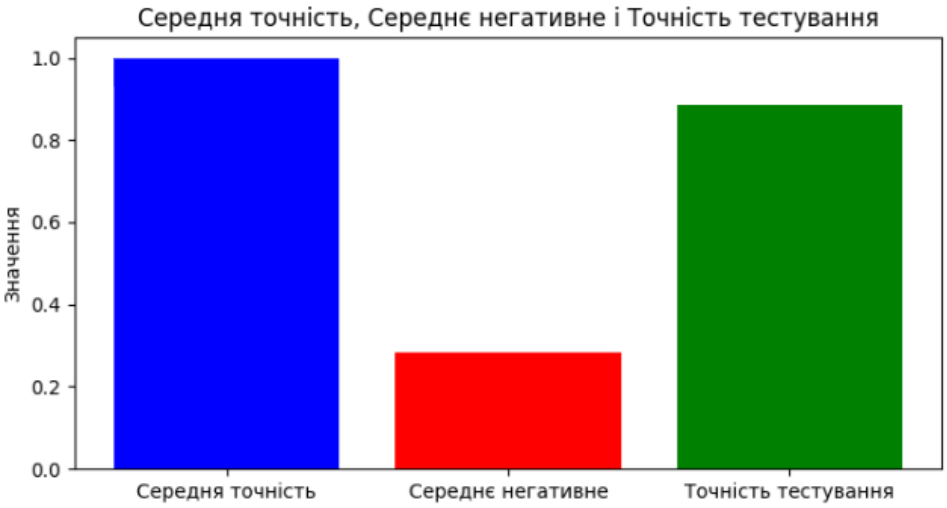

Рис. 14. Графік оцінювання основних аспектів ефективності створеної нейронної мережі

Останньою метрикою є точність тестування – це ймовірність правильного класифікаційного визначення відповідно до тестового набору даних. Графік допомагає оцінити три основні аспекти ефективності моделі для конкретного завдання розпізнавання обличчя.

На рис. 15 зображено перший етап автентифікації користувача в інтелектуальній системі за допомогою введення логіну та паролю, на рис. 16 – базову сторінку початку двофакторної автентифікації, для здійснення якої користувачу необхідно в поточному браузері дозволити використання вебкамери.

