ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ/ PRIVACY & PROTECTION FROM IDENTITY THEFT

DOI: 10.18372/2225-5036.30.19247

МОДУЛЬНА НЕЙРОМЕРЕЖЕВА МОДЕЛЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ПЕРСОНАЛУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ЗОБРАЖЕННЯМ ОБЛИЧЧЯ ТА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА

Олександр Корченко[1], Олег Терейковський[2]

[1]Державний університет інформаційно-комунікаційних технологій, Україна
[2]Національний авіаційний університет, Україна

КОРЧЕНКО Олександр Григорович, член-кореспондент НАН України, д.т.н., професор
Рік та місце народження: 1961 р., м. Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року Національний авіаційний університет).
Посада: перший проректор Державного університету інформаційно-комунікаційних технологій, професор Університету Комісії Народної Освіти (Краків, Польща).
Наукові інтереси: інформаційна та авіаційна безпека.
Публікації: понад 400 наукових публікацій, серед яких монографії, словники, енциклопедія, підручники, навчальні посібники, наукові статті та патенти на винаходи та ін.
E-mail: icaocentre@nau.edu.ua.
Orcid ID: 0000-0003-3376-0631.

ТЕРЕЙКОВСЬКИЙ Олег Ігоревич, аспірант
Рік та місце народження: 1999 р., смт Козин, Київська обл., Україна.
Освіта: КПІ ім. Ігоря Сікорського, магістр.
Посада: аспірант Національного авіаційного університету.
Наукові інтереси: кібербезпека.
Публікації: понад 20 наукових публікацій.
E-mail: tereikovskyio@gmail.com.
Orcid ID: 0000-0001-5045-0163.

Анотація. *Проблематика статті пов'язана із підвищенням ефективності систем біометричної автентифікації персоналу об'єктів критичної інфраструктури. Показано, що перспективи підвищення ефективності доцільно співвіднести з вдосконаленням нейромережевих засобів, що використовуються в процесі біометричної автентифікації. В результаті проведених досліджень розроблено модульну нейромережеву модель, що забезпечує ефективну автентифікацію персоналу за зображенням обличчя та райдужною оболонкою ока на об'єкті критичної інфраструктури з урахуванням необхідності розпізнавання спуфінг-атак та оперативного оновлення даних щодо переліку легітимних представників персоналу об'єкту. Новизна запропонованої модульної нейромережевої моделі полягає у застосуванні авторських варіантів нейронних мереж, що дозволяють реалізувати розпізнавання емоційного стану зареєстрованої особи, розпізнавання спуфінг-атак на основі природності емоцій та зображень фонових об'єктів, характерних для конкретних умов відеореєстрації, та розпізнавання особи шляхом порівняння піддослідного зображення обличчя із зображеннями обличчя легітимного персоналу, що дає змогу оперативно реагувати на зміну переліку легітимних представників персоналу об'єкту критичної інфраструктури без необхідності донавчання моделі.*

Ключові слова: *біометрична автентифікація; розпізнавання особи; зображення обличчя; райдужна оболонка ока; нейрона мережа; об'єкт критичної інфраструктури.*

Постановка проблеми

Практичний досвід та результати науково-технічних публікацій [11, 14, 17] однозначно свідчать про те, що за нинішніх обставин однією із найбільш важливих науково-практичних задач в області захисту об'єктів критичної інфраструктури (ОКІ) є задача підвищення

ефективності систем автентифікації персоналу вказаних об'єктів. При цьому одним із пріоритетних напрямків підвищення ефективності являється вдосконалення засобів біометричної автентифікації, що на сьогодні відносяться до ключових компонентів таких систем.

Хоча в системах автентифікації персоналу ОКІ використовуються засоби, що забезпечують біометричну автентифікацію на основі аналізу достатньо широкого спектру біометричних параметрів, однак найбільш широкого розповсюдження набули засоби, що базуються на аналізі зображення обличчя (ЗО). Це пояснюється доступністю та апробованістю як самих засобів реєстрації ЗО (відеокамер), так і технології їх застосування, що забезпечує можливість здійснення автентифікації не тільки під час перевірки особи представника персоналу під час входу на ОКІ, але і під час виконання ним службових обов'язків. Разом з тим, в багатьох науково-практичних роботах [12, 13, 17, 18] вказується на недосконалість сучасних засобів біометричної автентифікації на основі аналізу ЗО, пов'язану з: недостатньою ефективністю протидії атакам за допомогою муляжів; високою ресурсоємністю та недостатньою точністю нейромережевих моделей (НММ), що в переважній більшості випадків використовуються для аналізу біометричних параметрів; відсутністю можливості розпізнавання психоемоційного стану представника персоналу; недостатньо повною інтеграцією з засобами автентифікації на основі аналізу біометричних параметрів, що можуть бути зареєстровані за допомогою сучасних відеокамер одночасно з реєстрацією ЗО. Крім того, в роботах [9, 18] вказується на доцільність інтеграції засобів біометричної автентифікації за ЗО з засобами, які здійснюють автентифікацію за райдужною оболонкою ока (РОО), що пояснюється можливістю одночасної реєстрації вказаних біометричних параметрів за допомогою розповсюджених відеокамер.

Цим пояснюється актуальність досліджень, спрямованих на підвищення ефективності нейромережевих засобів біометричної автентифікації персоналу ОКІ за ЗО та РОО.

Аналіз останніх досліджень і публікацій

Оскільки в загальному випадку шляхи підвищення ефективності засобів біометричної автентифікації персоналу ОКІ доцільно співвіднести з виправленням їх недоліків, то перший етап аналізу присвячено розгляду відомих засобів відповідного призначення. Враховуючи закритий характер систем захисту інформації ОКІ та можливість оперативної інтеграції нових рішень у вказані системи захисту, було проаналізовано ряд засобів біометричної автентифікації, які знайшли своє використання на об'єктах, що не належать до критичної інфраструктури.

