КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.866
УДК 004.934

Корченко Олександр Григорович
член-кореспондент НАН України, доктор технічних наук, професор, перший проректор
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0003-3376-0631
agkorchenko@gmail.com

Терейковський Олег Ігоревич
аспірант кафедри кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0001-5045-0163
tereikovskyio@gmail.com

МЕТОД БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ПЕРСОНАЛУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ЗОБРАЖЕННЯМ ОБЛИЧЧЯ ТА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА ІЗ ЗАСТОСУВАННЯМ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ

Анотація. Широке впровадження нейромережевих засобів біометричної аутентифікації за зображеннями обличчя та райдужною оболонкою ока на об'єктах критичної інфраструктури дозволило підвищити рівень безпеки та оперативності ідентифікації персоналу. Водночас сучасні вимоги зумовлюють потребу в підвищенні стійкості до спуфінг-атак, адаптивності до завад реального середовища, а також у розширенні функціональності для врахування психоемоційного стану персоналу в момент проходження автентифікації. Традиційні нейромережеві методи, що базуються на нейронних мережах з монолітною архітектурою обмежені в реалізації цих вимог через недостатню гнучкість і складність адаптації до варіативних умов відеореєстрації. Тому в даній статті запропоновано метод біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережевих засобів. Метод реалізує багатокрокову адаптивну обробку відеопотоку та комплексне виконання процедур, необхідних для ефективної автентифікації в умовах варіативності параметрів зображення. Етапи методу структуровано як послідовність процедур, що відповідають типовим завданням біометричної автентифікації, кожне з яких реалізується окремою нейромережею. Уперше в межах єдиної архітектури забезпечено багаторівневий аналіз ознак спуфінг-атак із урахуванням візуальних артефактів обличчя, артефактів зовнішнього оточення, динаміки параметрів живучості та емоційного стану. Запропоновано механізм автоматичного оцінювання показників відображення, динамічного формування множини придатних до обробки зображень і їх попередньої обробки для підвищення якості. Фільтрація завад здійснюється шляхом семантичної сегментації та поелементного маскування піксельних областей, що дозволяє виключати з обробки ділянки із тінями, перекриттями чи сторонніми об'єктами. Ключовою особливістю є цілеспрямоване використання доступних і апробованих наперед навчених нейромережевих моделей з відкритим кодом (FaceMeshV2, Visual Transformer, DeepPixBiS, Siamese Network, Two_channel Networks, MobileNet), адаптованих до умов відеореєстрації на об'єктах критичної інфраструктури. За попередніми оцінками, застосування адаптивної обробки відеопотоку та багаторівневого аналізу спуфінг-атак дозволяє підвищити точність виявлення спуфінгу на 25–35 % і щонайменше в 1,5 раза скоротити час розробки системи на основі відкритих моделей.

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

© О.Г. Корченко, О.І. Терейковський, 2025

ВСТУП

Практичний досвід і результати науково-технічних публікацій [2], [4], [8] підтверджують, що однією з пріоритетних задач у сфері захисту об'єктів критичної інфраструктури (ОКІ) є підвищення ефективності систем автентифікації персоналу. Ключовим напрямом у цьому контексті є вдосконалення засобів біометричної автентифікації (БА), які відносяться до основних компонент означених систем. Незважаючи на використання різних біометричних параметрів (БП), найбільш поширеним залишається аналіз зображення обличчя — завдяки доступності відеокамер і відпрацьованим технологіям, що дозволяють здійснювати автентифікацію як на вході, так і в процесі виконання обов'язків. Разом із тим, у працях [10], [15], [22] наголошується на обмеженнях сучасних систем: недостатня ефективність протидії спуфінг-атакам, висока ресурсоємність та обмежена точність нейромережевих моделей (НММ), відсутність механізмів оцінки емоційного стану, а також слабка інтеграція з іншими БП, що можуть бути зареєстровані одночасно. Окремо підкреслюється доцільність поєднання автентифікації за зображенням обличчя (ЗО) та за райдужною оболонкою ока (РОО), що базується на доступності відеокамер з високою якістю реєстрації. Також зазначається, що недостатня ефективність нейромережевих засобів (НМЗ) БА персоналу ОКІ багато в чому пов'язана з недоліками методологічних підходів до їх розроблення, налаштування та адаптації до конкретних умов застосування

Постановка проблеми. Вдосконалення методологічного забезпечення побудови нейромережевих засобів біометричної автентифікації персоналу об'єктів критичної інфраструктури на основі зображення обличчя та райдужної оболонки ока.

Аналіз останніх досліджень і публікацій. Оскільки в загальному випадку шляхи підвищення ефективності засобів БА персоналу ОКІ доцільно пов'язати з виправленням їх недоліків, то перший етап аналізу присвячено розгляду відомих засобів відповідного призначення. Система FACETEC (www.facetec.com) забезпечує 3D-моделювання обличчя зі звичайної 2D-камери та протидію багатьом видам атак, включаючи маски, зображення, відеопроєкції й спроби використання мертвих облич. Її перевагою є висока точність і багаторівнева перевірка «живучості», однак недоліками залишаються значна вартість і високі вимоги до обладнання. Система Face Verification & Liveness компанії Acuity (www.acuitymi.com) орієнтована на перевірку справжності документів і дистанційну автентифікацію користувачів. Система має закриту архітектуру, що ускладнює адаптацію до специфічних потреб ОКІ. Пакет IDLive від ID R&D (https://www.idrnd.ai/passive-facial-liveness/) підтримує автономну роботу на мобільних пристроях і протидію атакам із використанням віртуальних і зовнішніх камер. Його обмеження полягають у відсутності розширеної мультибіометрії та обмежених механізмах виявлення емоцій. Система VisionLabs (https://visionlabs.ai/) забезпечує розпізнавання особи за фото і відео, визначення віку, статі, емоцій та оцінку якості зображення. До переваг належать багатофакторна перевірка «живучості» і високі показники точності. Недоліками є значна ресурсоємність моделей і обмеженість відкритого інструментарію. Система MegaMatcher (Neurotechnology) (https://www.neurotechnology.com/megamatcher-abis.html) реалізує автентифікацію на основі поєднання кількох біометричних ознак, зокрема обличчя і райдужної оболонки, відповідає міжнародним стандартам і демонструє високу точність. При цьому система є складною для інтеграції і вимагає значних обчислювальних ресурсів. Система Iris Access (https://www.irisid.com/productssolutions/irisaccesssystem/) орієнтована переважно на розпізнавання райдужної оболонки ока з близької відстані, має функцію автоматичного налаштування, однак не підтримує комплексної перевірки обличчя і поведінкових ознак.