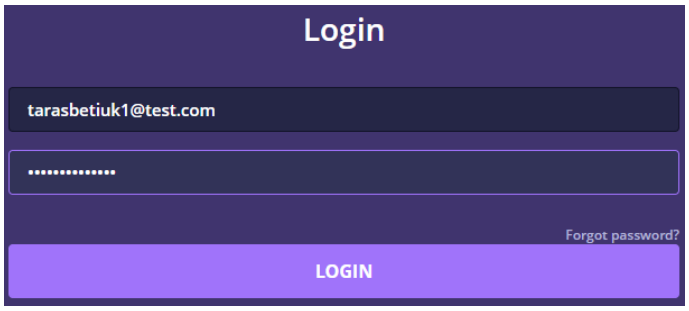

Рис. 15. Введення логіну та паролю користувача

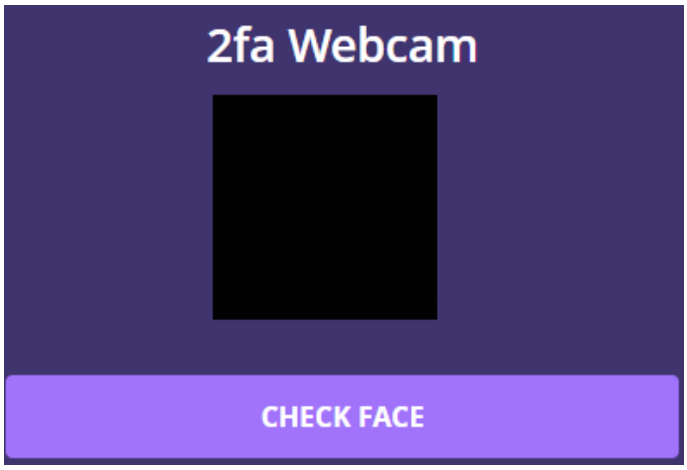

Рис. 16. Початкова сторінка двофакторної автентифікації

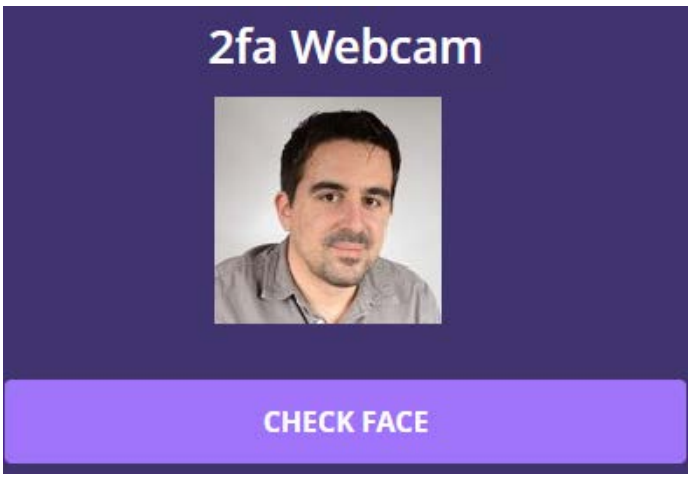

Рис. 17. Фотографування обличчя користувача інтелектуальної системи

На рис. 17 зображено увімкнення користувацької вебкамери та фотографування обличчя користувача інтелектуальної системи; на рис. 18 – опрацювання створеною раніше сіамською нейронною мережею фотографії та пошук на ній обличчя; на рис. 19 подано результат успішного

пошуку обличчя на фотографії та виділення зеленим кольором певної області зображення, де знайдено обличчя користувача.

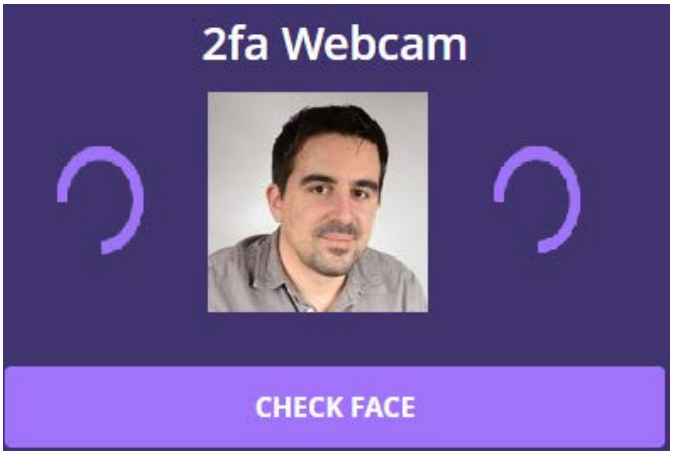

Рис. 18. Оброблення фотографії сіамською нейронною мережею

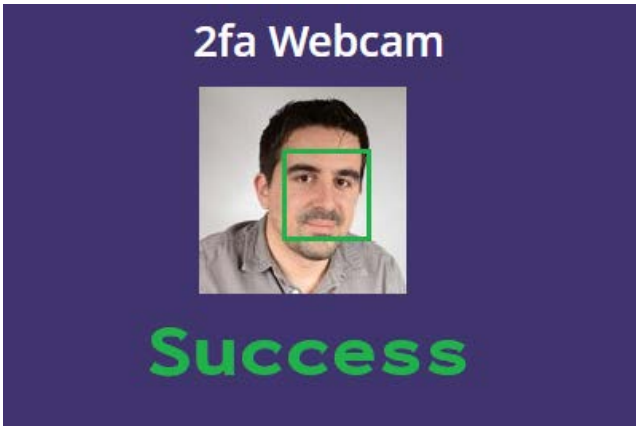

Рис. 19. Результат успішного пошуку обличчя на фотографії

На рис. 20 наведено порівняння поточної фотографії користувача, зробленої з використанням вебкамери, та фотографії, збереженої в базі даних. Результат: прогноз сіамської нейронної мережі є позитивним і користувач здійснив успішну автентифікацію в системі. На рис. 21 зображено спробу поточного користувача увійти в акаунт іншого користувача інтелектуальної системи, відповідно прогноз нейронної мережі є негативним і користувачу відмовлено в автентифікації.