Зазначимо, що відповідно до [2, 8, 17], в процесі аналізу увагу акцентовано на визначення можливостей забезпечення достатньої точності розпізнавання легітимного представника персоналу при різноманітних умовах реєстрації відеоінформації за необхідності протидії атакам за допомогою муляжів (спуфінг-атака, spoofing attack).

Система біометричної автентифікації від компанії FACETEC (www.facetec.com), вартість якої становить 600000$, орієнтована на розпізнавання особи, для реєстрації обличчя якої використовується одна відеокамера. Зареєстрований відеопотік підлягає спеціалізованій обробці за допомогою засобів штучного інтелекту, що забезпечує створення 3D карти ЗО. Декларується, що показник $FAR \approx 8 \times 10^{-9}$. При цьому система ефективно протидіє спуфінг-атакам, які реалізуються за допомогою двовимірних фотографій, цифрових зображень та відео, паперових масок з вирізами для очей та рота, "голівудських масок", створених з латексу, силікону, поліуретанової піни, гуми та спеціальних гримувальних матеріалів, воскових фігур, реалістичних ляльок, 3D-відеопроєкцій, емуляторів віртуальних відеокамер, а також сплячих (мертвих) користувачів із заплющеними очима.

Система біометричної автентифікації Iris Access від компанії Iridian Tech (www.iridiantech.com) носить універсальний характер і може бути використана на різноманітних підприємствах. Заявлено, що Iris Access забезпечує безконтактну автентифікацію людини за РОО з відстані біля 30 см. При цьому сервіс автоматичного налаштування кута нахилу зчитувача дає змогу прискорити процес розпізнавання під час використання пристрою як окремо, так і в комбінації з картками доступу або PIN-клавіатурою. Відзначається короткий термін реєстрації нового користувача.

Система біометричної автентифікації від компанії Blink Identity (www.blinkidentity.com) адаптована до різноманітних умов експлуатації, що забезпечує можливість її застосування на підприємствах, що працюють в умовах підвищеного ризику та громадських місцях. Система забезпечує можливість одночасної автентифікації до 60 осіб за хвилину навіть за умови швидкого пересування в натовпі. Особливістю системи є збереження ЗО легітимного користувача у вигляді спеціального шаблону, що не підлягає зворотному перетворенню у зображення. Цим забезпечується посилення захисту збережених даних від можливого витоку інформації.

Також проаналізовані можливості засобів ідентифікації особи за ЗО та РОО, що використовуються в сучасних мобільних пристроях на платформі Apple та на платформі Android. Визначено, що технологія Face ID (платформа Apple) передбачає проведення відеореєстрації як у видимому, так і у інфрачервоному діапазоні світла. При цьому на ЗО проєктується набір ключових точок, що забезпечує можливість створення шаблону обличчя легітимного користувача, який надалі використовується в якості еталону для порівняння. Зазначається, що засоби розпізнавання особи, побудовані за технологією Face ID, адаптовані до завад, пов'язаних з нанесенням макіяжу, появою волосся, наявністю капелюха, шарфа, прозорих окулярів, контактних лінз або медичної маски.

У останньому випадку необхідною умовою автентифікації являється відеореєстрація очей та увімкнення режиму "Face ID з маскою". Також вказані засоби можуть використовуватись в умовах різноманітного освітлення. Зазначається значне погіршення точності у випадку наявності темних сонцезахисних окулярів. В процесі налаштування Face ID обличчя користувача сканується декілька разів в різних ракурсах, що забезпечує створення 3D-шаблону обличчя, який в тому числі використовується для підтвердження "живучості" при розпізнаванні

спуфінг-атак. На відміну від Face ID, засоби на платформі Android передбачають відеореєстрацію обличчя лише у видимому діапазоні світла. При цьому розпізнавання спуфінг-атак реалізується за рахунок виявлення відблисків, характерних для скляної або паперової поверхні, визначення кордонів пристрою, який використовується для демонстрації підробленого зображення, аналізу артефактів на зображенні (муар, розфокусування, дисторсія) та наявності мікрорміки обличчя. Зазначається зниження функціоналу засобів розпізнавання при зниженні рівня освітлення.

Таким чином, аналіз відомих прикладних систем біометричної автентифікації за ЗО та зображенням РОО свідчить про те, що в загальному випадку перспективи їх вдосконалення пов'язані з забезпеченням достатньої точності розпізнавання особи з урахуванням можливості реалізації спуфінг-атак в умовах нерівномірного освітлення та впливу завад. Оскільки результати [8 , 16, 18] свідчать про те, що основою таких систем являються нейромережеві засоби, то на наступному етапі було проаналізовано науково-прикладні роботи, присвячені таким засобам.

Відповідно до даних літературного огляду [9, 14, 17], на сьогодні відома велика кількість досліджень, присвячених застосуванню нейронних мереж для розпізнавання особи за ЗО та РОО. При цьому можна виділити декілька різних підходів до побудови мережі. В роботах [1, 4] нейронна мережа використовується для здійснення порівняння вхідного зображення тільки з одним зображенням із набору даних, які відповідають еталонам ЗО та РОО легітимних користувачів. У цьому випадку процес автентифікації передбачає послідовне порівняння вхідного зображення із всіма зображеннями, асоційованими з кожним із користувачів.