Система Blink Identity (https://www.blinkidentity.com/) спеціалізується на швидкій ідентифікації великої кількості осіб у русі. Сильними сторонами є висока продуктивність і збереження біометричних шаблонів у безпечному вигляді, проте обмеженням виступає слабка адаптивність до детальної мультибіометричної перевірки. Система AxxonSoft (www.axxonsoft.com) дозволяє здійснювати пошук обличчя за фото або відео, інтегрується з базами державних органів і застосовується у масових місцях. Обмеженням є відсутність розвинених механізмів контролю «живучості» та оцінки емоційного стану.

Також проаналізовано можливості засобів ідентифікації особи на мобільних пристроях Apple і Android. Технологія Face ID (Apple) виконує відеореєстрацію у видимому та інфрачервоному діапазонах і створює 3D-шаблон обличчя за допомогою проєкції ключових точок. Система адаптована до більшості завад (макіяж, головні убори, маски), окрім темних сонцезахисних окулярів, що суттєво знижують точність. Розпізнавання «живучості» реалізується виключно шляхом аналізу мікрорухів і стану очей. На платформі Android відеореєстрація здійснюється лише у видимому спектрі. Спуфінг-атаки визначаються лише за ознаками відблисків, кордонів демонстраційних пристроїв, артефактів (муар, дисторсія, розфокусування) та міміки обличчя. Недоліком є зниження точності при поганому освітленні та відсутність інфрачервоного підсвічування.

Загалом, аналіз засвідчив, що існуючі рішення базуються на використанні НМЗ і хоча і демонструють високі показники точності, вони часто мають такі недоліки, як залежність від ресурсомістких моделей, відсутність комплексного аналізу множини біометричних ознак і обмежена відкритість інструментальних засобів для інтеграції та адаптації під специфічні вимоги ОКІ. При цьому результати достатньо ґрунтовного аналізу, проведеного в [8], [11], [13] вказують на те, що означені недоліки безпосередньо пов’язані з недосконалістю загальноприйнятих методологічних засад розробки НМЗ БА персоналу ОКІ за ЗО та РОО, які полягають у недостатній адаптації до розпізнавання широкого спектру спуфінг-атак, високій ресурсоємності нейромережевих моделей, обмежені точності розпізнавання біометричних ознак, відсутності механізмів оцінки емоційного стану персоналу та слабку інтеграцію різних біометричних параметрів у єдиній архітектурі. Разом із тим, авторські напрацювання в цій області дозволяють обґрунтовано стверджувати, що перспективи підвищення ефективності НМЗ БА персоналу ОКІ доцільно пов’язати з комплексною реалізацією запропонованих у [10] – [12] моделей процедури розпізнавання особи, модульної НММ та моделі семантичної сегментації ЗО.

Мета статті. Розробка методу біометричної аутентифікації персоналу об’єктів критичної інфраструктури, що за рахунок підтримки мультибіометричної автентифікації за зображенням обличчя та райдужної оболонки ока, адаптивної обробки відеопотоку, багаторівневому аналізу ознак спуфінг-атак та застосуванні доступних і апробованих нейромережевих засобів забезпечить підвищення ефективності відповідних систем.

РОЗРОБКА ТА ДОСЛІДЖЕННЯ

Використавши результати літературного аналізу та авторські напрацювання в області розробки НМЗ БА визначено, що в методі БА персоналу ОКІ за ЗО та РОО із застосуванням НМЗ доцільно врахувати необхідність реалізації означених в [1], [7], [20] процедур попередньої обробки вхідного відеопотоку та необхідність реалізації означених в [11], [21] процедур обробки відепотоку із застосуванням нейронних мереж. Базуючись на запропонованому підході, реалізація методу БА передбачає виконання етапів, що співвідносяться з реалізацією процедур: перевірки відповідності параметрів

зареєстрованого відеопотоку допустимим значенням, попередньої обробки відеопотоку, виділення кордонів ЗО у піддослідному кадрі вхідного відеопотоку, детектування спуфінг-атак на основі візуальних артефактів, детектування спуфінг-атак на основі артефактів зовнішнього оточення, виявлення областей завад, характерних для очікуваних умов відеореєстрації, виділення кордонів РОО, визначенням множин координат контрольних і ключових точок на ЗО, детектування спуфінг-атак за динамікою параметрів живучості, розпізнавання базових емоцій, детектування спуфінг-атак на основі розпізнаних емоцій, розпізнавання особи представника персоналу ОКІ. Узагальнена схема реалізації даного методу показана на рис. 1.

Зазначимо, що реалізація процедур виділення кордонів ЗО у піддослідному кадрі вхідного відеопотоку, виявлення областей завад, характерних для очікуваних умов відеореєстрації та виділення кордонів РОО асоціюється з виконанням етапу 3, а реалізація процедур детектування спуфінг-атак на основі візуальних артефактів, детектування спуфінг-атак на основі артефактів зовнішнього оточення, детектування спуфінг-атак за динамікою параметрів живучості та детектування спуфінг-атак на основі розпізнаних емоцій з виконанням етапу 4.