Рис. 20. Успішна автентифікація користувача в інтелектуальній системі

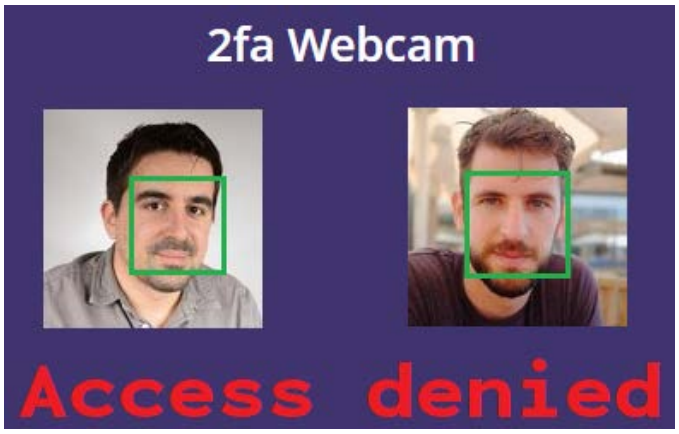

Рис. 21. Відмова користувачу в автентифікації в інтелектуальній системі

Отже, в ході роботи було імплементовано сіамську нейронну мережу з триплетною функцією втрат. Вона може як здійснювати загальний пошук користувацького обличчя на фотографії, так і виконувати порівняння двох фотографій, щоб визначити, чи них зображений той самий користувач. Здійснивши навчання моделі нейронної мережі і її подальше успішне тестування за допомогою поданого датасету, ми виконали модульну інтеграцію створеної нейронної мережі в інтелектуальну систему як важливий компонент сервісу забезпечення безпечного входу в систему, де він виконує функцію ефективної та надійної двофакторної автентифікації за допомогою візуальної біометрики.

Висновки

В ході дослідження та розроблення системи автентифікації на основі візуальної біометрики з використанням сіамської нейронної мережі виконано комплексний аналіз аспектів безпеки та ефективності автентифікаційного процесу в інтелектуальних системах. Важливими кроками у дослідженні стали вивчення та розгляд альтернатив реалізації сіамської нейронної мережі за допомогою функції контрастних втрат та триплетної функції втрат.

У результаті аналізу опублікованих робіт визначено основні переваги та недоліки сіамських нейронних мереж та способи оптимальної інтеграції нейронної мережі в інтелектуальну систему аутентифікації. Вибрано триплетну функцію втрат як оптимальний метод для навчання моделі, що дає змогу забезпечити високу точність розпізнавання обличчя користувача. Описано основні особливості сіамських нейронних мереж із використанням діаграм як роботу самої нейронної мережі у вигляді монолітного елемента, так і у вигляді сервісу у складі інтелектуальної системи. За допомогою блок-схем та діаграми послідовності описано алгоритм роботи системи та http-запитів між компонентами системи. За результатами концептуального проєктування написано програмний код, навчено та протестовано сіамську нейронну мережу з триплетною функцією втрат, що має реалізований функціонал як пошуку обличчя користувача на одній фотографії, так і порівняння декількох фотографій для визначення, чи сукупність фотографій належать тому самому користувачу, що є важливою вимогою під час інтеграції нейронної мережі в інтелектуальну систему. Додатково систему розширено функціоналом двофакторної автентифікації з використанням технології пошуку, розпізнавання та порівняння обличчя користувачів. Це не лише підвищило рівень безпеки, а й зробило процес автентифікації ефективнішим та надійнішим.

Інтеграція сіамської нейронної мережі в інтелектуальну систему автентифікації дала змогу створити ефективний засіб розпізнавання обличчя користувача, зберігання та порівняння отриманих даних. Такий підхід мінімізує ризик несанкціонованого доступу та гарантує безпеку користувацьких акаунтів. Отже, розроблена система являє собою ефективний та захищений інструмент для автентифікації користувачів, здатний мінімізувати загрози безпеки в інтелектуальних системах. Цей

підхід можна використовувати для покращення захисту конфіденційної інформації та забезпечення надійного контролю доступу до системи.