В роботі [12] пропонується використовувати нейронну мережу, навчену на прикладах зображень, які відповідають всім легітимним користувачам. Тобто така нейронна мережа вирішує задачу віднесення вхідного зображення до одного із наперед визначених класів легітимних користувачів. Хоча точність розпізнавання такої моделі вважається дещо вищою, однак її серйозним недоліком являється складність внесення даних нового користувача, що зумовлена необхідністю повного перенавчання моделі. При цьому у першому випадку процедуру автентифікації можливо співвіднести з вирішенням задачі класифікації зображень, а в другому випадку – з вирішенням задачі порівняння зображень.

Ще один підхід, описаний у [5], передбачає використання додаткового нейромережевого модулю, призначеного для попередньої обробки зображень перед їх подачею у модуль розпізнавання. Також відомий підхід до нейромережевого розпізнавання особи на основі інтегрального аналізу ЗО та РОО [15]. Ще один аспект розробки нейромережевих засобів розпізнавання досліджено в роботах [6, 7], де запропоновано реалізовувати нейромережевий аналіз зображень у відеопотоці з урахуванням інформації декількох кадрів. При цьому в роботі [6] пропонується проводити розпізнавання на основі покадрового порівняння вхідного відеопотоку з еталонним зображенням. В роботі [3] показана доцільність розпізнавання спуфінг-атак на основі аналізу аномалій вхідного відеопотоку та динаміки емоцій, що проявляються на обличчі людини.

Оскільки задачу розпізнавання особи за ЗО та РОО відносять до класу задач нейромережевого аналізу зображень, то в більшості відомих рішень в якості базису використовують один із апробованих типів згорткових нейронних мереж, що забезпечує досягнення досить високої точності та швидкості розпізнавання. Разом з тим, у відомих НММ, що використовуються для біометричної автентифікації, недостатньо повно враховано сучасні досягнення в області семантичної сегментації зображень, що можуть знайти своє застосування при попередній обробці вхідного зображення для виділення кордонів ЗО та РОО. Крім того, специфіка різних ОКІ, пов'язаних з оперативністю оновлення набору даних персоналу вказаних об'єктів, накладає такі обмеження, які складно забезпечити в монолітній НММ, побудованій на основі підходу до класифікації зображень або підходу до порівняння зображень, що можливо компенсувати за рахунок включення до складу моделі модулів з відповідною функціональністю.

Мета та постановка завдання

Метою дослідження є розробка модульної нейромережевої моделі, що забезпечує ефективну автентифікацію за зображенням обличчя та райдужною оболонкою ока на об'єкті критичної інфраструктури з урахуванням необхідності розпізнавання спуфінг-атак та оперативного оновлення даних щодо переліку легітимних представників персоналу об’єкту.

Виклад основного матеріалу дослідження

Базуючись на результатах проведеного літературного аналізу та даних [17, 14, 9], з урахуванням можливості попередньої обробки відеопотоку за допомогою класичних технологій, визначено, що до основних завдань нейромережевих засобів біометричної автентифікації персоналу ОКІ відносяться:

1. Виділення кордонів ЗО у піддослідному кадрі вхідного відеопотоку;
2. Детектування спуфінг-атак на основі візуальних артефактів, що відображаються за рахунок зміни текстури, кольору зображення, виникнення на ньому відблисків, розривів контурів зображення;
3. Детектування спуфінг-атак на основі артефактів зовнішнього оточення, наприклад, відображення обличчя на екрані мобільного пристрою або відсутність у відеокадрі предметів, які очікувано знаходяться у зоні відеореєстрації;
4. Виявлення областей завад, характерних для очікуваних умов відеореєстрації;
5. Виділення кордонів РОО;
6. Визначення множин координат контрольних і ключових точок, що використовуються для розпізнавання особи та емоцій;
7. Детектування спуфінг-атак за динамікою параметрів живучості (liveness detection parameters), що використовуються для розпізнавання відповідності зображення реальному обличчю живої людини;
8. Розпізнавання базових емоцій, відображених на обличчі;
9. Детектування спуфінг-атак на основі розпізнаних емоцій;

10. Розпізнавання особи представника персоналу об'єкту критичної інфраструктури.

Визначення вказаних завдань проведено з урахуванням апробованих рішень в області нейромережевого аналізу ЗО, включаючи РОО, та в області біометричної автентифікації. При цьому, з позицій реалізації нейромережевими засобами аналізу однорідних процесів, завдання детектування спуфінг-атак на основі спуфінг-артефактів розділено на два окремих завдання: детектування спуфінг-атак за візуальними артефактами та детектування спуфінг-атак за артефактами зовнішнього оточення.

Використовуючи результати [8, 16, 18], встановлено, що традиційні підходи до вирішення 1- 9 завдань передбачають використання класифікаційних згорткових нейронних мереж. Для вирішення 10 завдання крім класифікаційних використовуються згорткові нейронні мережі, адаптовані до задачі порівняння вхідних зображень. Класифікаційні згорткові нейронні мережі використовуються у випадку, коли не є критичним термін навчання, пов'язаний з внесенням в нейронну мережу даних нового представника персоналу, або із видаленням таких даних. Згорткові нейронні мережі, що призначені для порівняння зображень, використовуються у тому випадку, коли вказаний термін є критично важливим. Тому це завдання розділене на завдання 10.1 та 10.2.

Узагальнена структура модульної НММ, призначеної для вирішення перерахованих завдань, з урахуванням означених особливостей вирішення 10 завдання, показана на рис. 1. При формуванні даної структури передбачено, що виконання кожного окремого завдання реалізується за допомогою однойменного модулю.