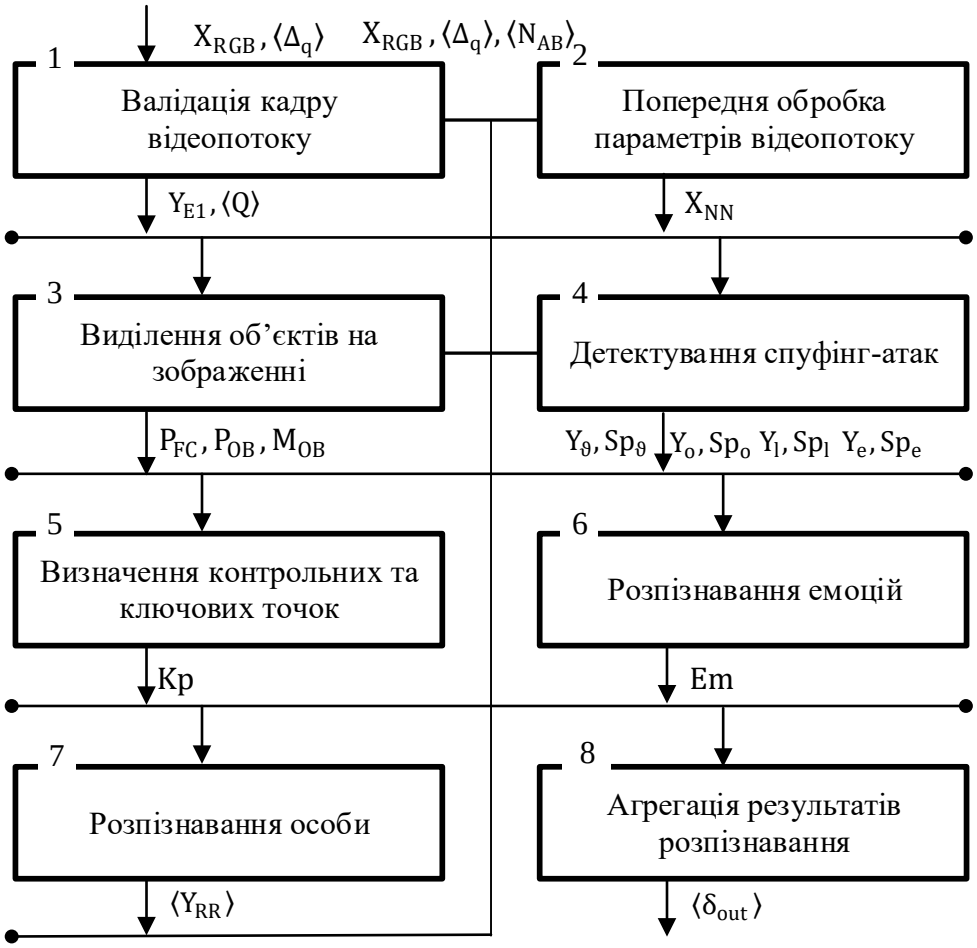

Рис. 1. Узагальнена схема реалізації методу біометричної аутентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережевих засобів

Етап 1. **Валідація кадру відеопотоку**. На вхід етапу подається матриця параметрів ($\boldsymbol{X}_{RGB}$), що описують кадр (зображення), отриманий із відеопотоку камер відеоспостереження, а також кортеж допустимих значень параметрів ($\langle\Delta_Q\rangle$), що характеризують якість зображення. При цьому $\boldsymbol{X}_{RGB} = |x_{RGB}|_{A\times B}$ — матриця, що описує колір кожного із пікселів вхідного RGB-зображення розміром $A \times B$. Кожен елемент цієї матриці представляє собою вектор, що містить значення яскравості червоного (R), зеленого (G), синього (B). Елементами $\langle\Delta_Q\rangle$ є: Δ_W — допустима ширина діапазону яскравості; $Y_{avg,min}, Y_{avg,max}$ — мінімальне та максимальне значення середньої яскравості зображення (в першому наближенні 70 та 180); $\lambda_{M,min}$ — мінімальне значення контрасту Міхельсона; $\Delta_{\sigma_Y,min}$, $\Delta_{\sigma_Y,max}$ — мінімальне та максимальне значення стандартного відхилення яскравості; $\Delta_{R_{br}}, \Delta_{R_{dr}}$ — допустимі значення індексів засвітлення та затемнення (в першому наближенні 0,1 та 0,05); $\Delta_{\sigma_L^2}$ — поріг розмитості.

В першому наближенні $\Delta_W = 40$, $Y_{avg,min} = 70, Y_{avg,max} = 180$, $\lambda_{M,min} = 0{,}35$, $\Delta_{\sigma_Y,min} = 0{,}1$, $\Delta_{\sigma_Y,max} = 0{,}05$, $\Delta_{\sigma_L^2} = 100$.

Відповідно до [20] етап базується на підході до безеталонної оцінки якості зображення, а його виконання розділено на два кроки.

Крок 1.1. Розрахунок показників відображення. Розрахунок здійснюється на основі каналу яскравості (Y) в кольоровій моделі YCbCr. Конвертація RGB-зображення в YCbCr — зображення реалізується відповідно до стандарту ITU-R BT.601:

$$Y(n) = 0.299R(n) + 0.587G(n) + 0.114B(n), \quad (1)$$

$$C_b(n) = -0.168736R(n) - 0.331264G(n) + 0.5B(n) + 128, \quad (2)$$

$$C_r(n) = -0.5R(n) - 0.418688G(n) - 0.081312B(n) + 128, \quad (3)$$

де n — номер пікселя зображення; $Y \in [0{,}255]$ — компонента яскравості; $C_b \in [0{,}255]$, $C_r \in [0{,}255]$ — компоненти, що відповідають за синьо-жовтий та червоно-зелений відтінок відповідно.

Передбачено розрахунок середньої (Y_{avg}), максимальної (Y_{max}), мінімальної (Y_{min}) яскравості, значень елементів вектору ($\boldsymbol{I} = |i|_{256}$), що забезпечує побудову гістограми яскравості. Також відповідно до виразів (4, 14) проводиться розрахунок контрасту Міхельсона (λ_M), стандартного відхилення яскравості (σ_Y), індексу засвітлення (R_{br}), індексу затемнення (R_{dr}), Лапласіан зображення ($\boldsymbol{L}$), дисперсію Лапласіана (σ_L^2), середню яскравість по кожному із каналів RGB-зображення (μ_R, μ_G, μ_B), середню яскравість каналів RGB-зображення (μ_{avgRGB}), максимальне відхилення яскравості каналу RGB-зображення (Δ_{avgRGB}).

$$\lambda_M = \frac{Y_{max} - Y_{min}}{Y_{max} + Y_{min}}, \quad (4)$$

$$\sigma_Y = \sqrt{N^{-1}\sum_{n=1}^{N}\left(Y_n - Y_{avg}\right)^2}, \quad (5)$$

$$R_{br} = \frac{N_{Y>220}}{N}, \quad (6)$$

$$R_{dr} = \frac{N_{Y<30}}{N}, \quad (7)$$

$$L(i,j) = \sum_{k=-1}^{1}\sum_{l=-1}^{1}(K(k,l) \times Y(i+k, j+l)), \quad (8)$$

$$K = \begin{vmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{vmatrix}, \quad (9)$$

$$L_{avg} = N^{-1} \sum_{n=1}^{N} L_n, \quad (10)$$

$$\sigma_L^2 = N^{-1} \sum_{n=1}^{N} \left(L_n - L_{avg}\right)^2, \quad (11)$$

$$\mu_R = N^{-1} \sum_{n=1}^{N} R(n), \mu_G = N^{-1} \sum_{n=1}^{N} G(n), \mu_B = N^{-1} \sum_{n=1}^{N} B(n), \quad (12)$$

$$\mu_{avgRGB} = \frac{1}{3}(\mu_R + \mu_G + \mu_B), \quad (13)$$

$$\Delta_{avgRGB} = \max\left(\left|\mu_R - \mu_{avgRGB}\right|, \left|\mu_G - \mu_{avgRGB}\right|, \left|\mu_B - \mu_{avgRGB}\right|\right), \quad (14)$$

де Y_{max}, Y_{min}, — максимальне та мінімальне значення яскравості пікселів; N — кількість пікселів у зображенні; $N_{Y>220}$ — кількість пікселів у зображення з яскравістю більшою ніж 220; $N_{Y<30}$ — кількість пікселів у зображення з яскравістю меншою ніж 30, L_{avg} — середнє значення.