Список літератури

1. Long, X., Zhuang, W., Xia, M., Hu, K., & Lin, H. (2024). SASiamNet: Self-adaptive Siamese Network for change detection of remote sensing image. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 17, 1021–1034. DOI: https://doi.org/10.1109/jstars.2023.3330753

2. Ning, M., Tang, J., Zhong, H., Wu, H., Zhang, P., & Zhang, Z. (2022). Scale-Aware Network with Scale Equivariance. Photonics, 9(3), 142–142. DOI: https://doi.org/10.3390/photonics9030142

3. Batiuk, T., & Dosyn, D. (2023). Intellectual system for clustering users of social networks derived from the message sentiment analysis. *Journal of Lviv Polytechnic National University "Information Systems and Networks"*, 13, 121–138. DOI: https://doi.org/10.23939/sisn2023.13.121

4. Zhao, Y., Song, X., Li, J., & Liu, Y. (2024). CSCNet: A Cross-Scale Coordination Siamese Network for Building Change Detection. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 17, 1377–1389. DOI: https://doi.org/10.1109/jstars.2023.3337999

5. Farabbi, A., & Mainardi, L. (2023). Domain-Specific Processing Stage for Estimating Single-Trail Evoked Potential Improves CNN Performance in Detecting Error Potential. *Sensors*, 23(22), 9049–9049. DOI: https://doi.org/10.3390/s23229049

6. Cheng, L., Zheng, X., Zhao, M., Dou, R., Yu, S., Wu, N., & Liu, L. (2022). SiamMixer: A Lightweight and Hardware-Friendly Visual Object-Tracking Network. *Sensors*, 22(4), 1585–1585. DOI: https://doi.org/10.3390/s22041585

7. Kummerow, A., Monsalve, C., & Bretschneider, P. (2021). Siamese recurrent neural networks for the robust classification of grid disturbances in transmission power systems considering unknown events. *IET Smart Grid*, 5(1), 51–61. DOI: https://doi.org/10.1049/stg2.12051

8. Batiuk T., Vysotska V., Lytvyn V. (2020). Intellectual System for Socialization by Personal Interests on the Basis of SEO Algorithms and Techniques of Machine Learning. CEUR Workshop Proceedings, 4th Intern. Conf. on Computational Linguistics and Intellectual Systems, COLINS 2020, 23–24 April 2020, Lviv, Ukraine, 2604. 1237–1250.

9. Gao, Y., Wu, H., Liao, H., Chen, X., Yang, S., & Han, X. (2023). A fault diagnosis method for rolling bearings based on graph neural network with one-shot learning. EURASIP Journal on Advances in Signal Processing, 2023(1). DOI: https://doi.org/10.1186/s13634-023-01063-6

10. Mo, W., Tan, Y., Zhang, Y., Zhi, Y., Cai, Y., & Ma, W. (2023). Multispectral Remote Sensing Image Change Detection Based on Twin Neural Networks. *Electronics*, 12(18), 3766–3766. DOI: https://doi.org/10.3390/electronics12183766

11. Batiuk, T., & Vysotska, V. (2022). Technology for personalities socialization by common interests derived from machine learning techniques and seo-algorithms. *Radio Electronics, Computer Science, Control*, 2, 53. DOI: https://doi.org/10.15588/1607-3274-2022-2-6

12. Pang, H., Xie, M., Liu, C., Ma, R., & Han, L. (2021). Siamese tracking combing frequency channel attention with adaptive template. *IET Communications*, 15(20), 2493–2502. DOI: https://doi.org/10.1049/cmu2.12280

13. Basu, T., Menzer, O., Ward, J., & SenGupta, I. (2022). A Novel Implementation of Siamese Type Neural Networks in Predicting Rare Fluctuations in Financial Time Series. *Risks*, 10(2), 39. DOI: https://doi.org/10.3390/risks10020039

14. Yuan, D., Li, Q., Yang, X., Zhang, M., & Sun, Z. (2022). Object-Aware Adaptive Convolution Kernel Attention Mechanism in Siamese Network for Visual Tracking. *Applied Sciences*, 12(2), 716. DOI: https://doi.org/10.3390/app12020716

15. Lee, D., & Jeong, J. (2023). Few-Shot Learning-Based Light-Weight WDCNN Model for Bearing Fault Diagnosis in Siamese Network. *Sensors*, 23(14), 6587–6587. DOI: https://doi.org/10.3390/s23146587

16. Batiuk T., Vysotska V., Holoshchuk R., Holoshchuk S. (2022). Intellectual System for Socialization of Individual's with Contributed Interests derived from NLP, Machine Learning and SEO Algorithms. CEUR Workshop Proceedings, 6th Intern. Conf. on Computational Linguistics and Intellectual Systems, COLINS 2022, 12–13 May 2022, Gliwice, Poland, 3171, 572–631.