Відповідно до відомих методів побудови нейромережевих засобів захисту інформації [10, 19], наступний етап розробки пов'язано з визначенням для кожного із модулів архітектури нейронної мережі, яка є найбільш ефективною в сенсі вирішення завдання даного модулю. Використано описаний в [19] підхід, що передбачає: визначення множини перспективних архітектур, розрахунок за допомогою виразу (1) значення функції ефективності кожної архітектури та вибір архітектур з найбільшим значенням функції ефективності:

$$E_i = \sum_{v=1}^{V} \alpha_v e_{d,v}, \qquad (1)$$

де E_i – ефективність архітектури і-ої архітектури; V – кількість критеріїв ефективності; α_v– ваговий коефіцієнт v-го критерію ефективності; $e_{d,v}$ – значення v-го критерію ефективності для і-ої архітектури.

Відповідно до [17], в базовому варіанті до критеріїв ефективності віднесено: точність розпізнавання (e_1); обчислювальну складність розпізнавання (e_2); пристосованість до розпізнавання в реальному масштабі часу (e_3); апробованість при вирішенні завдань, аналогічних до завдання модулю (e_4); доступність інструментального забезпечення (e_5). Крім того, до переліку критеріїв ефективності включено критерії, що співвідносяться із наявністю доступної попередньо навченої НММ (e_6) та із можливістю пройти донавчання задля досягнення заданих показників в умовах поставленого завдання (e_7). Це пояснюється складністю формування репрезентативних навчальних вибірок, високою обчислювальною ресурсоємністю процесу навчання, можливою необхідністю адаптації нейронної мережі до особливостей поставленого завдання та наявністю доступних апробованих переднавчених нейронних мереж, що забезпечують ефективне вирішення широкого спектру задач в області комп'ютерного зору.

Рис. 1. Структура модульної НММ

Враховуючи складність експертного оцінювання значень вказаних критеріїв, для їх оцінювання використана бінарна шкала. Значення критерію дорівнює 1, якщо відповідна вимога забезпечена, та дорівнює 0 у протилежному випадку. При цьому e_1 встановлювалось рівним 1 у випадку, якщо заявлена точність розпізнавання нейронної мережі була більшою ніж 0,95. При розрахунках виразу (1) прийняті наступні значення вагових коефіцієнтів: $\alpha_1 = 0{,}2$, $\alpha_1 = 0{,}1$, $\alpha_1 = 0{,}14$, $\alpha_1 = 0{,}14$, $\alpha_1 = 0{,}14$, $\alpha_1 = 0{,}14$, $\alpha_1 = 0{,}14$. Підвищення вагомості критерію e_1 пояснюється підвищеними вимогами до точності розпізнавання особи на об'єктах критичної інфраструктури, а зменшення вагомості критерію e_2– доступністю потужного апаратного забезпечення, що може частково компенсувати високу обчислювальну складність розпізнавання загальновідомих НММ.

Використавши наведений підхід для кожного із означених завдань, визначено множину ефективних архітектур нейронних мереж, що дозволило сформувати наведену в табл.1 матрицю відповідності архітектур нейронних мереж до основних завдань нейромережевих засобів біометричної автентифікації персоналу ОКІ.

Зазначимо, що для наведених в табл. 1 архітектур значення функції ефективності знаходиться в межах від 0,95 до 1. При цьому наявність в табл. 1 на перетині рідка з назвою архітектури та колонки з номером завдання позначки «+» означає, що у вільному доступі є відповідне апробоване, доступне для модифікації програмне забезпечення, задекларовані можливості якого забезпечують вирішення вказаного завдання. Позначка «+/-» стосується мережі DeepPixBiS та свідчить про обмежені можливості даної мережі при детектуванні спуфінг-атак за артефактами зовнішнього оточення, які стосуються об'єктів, що мають бути зафіксовані при відеореєстрації обличчя. Також ця позначка стосується можливості застосування мережі Face Mesh для виділення контурів РОО та свідчить про те, що хоча дана мережа і строго кажучи не виділяє контур, однак визначає ключові точки, які стосуються РОО. Цифри в колонці з номером завдання 6 вказують кількість ключових точок, що визначаються на обличчі при використанні відповідної нейронної мережі. Позначка «!» означає, що відповідне програмне забезпечення у вільному доступі відсутнє, але наявність відкритого програмного коду, доведена ефективність в дотичних областях та доступність репрезентативних наборів даних забезпечують можливість реалізації відповідної розробки.

Таблиця 1

Матриця відповідності архітектур нейронних мереж до основних завдань нейромережевих засобів біометричної автентифікації персоналу ОКІ

Архітектура	Номер завдання										
	1	2	3	4	5	6	7	8	9	10.1	10.2
MTCNN	+					5					
RetinaFace	+					5					
BlazeFace	+					5					
U-Net	!		!	!	!	!					
DeepPixBiS		+	+/-				+				
FaceNet										+	
Face Mesh					+/-	468					
Open Face						68		+			
Face Alignment Network						68					
MobileNet					!	!			!		!
Siamese Network										!	
Two_channel Networks										!	

Використовуючи дані табл. 1, проведено дослідження, спрямовані на уточнення перспектив застосування представлених в ній нейронних мереж для вирішення відповідних завдань, що реалізуються відповідними модулями в різних умовах експлуатації на об'єктах критичної інфраструктури. Для цього проведено дві серії експериментів. В першій серії проведено уточнення заявлених можливостей нейронних мереж, позначених символом «+» в табл. 1, а в другій серії експериментів перевірено можливості авторської реалізації нейронних мереж, позначених символом «!». Хід проведення першої серії експериментів проілюстровано за допомогою рис. 2-3, на яких показано результати застосування мережі Face Mesh для нанесення ключових точок на ЗО, виділеного на фотокартці за допомогою мережі BlazeFace. На рис. 2 показано результати нанесення ключових точок на обличчя чоловіка європеоїдної раси, зареєстроване без впливу завад та у випадку наявності на обличчі медичної маски. На рис. 3 показано результати нанесення ключових точок на обличчя чоловіка монголоїдної раси, зареєстроване без впливу завад, у випадку наявності на обличчі медичної маски та у випадку наявності темних окулярів.