Крок 1.2. Перевірка придатності кадру. Зображення, що асоціюється з кадром відеопотоку вважається непридатним для подальшого аналізу якщо: більш ніж 50% пікселів мають яскравість нижчу за 50 або вищу ніж 200; $Y_{avg} \notin [Y_{avg,min}, Y_{avg,max}]$; $\lambda_M < \lambda_{M,min}$; $\sigma_Y \notin [\Delta_{\sigma Y,min}, \Delta_{\sigma Y,max}]$; $R_{br} < \Delta_{R_{br}}$; $R_{dr} < \Delta_{R_{dr}}$; $\sigma_L^2 < \Delta_{\sigma_L^2}$. Крім того кадр є непридатним, якщо ширина основного діапазону яскравості, є недостатньою. Тобто:

$$W_Y = P_{95} - P_5, \quad (15)$$

$$W_Y < \Delta_W, \quad (16)$$

де P_{95}, P_5 — відповідно 5-й та 95-й перцентилі розподілу яскравості.

Виходом кроку та етапу в цілому є сигнал про можливість подальшого розпізнавання (Y_{E1}) та у випадку можливості подальшого розпізнавання ($Y_{E1} = 1$) кортеж, що містить розраховані показники яскравості, різкості та контрастності ($\langle Q \rangle$).

Етап 2. **Попередня обробка параметрів відеопотоку**. На вхід етапу подається $\boldsymbol{X}_{RGB}$, $\langle Q \rangle$, а також розміри вхідних полів НММ ($\langle \boldsymbol{N}_{A \times B} \rangle$), що використовуються для подальшого аналізу зображень. Основним завданням виконання етапу являється нормалізація кольорових характеристик зображення, узгодження розмірів зображення з розмірами вхідних полів НММ, що використовуються в системі БА та фільтрацію шуму. Виконання етапу розділено на п’ять кроків.

Крок 2.1. Корекція кольорових характеристик.

– Корекція балансу білого кольору, що здійснюється відповідно до виразу (17), за правдивості умови (18)

$$R(i) = R(i)\frac{\mu_{avgRGB}}{\mu_R}, G(i) = G(i)\frac{\mu_{avgRGB}}{\mu_G}, B(i) = B(i)\frac{\mu_{avgRGB}}{\mu_B}, \quad (17)$$

$$\Delta_{avgRGB} > \Delta_{avgRGB}^{ent}, \quad (18)$$

де Δ_{avgRGB}^{ent} — допустима величина Δ_{avgRGB}, що відповідно до [20] дорівнює 15.

– Конвертація RGB-зображення в YCbCr-зображення, що здійснюється за допомогою виразів (1–3).

– Якщо в конвертованому YCbCr-зображенні $Y_{avg} < 70$ або $Y_{avg} > 180$, то застосовується гамма-корекція:

ISSN 2663 - 4023

$$Y(n) = 255 \times \left(\frac{Y(n)}{255}\right)^{\gamma} \quad \gamma = \begin{cases} 1.2, Y_{avg} < 70 \\ 0.8, Y_{avg} > 180 \end{cases} \tag{19}$$

– Якщо після гама корекції $\sigma_Y < 20$ або $\lambda_M < 0.35$, то здійснюється наведена в [20] процедура адаптивного вирівнювання гістограми яскравості (Contrast Limited Adaptive Histogram Equalization, CLAHE) з параметром обмеження контрасту (clip limit) рівним 2.

Крок 2.2. Фільтрація шуму. Виконання кроку полягає у почерговому застосуванні медіанного, білатерального фільтрів та фільтру підвищення чіткості.

– Медіанна фільтрація застосовується у випадку виявлення ознак імпульсного шуму типу «сіль-перець», що характеризуються надмірною часткою пікселів з екстремальною яскравістю зображенні з низькою контрастністю та недостатньою варіативністю компонент яскравості. Тобто медіанна фільтрація застосовується за виконання умови (20) та реалізується відповідно до виразу (21).

$$\frac{N_{Y>240} + N_{Y<15}}{N} > 0.03 \wedge \lambda_M < 0.5 \wedge \sigma_Y < 50, \tag{20}$$

$$Y(i,j) = median\{Y(i+k, j+l)\}\, k, l \in [-r; r], \tag{21}$$

де $median$ — оператор вибору медіани (центрального значення впорядкованого списку); r — радіус фільтра (для ядра 3×3 $r = 1$).

– Білатеральна фільтрація застосовується для зменшення локального шуму в каналі яскравості із збереженням контурів при виявленні гаусівського шуму у разі виконання умов (22) та реалізується відповідно до виразів (23–27).

$$\sigma_Y \in [25{,}50] \wedge \sigma_L^2 \in [500, 1500] \wedge \lambda_M < 0.6, \tag{22}$$

$$Y(i,j) = \frac{1}{W(i,j)} \sum_{k=-r}^{r} \sum_{l=-r}^{r} Y(i+k, j+l) \times G_s(k,l) \times G_r\big(Y(i,j) - Y(i+k, j+l)\big), \tag{23}$$

$$W(i,j) = \sum_{k=-r}^{r} \sum_{l=-r}^{r} G_s(k,l) \times G_r\big(Y(i,j) - Y(i+k, j+l)\big), \tag{24}$$

$$G_s(k,l) = exp\left(-\frac{k^2 + l^2}{2\sigma_s^2}\right), \tag{25}$$

$$G_r(\delta) = exp\left(-\frac{\delta^2}{2\sigma_r^2}\right), \tag{26}$$

$$\delta = |Y(i,j) - Y(i+k, j+l),| \tag{27}$$

де G_s — просторове ядро Гауса; G_r — радіальне (яскравісне) ядро Гауса; $W(i,j)$ — нормалізуючий коефіцієнт; $r = 2$ — радіус вікна фільтрації (вікно 5x5); $\sigma_s = 5$ — параметр просторового розмазування; $\sigma_r = 10$ — параметр інтенсивністного розмазування.