17. Ahmed, S., Lee, K. H., & Jung, H. Y. (2022). Robust Hippocampus Localization From Structured Magnetic Resonance Imaging Using Similarity Metric Learning. *IEEE Access*, 10, 7141–7152. DOI: https://doi.org/10.1109/access.2021.3137824

18. Islem Jarraya, F. Saïd, Hamdani, T. M., Bilel Neji, & Alimi, A. M. (2022). Biometric-Based Security System for Smart Riding Clubs. *IEEE Access*, 10, 132012–132030. DOI: https://doi.org/10.1109/access.2022.3229260

19. Song, C., & Ji, S. (2022). Face Recognition Method Based on Siamese Networks Under Non-Restricted Conditions. *IEEE Access*, 10, 40432–40444. DOI: https://doi.org/10.1109/access.2022.3167143

References

1. Long, X., Zhuang, W., Xia, M., Hu, K., & Lin, H. (2024). SASiamNet: Self-adaptive Siamese Network for change detection of remote sensing image. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 17, 1021–1034. DOI: https://doi.org/10.1109/jstars.2023.3330753

2. Ning, M., Tang, J., Zhong, H., Wu, H., Zhang, P., & Zhang, Z. (2022). Scale-Aware Network with Scale Equivariance. *Photonics*, *9*(3), 142–142. DOI: https://doi.org/10.3390/photonics9030142

3. Batiuk, T., & Dosyn, D. (2023). Intellectual system for clustering users of social networks derived from the message sentiment analysis. *Journal of Lviv Polytechnic National University "Information Systems and Networks"*, 13, 121–138. DOI: https://doi.org/10.23939/sisn2023.13.121

4. Zhao, Y., Song, X., Li, J., & Liu, Y. (2024). CSCNet: A Cross-Scale Coordination Siamese Network for Building Change Detection. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 17, 1377–1389. DOI: https://doi.org/10.1109/jstars.2023.3337999

5. Farabbi, A., & Mainardi, L. (2023). Domain-Specific Processing Stage for Estimating Single-Trail Evoked Potential Improves CNN Performance in Detecting Error Potential. *Sensors*, *23*(22), 9049–9049. DOI: https://doi.org/10.3390/s23229049

6. Cheng, L., Zheng, X., Zhao, M., Dou, R., Yu, S., Wu, N., & Liu, L. (2022). SiamMixer: A Lightweight and Hardware-Friendly Visual Object-Tracking Network. *Sensors*, *22*(4), 1585–1585. DOI: https://doi.org/10.3390/s22041585

7. Kummerow, A., Monsalve, C., & Bretschneider, P. (2021). Siamese recurrent neural networks for the robust classification of grid disturbances in transmission power systems considering unknown events. *IET Smart Grid*, *5*(1), 51–61. DOI: https://doi.org/10.1049/stg2.12051

8. Batiuk T., Vysotska V., Lytvyn V. (2020). Intellectual System for Socialization by Personal Interests on the Basis of SEO Algorithms and Techniques of Machine Learning. *CEUR Workshop Proceedings, 4th Intern. Conf. on Computational Linguistics and Intellectual Systems*, COLINS 2020, 23–24 April 2020, Lviv, Ukraine, 2604, 1237–1250.

9. Gao, Y., Wu, H., Liao, H., Chen, X., Yang, S., & Han, X. (2023). A fault diagnosis method for rolling bearings based on graph neural network with one-shot learning. *EURASIP Journal on Advances in Signal Processing*, *2023*(1). DOI: https://doi.org/10.1186/s13634-023-01063-6

10. Mo, W., Tan, Y., Zhang, Y., Zhi, Y., Cai, Y., & Ma, W. (2023). Multispectral Remote Sensing Image Change Detection Based on Twin Neural Networks. *Electronics*, *12*(18), 3766–3766. DOI: https://doi.org/10.3390/electronics12183766

11. Batiuk, T., & Vysotska, V. (2022). Technology for personalities socialization by common interests derived from machine learning techniques and seo-algorithms. *Radio Electronics, Computer Science, Control*, 2, 53. DOI: https://doi.org/10.15588/1607-3274-2022-2-6