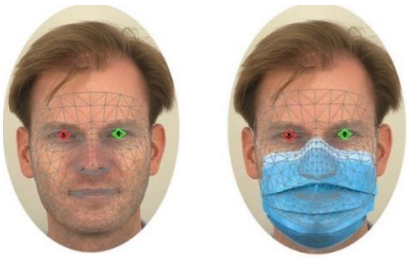

Рис. 2. Нанесення ключових точок на обличчя чоловіка європеоїдної раси

Рис. 3. Нанесення ключових точок на обличчя чоловіка монголоїдної раси

Результати першої серії експериментів показали можливість ефективного застосування мереж MTCNN, RetinaFace та BlazeFace для виділення у кадрах відеопотоку прямокутної області, що відповідає обличчю людини незалежно від її статі та раси як у випадку відсутності завад при відеореєстрації, так і у випадках наявності типових завад, що перекривають біля 60% площі обличчя. При цьому:

- мережа BlazeFace забезпечує при помірній точності найбільш високу швидкодію та можливість розгортання на пристроях з обмеженою обчислювальною потужністю;

- мережа MTCNN завдяки каскадній структурі є найбільш точною при необхідності виділення обличчя на зображеннях з різними розмірами та різною роздільною здатністю. Однак каскадна структура MTCNN зумовлює її відносно низьку швидкодію, що ускладнює оперативний аналіз відеопотоку. Також слід відзначити низьку точність виділення у випадку, коли розмір обличчя займає менше 10% зображення;

- мережа RetinaFace забезпечує найбільш високу точність виділення обличчя, зафіксованого в різних ракурсах, по відношенню до MTCNN, має вищу швидкодію, однак потребує апаратного забезпечення з високою обчислювальною потужністю.

При виборі мережі слід враховувати розмір вхідного поля, що для MTCNN становить 320x240 або 640x480 пікселів, для RetinaFace - 640x640 або 800x800 пікселів, а для BlazeFace - 128x128 або 256x256 пікселів.

Також визначено, що використання мережі Face Mesh для виділення ключових точок можливо лише при відсутності завад на обличчі. В протилежному випадку мережа Face Mesh наносить на обличчя точки, які перекриваються завадами, а тому не можуть бути використані для розпізнавання особи та емоцій.

Мережа DeepPixBiS забезпечує задовільне розпізнавання спуфінг-атак:

- за візуальними артефактами типу зміна текстури та кольору зображення, неприродні відблиски та тіні, неприродні варіації відстаней між різними частинами обличчя;

- за живучістю, що оцінюється за наявністю рухів обличчя та мімікою;

- за артефактами зовнішнього оточення, пов'язаними з кордонами маски та відблисками і кордонами екрану, що використовується для демонстрації обличчя.

Разом з тим, мережа DeepPixBiS не забезпечує можливості розпізнавання спуфінг-атак на основі зображень об'єктів, що мають бути зареєстровані одночасно з ЗО в процесі біометричної автентифікації. Це пов'язано зі складністю оперативного донавчання мережі. Характеристики мереж FaceNet, Face Alignment Network та OpenFace відповідають заявленим можливостям, однак їх функціональність значно погіршується у випадку наявності завад та зміни очікуваних умов відеореєстрації. В другій серії експериментів увагу було акцентовано на визначенні можливостей означених в табл. 1 нейронних мереж для вирішення тих завдань, для яких нейромережеві інструментальні засоби у вільному доступі не знайдено. В першу чергу досліджено можливість мереж типу Siamese Network та Two_channel Networks для визначення легітимності особи представника персоналу ОКІ за рахунок порівняння зареєстрованого ЗО з ЗО легітимних користувачів.

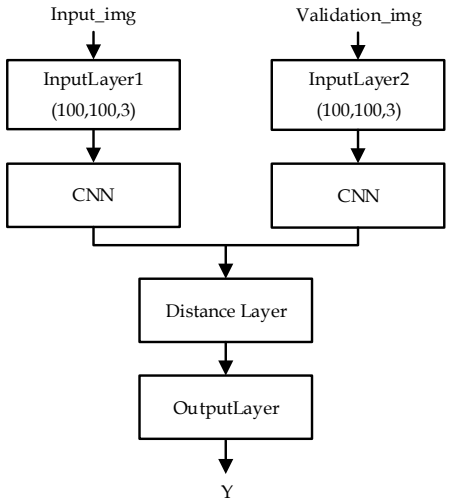

Рис. 4. Загальна структура мережі Siamese Network, призначеної для розпізнавання особи

Загальна структура мережі Siamese Network, що була використана в авторській реалізації відповідного програмного комплексу, показана на рис. 4. Відмінності авторської реалізації від базового варіанту Siamese Network полягають у модифікації архітектурних параметрів нейронної мережі, яка була використана в якості базису окремих гілок Siamese Network. Також передбачено, що в залежності від розмірів вхідного зображення в базову структуру мережі Two_channel Networks слід вносити зміни, що забезпечують зведення розмірів вхідного зображення до 1 пікселя.

Зазначимо, що в Siamese Network відмінність між двома вхідними зображеннями розраховується на основі манхетенської відстані між вихідними сигналами кожної із двох ЗНМ, що входять до її складу:

$$L_1 = \sum_{i=1}^{I} |y_{1,i} - y_{2,i}|, \qquad (2)$$

де $y_{1,i}$, $y_{2,i}$ – і-ий вихідний сигнал першої та другої ЗНМ; I - кількість вихідних нейронів в ЗНМ.