Зазначимо, що σ_Y відображає загальну варіативність яскравості у зображенні. При $\sigma_Y > 50$ можливо присутній текстурний шум, але не гаусівський; білатеральна фільтрація може бути неефективною або навіть шкідливою. При $\sigma_Y < 25$ фільтрація не має сенсу, адже варіативність дуже слабка. Умова $\sigma_L^2 \in [500, 1500]$ вказує на те, що фільтр буде застосовано до не надто розмитих та чітких зображень. В протилежному випадку білатеральна фільтрація або не дасть результату, або загладить важливі дрібні деталі. Умова $\lambda_M < 0.6$ свідчить про те, що фільтр буде застосовано до висококонтрастних зображень. В протилежному разі застосування фільтра може до втрати деталізації.

– Якщо після застосування медіанного та білатерального фільтрів чіткість зображення є помірною ($\sigma_L^2 \in [100, 200]$), то застосовується фільтр підвищення чіткості (unsharp masking):

$$G(x,y) = \sum_{i=-k}^{k} \sum_{j=-k}^{k} Y(x+i, y+j) \times w(i,j), \quad (28)$$

$$w(i,j) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{i^2+j^2}{2\sigma^2}\right), \quad (29)$$

$$Y(x,y) = Y(x,y) + \alpha\big(Y(x,y) - G(x,y)\big), \quad (30)$$

де $G(x,y)$ — зображення розмите за допомогою фільтра Гауса; w — ядро фільтра Гауса; α — коефіцієнт підсилення чіткості (в базовому випадку 0.5); k — радіус фільтра (в базовому випадку 2, що відповідає ядру 5×5); σ — стандартне відхилення розподілу (в базовому випадку 1).

Крок 2.3. Конвертація зображення. Виконується відповідно до виразів (31–33) та полягає у конвертації YCbCr — зображення в формат RGB.

$$R(n) = Y(n) + 1.402 \cdot (C_r(n) - 128) \quad (31)$$

$$G(n) = Y(n) - 0.344136 \cdot (C_b(n) - 128) - 0.714136 \cdot (C_r(n) - 128) \quad (32)$$

$$B(n) = Y(n) + 1.772 \cdot (C_b(n) - 128) \quad (33)$$

Крок 2.4. Узгодження розмірів. Виконується за умов можливості ефективного масштабування, наведених [16], [20]. Реалізується методом бікубічної інтерполяції з урахуванням масштабного коефіцієнту між розміром вхідного зображення та розміром вхідного поля кожної із НММ.

Крок 2.5. Нормалізація кольору. Виконується відповідно до загальноприйнятих підходів [14], [18] та полягає у приведенні значень відображення кольору кожного пікселя в заданий діапазон.

Виходом кроку 2.5 та етапу 2 в цілому є $\boldsymbol{X}_{NN}$ — матриця, що описує колір кожного із пікселів вхідного RGB-зображення розміром $H_{NN} \times W_{NN}$, який відповідає вхідному полю НММ. Зазначимо, що порогові значення параметрів, що використовуються в умовах визначення доцільності застосування процедур обробки зображення можуть бути в подальшому модифіковані з урахуванням практичного досвіду та результатів теоретичних досліджень. Крім того, в подальшу перспективним є впровадження додаткових механізмів обробки на основі вейвлет-перетворень.

Етап 3. Виділення об'єктів на зображенні. Реалізація етапу базується на авторських рішеннях щодо семантичної сегментації растрових зображень [10], [22], адаптованих до застосування в системах БА та відповідно до асоційованих з ними процедур розділена на три кроки:

Крок 3.1. Виділення ЗО. Виконується для виділення кордонів ЗО у піддослідному кадрі вхідного відеопотоку.

Крок 3.2. Виділення завад. Передбачає виділення на ЗО кордонів областей завад, характерних для очікуваних умов відеореєстрації.

Крок 3.3. Виділення РОО. Здійснюється виділення кордонів РОО на ЗО.

Загалом на вхід етапу 3 подається кортеж $\langle Lt \rangle$, що містить елементи, які описують умови задач виділення кордонів об'єктів (ЗО, областей завад, РОО) на піддослідному зображенні. Крім того, на вхід кроку 3.1 подається матриця $\boldsymbol{X}_{NN}$, отримана після попередньої обробки параметрів відеопотоку. На вхід кроку 3.2, крім $\boldsymbol{X}_{NN}$ подається отриманий в результаті виконання кроку 3.1, $\boldsymbol{P}_{FC}$ — масив, що містить значення яскравості пікселів по кожному з трьох каналів кольору (R, G, B) для області ЗО. Виходом кроку 3.2 є $\boldsymbol{P}_{OB}$ — масив, що містить значення яскравості пікселів для областей завад та бінарна маска завад $\boldsymbol{M}_{OB}$, що розраховується за допомогою виразу:

$$\boldsymbol{M}_{OB}(x,y) = \mathbb{I}(\boldsymbol{P}_{OB}(x,y) < \theta_{OB}) \quad (34)$$

де $\mathbb{I}$ — індикаторна функція; θ_{OB} — порогове значення ($\theta_{OB} = 0.85$).

На вхід кроку 3.3 подаються $\boldsymbol{P}_{FC}$ та $\boldsymbol{M}_{OB}$, а виходом кроку є $\boldsymbol{P}_{IR}$ масив, що містить значення яскравості пікселів для областей РОО.

Відповідно до [3, 5, 6] виконання кожного кроку розділено на три операції:

1 — визначення параметрів НММ з енкодер-декодерною архітектурою;

2 — навчання НММ;

3 — застосування навченої НММ для здійснення семантичної сегментації.

При цьому реалізація кожної операції на конкретному кроці враховує специфіку відповідного завдання: тип об'єкта сегментації, а також особливості просторових ознак, притаманних цільовим областям (ЗО, завадам або РОО). Зазначимо, що при виконанні кроку 3.1. виходом етапу 3 являється $\boldsymbol{P}_{FC}$, при виконанні кроку 3.2 — $\boldsymbol{P}_{OB}$, $\boldsymbol{M}_{OB}$, а при виконанні кроку 3.3 — $\boldsymbol{P}_{IR}$.

Етап 4. Детектування спуфінг-атак. Реалізація етапу базується на авторських рішеннях щодо розробки НМЗ детектування спуфінг-атак [11]. Відповідно до результатів [10], [12], [21] виконання етапу розділено на чотири кроки:

Крок 4.1. Детектування спуфінг-атак на основі візуальних артефактів. Виконання кроку полягає у застосуванні НММ DeepPixBiS на вхід якої подається масив $\boldsymbol{P}_{FC}$, отриманий в результаті виконання кроку 3.1, а також заздалегідь визначене порогове значення класифікації γ_v. Виходом кроку 4.1 є вихідне значення DeepPixBiS (Y_v) та бінарний сигнал (Sp_v) щодо наявності спуфінг-атаки, сформований на основі порівняння Y_v з порогом γ_v.