12. Pang, H., Xie, M., Liu, C., Ma, R., & Han, L. (2021). Siamese tracking combing frequency channel attention with adaptive template. *IET Communications*, *15*(20), 2493–2502. DOI: https://doi.org/10.1049/cmu2.12280

13. Basu, T., Menzer, O., Ward, J., & SenGupta, I. (2022). A Novel Implementation of Siamese Type Neural Networks in Predicting Rare Fluctuations in Financial Time Series. *Risks*, *10*(2), 39. DOI: https://doi.org/10.3390/risks10020039

14. Yuan, D., Li, Q., Yang, X., Zhang, M., & Sun, Z. (2022). Object-Aware Adaptive Convolution Kernel Attention Mechanism in Siamese Network for Visual Tracking. *Applied Sciences*, *12*(2), 716. DOI: https://doi.org/10.3390/app12020716

15. Lee, D., & Jeong, J. (2023). Few-Shot Learning-Based Light-Weight WDCNN Model for Bearing Fault Diagnosis in Siamese Network. *Sensors*, *23*(14), 6587–6587. DOI: https://doi.org/10.3390/s23146587

16. Batiuk T., Vysotska V., Holoshchuk R., Holoshchuk S. (2022). Intellectual System for Socialization of Individual's with Contributed Interests derived from NLP, Machine Learning and SEO Algorithms. *CEUR Workshop Proceedings, 6th Intern. Conf. on Computational Linguistics and Intellectual Systems*, COLINS 2022, 12–13 May 2022, Gliwice, Poland, 3171, 572–631.

17. Ahmed, S., Lee, K. H., & Jung, H. Y. (2022). Robust Hippocampus Localization From Structured Magnetic Resonance Imaging Using Similarity Metric Learning. *IEEE Access*, *10*, 7141–7152. DOI: https://doi.org/10.1109/access.2021.3137824

18. Islem Jarraya, F. Saïd, Hamdani, T. M., Bilel Neji, & Alimi, A. M. (2022). Biometric-Based Security System for Smart Riding Clubs. *IEEE Access*, *10*, 132012–132030. DOI: https://doi.org/10.1109/access.2022.3229260

19. Song, C., & Ji, S. (2022). Face Recognition Method Based on Siamese Networks Under Non-Restricted Conditions. *IEEE Access*, *10*, 40432–40444. DOI: https://doi.org/10.1109/access.2022.3167143

REALIZATION OF RELIABLE AND EFFECTIVE AUTHENTICATION IN INTELLIGENT SYSTEMS BY USING VISUAL BIOMETRICS METHODS

Taras Batiuk[1], Dmytro Dosyn[2]

Lviv Polytechnic National University,
Information Systems and Networks Department, Lviv, Ukraine
[1] E-mail: taras.m.batiuk@lpnu.ua, ORCID: 0000-0001-5797-594X
[2] E-mail: dmytro.h.dosyn@lpnu.ua, ORCID: 0000-0003-4040-4467

The main purpose of this article is to consider the aspects of ensuring security and increasing the efficiency of the authentication process in intelligent systems using visual biometrics. The work is aimed at the development and improvement of authentication systems using advanced biometric identification methods. An intelligent system has been created that ensures secure authentication of users of the current system, using a Siamese neural network. In addition to the implementation of basic security measures in the form of hashing and saving user logins and passwords, the implementation of two-factor authentication is important nowadays, which significantly strengthens the protection of user data and prevents most modern methods of hacking and stealing user data. Two-factor authentication is implemented as a technology for searching, recognizing and comparing the faces of system users, as visual biometrics is more secure than other types of two-factor authentication. Different variations of the possible implementation of Siamese neural network using Contrastive loss function and more modern Triplet loss function were reviewed and accordingly, a neural network using Triplet loss function was accomplished and trained. After training and verifying the correct operation of the neural network, it was integrated into the created intelligent system, thanks to which an effective way of recognizing the face of the system user was created, saving the received information in the database and further comparing the current user with the stored face during authentication. As a result, a secure and reliable intelligent system was created that cutting down the risk of unapproved access to the user account and uses an effective and modern method of user authentication.

Key words: two-factor authentication; siamese neural network; Triplet Loss Function; visual biometrics; facial recognition technologies.