В авторській реалізації Siamese Network, адаптованій до аналізу трьохканальних зображень розміром 100 на 100 пікселів, I=4096.

Особливістю математичного забезпечення Two_channel Networks є використання в якості функції втрат функції Hinge Loss, розрахунок якої здійснюється за допомогою виразу (3).

$$\text{H\_Loss} = max(0; 1 - y_e \times y_r), \qquad (3)$$

де y_e – очікуваний вихідний сигнал; y_r – реальний вихідний сигнал.

У випадку, коли в процесі навчання на вхід мережі Two_channel Networks подаються зображення, що класифікуються як однакові, $y_e = 1$, а у протилежному випадку $y_e = -1$.

Графіки, які ілюструють параметри динаміки навчання Siamese Network та Two_channel Networks, показані на рис. 5 та на рис. 6. Для навчання Siamese Network та Two_channel Networks використано набір даних LFW (Labeled Faces in the Wild), який є у вільному доступі за посиланням https://vis-www.cs.umass.edu/lfw/. До складу LFW входять приблизно 13000 фотографій з ЗО, зафіксованими у різних ракурсах. Розмір кожного зображення 250x250 пікселів, роздільна здатність 96 dpi, кольорова модель RGB, глибина кольору 24 біт. Перед подачею на вхід нейронної мережі розміри зображення підлягали масштабуванню методом бікубічної інтерполяції.

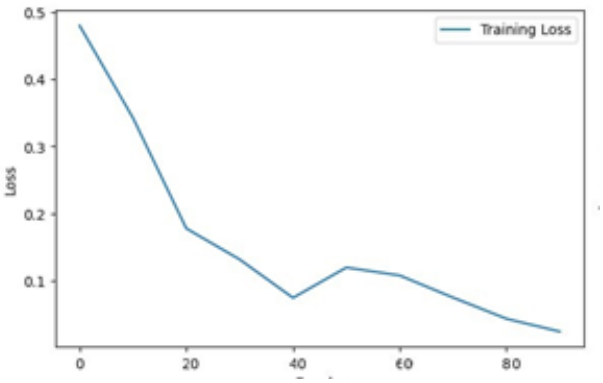

Рис. 5. Графіки динаміки показника Loss навчання мережі Siamese Network, що призначена для розпізнавання особи на основі порівняння зображень обличчя

Як свідчать показані на рис. 5 та на рис. 6 графіки, процес навчання мереж Siamese Network та Two_channel Networks достатньо стабільний та здійснюється за відносно невелику кількість епох. При цьому після 80 епохи навчання для мережі Siamese

Network показник Loss (співвідноситься з мірою невідповідності між передбаченнями нейронної мережі та фактичними мітками даних) дорівнює 0,02, показники Accuracy (частка правильних передбачень серед усіх передбачень, визначених нейронною мережею), Precision (частка правильних позитивних передбачень серед усіх передбачених позитивних випадків), Recall (частка правильних позитивних передбачень серед усіх реальних позитивних випадків) дорівнюють 0,99. Для мережі Two_channel Networks досягнення приблизно таких самих значень параметрів Loss, Accuracy, Precision та Recall відбувається вже після 50 епохи навчання.

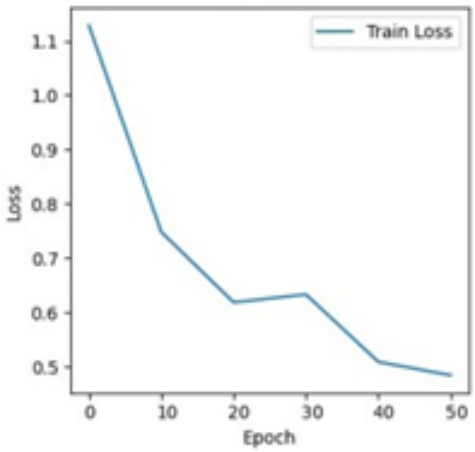

Рис. 6. Графіки динаміки показника Loss навчання мережі Two_channel Networks, що призначена для розпізнавання особи на основі порівняння зображень обличчя

Таким чином, експериментальні дослідження підтвердили доцільність застосування мереж Siamese Network та Two_channel Networks для визначення легітимності представника персоналу OKI за рахунок розпізнавання особи, що реалізується шляхом порівняння зареєстрованого ЗО із ЗО легітимних представників. Разом з тим, порівняння динаміки параметрів навчання Siamese Network та Two_channel Networks свідчать про те, що з точки зору оперативності навчання більш ефективною являється мережа Two_ channel Networks. При цьому кількість вагових коефіцієнтів Siamese Network становить 38964545, а кількість вагових коефіцієнтів Two_ channel Networks становить 2570849. Тобто обчислювальна ресурсоємність Two_channel Networks приблизно в 15 разів менша, ніж обчислювальна ресурсоємність Siamese Network, що являється ще однією перевагою Two_channel Networks. Разом з тим, до переваг Siamese Network слід віднести гнучкість концепції її побудови, яка потенційно дозволяє значно підвищити її ефективність за рахунок використання в блоці CNN найбільш передових нейромережевих архітектур, адаптованих до аналізу зображень обличчя. Наприклад, в блоці CNN замість традиційно використаної архітектури типу LeNet можливо використати архітектуру типу MobileNet, що було підтверджено за допомогою оціночних експериментальних досліджень. Таким чином, за необхідності оперативного розгортання системи біометричної автентифікації пріоритет слід віддати мережі Two_channel Networks, однак при відсутності жорстких обмежень щодо терміну та ресурсів на розробку доцільно провести дослідження, спрямовані на розробку модифікованої мережі Siamese Network.