Крок 4.2. Детектування спуфінг-атак на основі артефактів зовнішнього оточення. Відповідно до [9], [11] детектування здійснюється за рахунок нейромережевого аналізу $\boldsymbol{X}_{NN}$, що разом з пороговим значенням класифікації γ_o подається на вхід даного кроку. В якості нейромережевого класифікатора використовується НММ з енкодер-декодерною архітектурою, побудова якої виконується за допомогою наведеного в [10] методу. Виходом кроку 4.2 є значення вихідного сигналу НММ (Y_o) та бінарний сигнал (Sp_o) щодо наявності спуфінг-атаки, сформований на основі порівняння Y_o з порогом γ_o.

Крок 4.3. Детектування спуфінг-атак за динамікою параметрів живучості. Виконання кроку полягає у нейромережевому аналізі 10 кадрів, що містять відфільтроване ЗО (включно з РОО). В базовому випадку для аналізу прийнято застосувати описану в [6], [7] НММ типу ViT (Visual Transformer), яка пройшла донавчання на наборі даних CelebA-Spoof, доступному за посиланням https://www.kaggle.com/datasets/attentionlayer241/celeba-spoof-for-face-antispoofing. На вхід кроку подається порогове значення γ_l та матриці $\boldsymbol{P}_{FC}$, $\boldsymbol{M}_{OB}$, $\boldsymbol{P}_{IR}$, отримані в результаті виконання етапу 3 при обробці 10 кадрів відеопотоку. Виходом кроку 4.3 є усереднене вихідне значення НММ (Y_l) та бінарний сигнал (Sp_l) про наявність спуфінг-атаки, сформований на основі порівняння з порогом γ_o.

Крок 4.4. Детектування спуфінг-атак на основі розпізнаних емоцій. Виконання кроку полягає у нейромережевому аналізі динаміки емоцій на предмет їх природності. На вхід кроку подається множина $\boldsymbol{E}$, що містить числові значення інтенсивностей 7 базових емоцій розпізнаних на протязі 1,2–2 с та наперед задане порогове значення γ_e. Для аналізу в залежності від обсягу доступних навчальних датасетів використовується або мережа PNN (менше 1000 навчальних прикладів) або багатошаровий персептрон, на вхід якого подаються числові значення інтенсивності 7 базових емоцій, а виходом являється ступінь впевненості в реалізації спуфінг-атаки. Виходом кроку 4.4 є вихідне значення НММ (Y_e) та бінарний сигнал (Sp_e) про наявність спуфінг-атаки, сформований на основі порівняння Y_e з порогом γ_e.

Виходом етапу 4 при виконанні кроку 4.1 є Y_v, Sp_v, при виконанні кроку 4.2 — Y_o, Sp_o, при виконанні кроку 4.3 — Y_l, Sp_l, а при виконанні кроку 4.4 — Y_e, Sp_e.

Етап 5. Визначення контрольних точок. Виконання етапу передбачає визначення множини контрольних точок обличчя, очищеної від елементів, що потрапили в зони завад. На вхід етапу подається $\boldsymbol{P}_{FC}$, $\boldsymbol{M}_{OB}$. Реалізація етапу розділена на два кроки.

Крок 5.1. Первинна локалізація та визначення Blendshape Scores. Виконання кроку передбачає застосування HMM FaceMeshV2, яка навіть при розгортанні на малопотужних мобільних пристроях забезпечує обробку із затримкою 20–100 мс, що дозволяє в реальному часі на основі $\boldsymbol{P}_{FC}$, сформувати масив $\boldsymbol{Kp}$, елементи якого співвідносяться з тривимірними координатами 478 контрольних точок обличчя (468 точок відповідають власне ЗО, а 10 точок відповідають зіницям очей). Зазначимо, що використання FaceMeshV2 дозволяє визначити масив $\boldsymbol{Bs}$, елементи якого співвідносяться з 52 Blendshape Scores, які є числовим представленням інтенсивності різних мімічних виразів. Відповідно до [12], [17], [19] такі показники забезпечують достатньо оперативне та топологічно точне представлення ЗО для подальшого нейромережевого розпізнавання емоцій та особи представника персоналу ОКІ.

Крок 5.2. Фільтрація координат у зоні завад. На даному кроці обнуляються елементи масиву $\boldsymbol{Kp}$, що відповідають контрольним точкам, які знаходяться в зоні завад. Виходом кроку та етапу в цілому є масив $\boldsymbol{Kp}$, модифікований відповідним чином.

Етап 6. Розпізнавання емоцій. Виконання етапу полягає у визначенні множини $\boldsymbol{Em}$ якої відповідають інтенсивності відображенні на ЗО семи базових емоцій. Таким чином виходом етапу 6 є множина $\boldsymbol{Em}$**.** Враховуючи особливості задачі та рекомендації [12] в базовому варіанті передбачено використання багатошарового персептрону зі структурою 52 (вхідний шар) — 128 (перший схований шар) — 64 (другий схований шар) — 7 (вихідний шар) для навчання якого в дослідницьких цілях можливо використати попередньо оброблений за допомогою FaceMeshV2 набір даних CK+ (Extended Cohn-Kanade Dataset), з розрахованими значеннями Blendshape Scores..

Етап 7. Розпізнавання особи. На вхід етапу подаються $\boldsymbol{Kp}$, $\boldsymbol{P}_{IR}$, $\boldsymbol{M}_{OB}$, параметр tp_r, значення якого вказує на тип розпізнавання особи та порогове значення γ_{rr} з яким порівнюється інтегрована оцінка схожості, отримана за рахунок об'єднання результатів аналізу ЗО і РОО. У випадку $tp_r = 0$ розпізнавання здійснюється за допомогою нейромережевого порівняння ознак ЗО та РОО особи, що проходить перевірку, з відповідними ознаками легітимних представників персоналу ОКІ. У випадку $tp_r = 1$ розпізнавання асоціюється з класифікацією особи за допомогою HMM, попередньо навченої на ЗО та РОО легітимних представників персоналу. Виконання етапу розділено на три кроки.

Крок 7.1. Розпізнавання особи за ЗО. Виконується нейромережевий аналіз $\boldsymbol{Kp}$ обличчя з метою формування оцінки подібності r_{FC} між ЗО особи, яка підлягає розпізнаванню та ЗО легітимних представників.

Крок 7.2. Розпізнавання особи за РОО. Полягає у нейромережевому аналізі відфільтрованої від завад області РОО з метою формування оцінки подібності r_{IR} між РОО особи, яка підлягає розпізнаванню та РОО легітимних представників. Фільтрація реалізується через поелементне співставлення значень масиву $\boldsymbol{P}_{IR}$ з відповідними значеннями маски $\boldsymbol{M}_{OB}$.