Експерименти, пов'язані з дослідженням мереж U-Net та MobileNet, показали доцільність їх застосування при вирішенні відповідних їм завдань, перерахованих в табл. 1. При цьому в завданні 6 (визначення множин координат контрольних і ключових точок) в умовах обмеженості ресурсів пріоритет має мережа MobileNet, а застосування U- Net можливо співвіднести з необхідністю забезпечення високої точності результатів. Також при вирішенні завдання 6 перевагами засобів на основі U- Net та MobileNet відносно наведеного в табл. 1 доступного інструментального забезпечення на основі мереж MTCNN, RetinaFace, BlazeFace, Face Mesh, OpenFace та Face Alignment Network являється можливість визначення множини ключових точок, що відповідають конкретним умовам поставленої задачі. Доцільність застосування мережі U-Net при вирішенні завдання 1 (виділення кордонів ЗО) пояснюється можливістю точного виділення саме контурів кордонів ЗО, а не обрамлення ЗО за допомогою прямокутної рамки, характерної для мереж MTCNN, RetinaFace, BlazeFace, що проілюстровано за допомогою рис. 7.

Рис. 7. Виділення кордонів ЗО у вигляді контуру та у вигляді прямокутної рамки

Зазначимо, що виділення кордонів ЗО за допомогою прямокутної рамки призводить до того, що на рисунку, який подається для подальшого аналізу, можуть бути присутні сторонні об'єкти, які негативно впливають на точність розпізнавання особи представника персоналу OKI. Відповідно, використання U-Net дозволяє запобігти виникненню вказаного недоліку. Крім того, ефективність застосування архітектури U-Net для вирішення завдань, означених в табл. 1, може бути підвищена за рахунок застосуванню в кодері та декодері моделі замість мережі VGG інших, більш сучасних типів НММ, характеристики яких забезпечують можливість достатньо точного виділення контурів ЗО при зменшенні обсягу обчислювальних ресурсів. Таким чином, результати другої серії експериментів дозволили окреслити умови доцільності застосування мереж типу U-Net, MobileNet, Siamese Network та Two_channel Networks для вирішення відповідних їм завдань, означених в табл.1. В цілому результати експериментальних досліджень свідчать про те, що для вирішення кожного із основних завдань нейромережевих засобів біометричної автентифікації персоналу OKI можливо використовувати декілька із наведених в табл.1 типів нейронних мереж, ефективність яких залежить від конкретних умов застосування. Таким чином, остаточний склад запропонованої модульної НММ має бути сформований з урахуванням особливостей поставленої задачі біометричної автентифікації персоналу OKI, що визначає необ-

хідність проведення подальших досліджень в напрямку створення відповідного методу адаптації модульної НММ до очікуваних умов застосування для біометричної автентифікації персоналу ОКІ.

Висновки. В результаті проведених досліджень розроблено модульну нейромережеву модель, що забезпечує ефективну автентифікацію персоналу за зображенням обличчя та райдужною оболонкою ока на об'єкті критичної інфраструктури з урахуванням необхідності розпізнавання спуфінг-атак та оперативного оновлення даних щодо переліку легітимних представників персоналу об'єкту. Передбачено співставлення функціоналу модулів з вирішенням завдань біометричної автентифікації, які загальноприйнято вирішувати за допомогою окремої нейромережевої моделі. При обґрунтуванні можливості застосування в окремому модулі нейромережевої моделі певного типу застосовано підхід, що передбачає доцільність використання апробованих вільнодоступних нейромережевих засобів, інструментальне забезпечення яких можливо модифікувати під очікувані умови застосування. На основі запропонованого підходу, з урахуванням результатів проведених експериментальних досліджень, для кожного з модулів визначено альтернативні варіанти застосування нейромережевих моделей, функціонал яких співвідноситься з різними очікуваними варіантами умов застосування.

Також оригінальність запропонованої модульної нейромережевої моделі забезпечена розробкою авторських варіантів нейронних мереж, що дозволяють реалізувати: розпізнавання емоційного стану зареєстрованої особи; розпізнавання спуфінг-атак на основі природності емоцій та зображень фонових об'єктів, характерних для конкретних умов відеореєстрації; розпізнавання особи шляхом порівняння піддослідного зображення обличчя із зображеннями обличчя легітимного персоналу без необхідності донавчання моделі. Перспективи подальших досліджень доцільно співвіднести з формуванням остаточного переліку нейромережевих моделей, що входять до складу модулів, що визначає необхідність розробки відповідного методу адаптації модульної нейромережевої моделі до очікуваних умов застосування при біометричній автентифікації персоналу об'єктів критичної інфраструктури.

Список літератури

[1]. Ahmad Sabri N.I., Setumin S. One-Shot Learning for Facial Sketch Recognition using the Siamese Convolutional Neural Network. 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 2021, pp. 307-312. DOI: 10.1109/ISCAIE51753.2021.9431773.

[2]. Daniel N., Anitha A. Texture and quality analysis for face spoofing detection. Computers & Electrical Engineering, Volume 94, 2021, 107293, ISSN 0045-7906. DOI: 10.1016/j.compeleceng.2021.107293.

[3]. Edmunds T., Caplier A. Motion-based countermeasure against photo and video spoofing attacks in face recognition. Journal of Visual Communication and Image Representation, Volume 50, 2018, Pages 314-332, ISSN 1047-3203. DOI: 10.1016/j.jvcir.2017.12.004.

[4]. Hamdani N., Bousahba N., Bousbai A., Braikia A. Face Detection and Recognition Using Siamese Neural Network. International Journal of Computing and Digital System (Jāmiʿat al-Baḥrayn. Markaz al-Nashr al-ʻIlmī), 2023, Vol. 14, No. 1, pp. 889–897. DOI: 10.12785/ijcds/140169.