Крок 7.3. Інтеграція результатів. На цьому кроці обидві оцінки r_{FC} і r_{IR} за допомогою виразу (35) об'єднуються в інтегровану метрику r_{rr} та приймається остаточне рішення на основі порівняння r_{rr} з пороговим значенням γ_{RR}, що реалізується за допомогою виразу (36)

$$r_{RR} = \alpha \times r_{FC} + (1 - \alpha) \times r_{IR} \quad (35)$$

$$if\ r_{RR} > \gamma_{RR} \Longrightarrow RR = true\ else\ RR = false \quad (36)$$

Якщо $RR = true$ вважається, що особа розпізнана як легітимний представник персоналу ОКІ після чого визначається відповідний ідентифікатор (ID). У базовому випадку $\alpha = 0.7$, а $\gamma_{rr} = 0.82$, що зважаючи на результати [21], [22] відповідає співвідношенню True Acceptance Rate (TAR) ≈ 97–98 % при False Acceptance Rate (FAR) ≤ 1 %, і є прийнятним у системах доступу до об'єктів критичної інфраструктури.

Зазначимо, що у випадку $tp_r = 0$ при реалізації кроків 7.1 та 7.2 відповідно до [11] пропонується використання НММ на основі Siamese Network або Two_channel Networks, а при $tp_r = 1$ — НММ типу MobileNet. Виходом етапу 7 являється $\langle Y_{RR} \rangle = \langle r_{rr}, r_{FC}, r_{IR}, RR \rangle$.

Етап 8. Агрегація результатів розпізнавання. Етап призначено для формування вихідного сигналу $\langle \mathcal{S}_{out} \rangle$ даного методу відповідно до специфікації формату (Ω), що подається на вхід етапу. Ω — визначає структуру вихідного сигналу, включаючи формат представлення даних (наприклад, JSON), перелік необхідних полів, їх порядок, типи даних, а також правила ідентифікації кожного поля.

Специфікація подається у вигляді шаблону, який забезпечує уніфікацію вихідної інформації для подальшої обробки або передачі до зовнішніх систем. В базовому випадку $\langle \mathcal{S}_{out} \rangle = \langle Y_{E1}, Y_v, Sp_v, Y_o, Sp_o, Y_l, Sp_l, Y_e, Sp_e, \boldsymbol{Em}, r_{FC}, r_{IR}, r_{RR}, RR, ID \rangle$. При достроковому завершенні виконання методу (наприклад, через виявлення спуфінг-атаки), що призводить до неможливості отримання значень всіх полів вихідного сигналу, $\langle \mathcal{S}_{out} \rangle$ формується неповністю. Поля, що не можуть бути визначені, залишаються порожніми (null або «-» згідно зі специфікацією формату). Зазначимо, що відповідно до опису наведеної в [12] моделі процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ із застосуванням НМЗ та наведеної в [11] модульної НММ БА персоналу ОКІ за ЗО та РОО послідовність виконання запропонованого методу полягає у валідації кадрів відеопотоку (етап 1), попередній обробці кадрів відеопотоку (етап 2), виділенні ЗО (етап 3, крок 3.1), детектування спуфінг-атак на основі на основі візуальних артефактів та на основі артефактів зовнішнього оточення (етап 4, кроки 4.1 та 4.2), виділення завад та РОО (етап 3, кроки 3.2 та 3.3), визначенні контрольних точок (етап 5), розпізнавання емоцій (етап 6), детектування спуфінг-атак на основі на основі розпізнаних емоцій (етап 4, крок 4.3), розпізнавання особи (етап 7), агрегацію результатів розпізнавання (етап 8). У випадку недопустимих параметрів кадру або виявлення ознак спуфінг-атак логіка виконання методу передбачає негайний перехід до етапу 8, на якому здійснюється формування вихідного сигналу з урахуванням наявних результатів.

ВИСНОВКИ

В результаті проведених досліджень розроблено метод біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережевих засобів, що реалізує багатокрокову адаптивну обробку відеопотоку та забезпечує комплексне виконання ключових процедур, необхідних для забезпечення ефективної автентифікації в варіативних умовах застосування. Етапи методу із застосуванням нейромережевих рішень структуровано як послідовність процедур, що відповідають типовим завданням біометричної автентифікації, які зазвичай реалізуються окремими нейромережевими моделями. Вперше в межах єдиної архітектури реалізовано багаторівневий аналіз ознак спуфінг-атак з урахуванням візуальних артефактів

зображення обличчя, артефактів зовнішнього оточення, динаміки параметрів живучості та динаміки емоційного стану. При цьому реалізовано механізм адаптивної обробки відеопотоку, який передбачає автоматичне оцінювання показників відображення, динамічне формування множини зображень, придатних для подальшої обробки, а також попередню обробку зображень з метою підвищення якості їх відображення. Фільтрацію зображення обличчя та райдужної оболонки від типових завад забезпечено за рахунок застосування процедури семантичної сегментації з наступним поелементним маскуванням піксельних значень, що дозволяє виключити з обробки ділянки зображення, які містять завади, та уникнути врахування хибно визначених контрольних точок у зонах перекриття, тіней або сторонніх об'єктів. Однією з ключових особливостей методу є цілеспрямоване використання доступних, апробованих наперед навчених нейромережевих моделей з відкритим кодом (FaceMeshV2, Visual Transformer, DeepPixBiS, Siamese Network, Two_channel Networks, MobileNet), інструментальне забезпечення яких адаптовано до умов відеореєстрації на об'єктах критичної інфраструктури. За попередніми оцінками адаптивна обробка відеопотоку, багаторівневий аналіз ознак спуфінг-атак, а також використання доступних і апробованих нейромережевих моделей забезпечують пристосованість до варіативних умов відеореєстрації та дозволяють у середньому на 25–35 % підвищити точність виявлення спуфінг-атак, а також щонайменше в 1,5 рази скоротити час на розробку системи на основі відкритих моделей щонайменше в 1,5 раза.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Abraham J., Paul V. "An imperceptible spatial domain color image watermarking scheme". Journal of King Saud University – Computer and Information Sciences. 2019. Vol. 31 (1), pp. 125-133.
2. Adithya U., Nagaraju C. "Object Motion Direction Detection and Tracking for Automatic Video Surveillance", International Journal of Education and Management Engineering (IJEME), Vol.11, No.2, pp. 32-39, 2021. DOI: 10.5815/ijeme.2021.02.04.
3. Badrinarayanan V., Kendall A., Cipolla R. "SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation". URL: http://arxiv.org/abs/1511.0051 (accessed October 12, 2022).
4. Cherrat, Rachid Alaoui, Hassane Bouzahir. "Score Fusion of Finger Vein and Face for Human Recognition Based on Convolutional Neural Network Model". International Journal of Computing, 2020. 19, pp. 11-19.
5. Dai, J., He, K., & Sun, J. (2016). Instance-aware semantic segmentation via multi-task network cascades. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 3150-3158). https://doi.org/10.48550/arXiv.1512.04412.
6. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., ... & Houlsby, N. An image is worth 16x16 words: Transformers for image recognition at scale. 2020. arXiv preprint arXiv:2010.11929. https://doi.org/10.48550/arXiv.2010.11929
7. Jun Shen. "Motion detection in color image sequence and shadow elimination". Visual Communications and Image Processing. 2014. Vol. 5308, pp. 731-740.
8. Keresh, A., & Shamoi, P. Liveness detection in computer vision: Transformer-based self-supervised learning for face anti-spoofing. 2024. IEEE Access. https://doi.org/10.48550/arXiv.2406.13860
9. Kong T., et al. "FoveaBox: Beyound Anchor-Based Object Detection", IEEE Trans. Image Process. 29 (2020), pp. 7389–7398.
10. Korchenko O., & Tereikovskyi O. Semantic segmentation of facial images in biometric authentication systems of personnel of critical infrastructure facilities . Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique». 2025. 4(28), 385–399. https://doi.org/10.28925/2663-4023.2025.28.816
11. Korchenko O., Tereikovskyi I., Ziubina R., Tereikovska L., Korystin O., Tereikovskyi O., Karpinskyi V. Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images. Applied Sciences. 2025, 15, 2553. https://doi.org/10.3390/app15052553.