[5]. Hangaragi S., Singh T., Neelima N. Face Detection and Recognition Using Face Mesh and Deep Neural Network. Procedia Computer Science, Volume 218, 2023, pp. 741-749, ISSN 1877-0509. DOI: 10.1016/j.procs.2023.01.054.

[6]. Kumar C.R., Saranya N., Priyadharshini M., Gilchrist E.D., Rahman M.K. Face recognition using CNN and siamese network. Measurement: Sensors, Vol. 27, 2023, 100800, ISSN 2665-9174.

[7]. Li L., Correia P.L., Hadid A. Face recognition under spoofing attacks: countermeasures and research directions. IET Biometrics, 2018, Vol. 7, pp. 3-14.

[8]. Ma Y., Wu L., Li Z., Liu F. A novel face presentation attack detection scheme based on multi-regional convolutional neural networks. Pattern Recognition Letters, Volume 131, 2020, pp. 261-267, ISSN 0167-8655.

[9]. Muthukumaran B., Harshavarthanan L., Dhyaneshwar S., Sharief M.Z. Face and Iris based Human Authentication using Deep Learning. 2023. 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 841-846.

[10]. Osa E., Orukpe P.E., Iruansi U. Design and implementation of a deep neural network approach for intrusion detection systems. e-Prime - Advances in Electrical Engineering, Electronics and Energy. Vol. 7, 2024, 100434, ISSN 2772-6711.

[11]. Perdana R.N., Ardiyanto I., Nugroho H.A. A Review on Face Anti-Spoofing. IJITEE (International Journal of Information Technology and Electrical Engineering), 2021. Vol. 5, No. 1, pp. 29.

[12]. Pranav K.B., Manikandan J. Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks. Procedia Computer Science. Vol. 171, 2020, pp. 1651-1659, ISSN 1877-0509.

[13]. Tran H.N., Phan P.H., Nguyen K.H., et al. Augmentation-Enhanced Deep Learning for Face Detection and Emotion Recognition in Elderly Care Robots. PREPRINT, 07 February 2024, Research Square.

[14]. Wang Y., Tan T., Jain A.K. Combining Face and Iris Biometrics for Identity Verification. In: Kittler J., Nixon M.S. (eds) Audio- and Video-Based Biometric Person Authentication. AVBPA 2003, Lecture Notes in Computer Science. Vol. 2688. Springer, Berlin, Heidelberg. 2003.

[15]. Yergesh A.K. Development of an advanced biometric authentication system using iris recognition based on a convolutional neural network. Herald of Science. Vol. 2, no. 5 (74), 2024, pp. 615-625.

[16]. Бушуєв С.Д., Кулаков Ю.О., Терейковська Л.О., Терейковський І.А., Терейковський О.І. Нейромережева модель детектування кордонів обличчя людини. Науково-технічний збірник «Управління розвитком складних систем» Київського національного університету будівництва і архітектури, 2022. Вип. 51, С. 5-11.

[17]. Корченко О.Г., Терейковський О.І. Аналіз та оцінювання засобів біометричної аутентифікації за

зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка, №1(21), 2023. С. 136-148.

[18]. Корченко О.Г., Терейковський О.І. Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів. Захист інформації, №1(26), 2024. С. 157-170.

[19]. Терейковський І.А., Заріцький О.В., Терейковська Л.О., Погорелов В.В. Метод розробки архітектури глибокої нейронної мережі, призначеної для розпізнавання комп'ютерних вірусів. Захист інформації, Том 20, № 3 (2018). С. 188-199.

УДК 681.3.06

Korchenko O., Tereikovskyi O. Model of the facial recognition procedure model and the iris of the eye during biometric authentication of personnel of critical infrastructure facilities using neural network tools

Abstract. *The problematics of the article is related to increasing the effectiveness of biometric authentication systems for personnel of critical infrastructure facilities. It is shown that the prospects of increasing efficiency should be correlated with the improvement of neural network tools used in the process of biometric authentication. As a result of the conducted research, a modular neural network model was developed that provides effective authentication of personnel based on the image of the face and the iris of the eye at a critical infrastructure facility, taking into account the need to recognize spoofing attacks and promptly update data on the list of legitimate personnel representatives of the facility. The novelty of the proposed modular neural network model consists in the application of the author's variants of neural networks, which allow to realize the recognition of the emotional state of the registered person, the recognition of spoofing attacks based on the naturalness of emotions and images of background objects characteristic of specific conditions of video registration, and the recognition of a person by comparing the test image faces with images of the faces of legitimate personnel, which makes it possible to quickly respond to a change in the list of legitimate personnel representatives of a critical infrastructure object without the need to retrain the model.*

Keywords: *biometric authentication; person recognition; face image; iris of the eye; neural network; critical infrastructure object.*

Корченко Олександр Григорович, член-кореспондент НАН України, лауреат Державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України, доктор технічних наук, професор, перший проректор Державного університету інформаційно-комунікаційних технологій, професор Університету Комісії Народної Освіти (Краків, Польща).

Oleksandr Korchenko, Corresponding Member of the National Academy of Sciences of Ukraine, laureate of the State Prize of Ukraine in the field of Science and Technology, Honored Worker of Science and Technology of Ukraine, Dr Hub. (Eng), Professor, first vice-rector, State University of Information and Communication Technologies, Professor of the National Education Commission of the University, Krakow, Poland.

Терейковський Олег Ігорьович, аспірант, Національний авіаційний університет.

Oleh Tereikovskyi, PhD student, National Aviation University.

Отримано *18 червня 2024 року,* затверджено редколегією *26 червня 2024 року*