12. 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. Information security. 2024. V. 26, № 1, pp. 157-170. DOI: https://doi.org/10.18372/2410-7840.26.18839
13. Liu, X.-P., Li, G., Liu, L., Wang, Z. “Improved YOLOV3 target recognition algorithm based on adaptive eged optimization”. Microelectron. Comput. 2019. Vol. 36, pp. 59–64.
14. Prilianti, K. R et al. “Non-destructive Photosynthetic Pigments Prediction using Multispectral Imagery and 2D-3HM”. International Journal of Computing. 2021. 20(3), pp. 391-399.
15. Reja, S. A., Rahman, M. M. “Sports Recognition using Convolutional Neural Network with Optimization Techniques from Images and Live Streams”. International Journal of Computing, 2021. 20(2), pp. 276-285.
16. Ronneberger O., Fischer P., Brox T. “U-Net: Convolutional Networks for Biomedical Image Segmentation”. Medical Image Computing and Computer-Assisted Intervention (MICCAI), 2015. Vol.9351, pp. 234-241.
17. Senocak A. et al. “Part-based player identification using deep convolutional representation and multi-scale pooling”. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018, pp. 1732-1739.
18. Shkurat O. et al. “Image Segmentation Method Based on Statistical Parameters of Homogeneous Data Set”. Advances in Intelligent Systems and Computing. 2020. Vol. 902, pp. 271–281.
19. Simonyan K., Zisserman A. “Very deep convolutional networks for large-scale image recognition”. ArXiv1409.1556 Cs. (2019). http://arxiv.org/abs/1409.1556 (accessed October 11, 2022).
20. Tereikovska L., Tereikovskyi I. Evaluation and correction of visual characteristics of images. Science, technology and innovation in the context of global transformation : Scientific monograph. Riga, Latvia : Baltija Publishing, 2024. P. 205-225. ISBN 978-9934-26-499-3 DOI: https://doi.org/10.30525/978-9934-26-499-3-11
21. Tereikovskyi I., Korchenko O., Bushuyev S., Tereikovskyi O., Ziubina R. & Veselska O. A Neural Network Model for Object Mask Detection in Medical Images. International Journal of Electronics and Telecommunication. 2023. Vol. 69(1), pp. 41–46. https://doi.org/10.24425/ijet.2023.144329
22. Tereikovskyi I., Hu Z., Chernyshev D., Tereikovska L., Korystin O., & Tereikovskyi O.. The method of semantic image segmentation using neural networks. International Journal of Image, Graphics and Signal Processing. 2022. Vol. 10(6), 1,14(6), pp. 1–14. https://doi.org/10.5815/ijigsp.2022.06.0110.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Oleksandr Korchenko
Corresponding Member of the National Academy of Sciences of Ukraine,
Doctor of Technical Sciences, Professor, First vice-rector
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-3376-0631
agkorchenko@gmail.com

Oleh Tereikovskyi
Postgraduate student of the Department of Cybersecutiry,
The National University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0001-5045-0163
tereikovskyio@gmail.com

METHOD OF BIOMETRIC AUTHENTICATION OF PERSONNEL OF CRITICAL INFRASTRUCTURE FACILITIES BY FACIAL IMAGE AND IRIS OF THE EYE USING NEURAL NETWORK TOOLS

Abstract. The widespread implementation of neural network biometric authentication tools based on facial and iris images at critical infrastructure facilities has made it possible to increase the level of security and efficiency of personnel identification. At the same time, modern requirements dictate the need to increase resistance to spoofing attacks, adaptability to interference from the real environment, as well as expand functionality to take into account the psycho-emotional state of personnel at the time of authentication. Traditional neural network methods based on neural networks with monolithic architecture are limited in implementing these requirements due to insufficient flexibility and difficulty in adapting to variable video recording conditions. Therefore, this article proposes a method for biometric authentication of personnel at critical infrastructure facilities based on facial and iris images using neural network tools. The method implements multi-step adaptive processing of the video stream and comprehensive execution of procedures necessary for effective authentication in conditions of variability of image parameters. The stages of the method are structured as a sequence of procedures that correspond to typical biometric authentication tasks, each of which is implemented by a separate neural network. For the first time, a multi-level analysis of signs of spoofing attacks is provided within a single architecture, taking into account visual facial artifacts, artifacts of the external environment, the dynamics of survivability parameters and emotional state. A mechanism for automatic evaluation of display indicators, dynamic formation of a set of images suitable for processing and their pre-processing to improve quality is proposed. Interference filtering is carried out by semantic segmentation and element-wise masking of pixel areas, which allows excluding areas with shadows, overlaps or extraneous objects from processing. A key feature is the targeted use of available and tested pre-trained neural network models with open source (FaceMeshV2, Visual Transformer, DeepPixBiS, Siamese Network, Two_channel Networks, MobileNet), adapted to the conditions of video recording at critical infrastructure facilities. According to preliminary estimates, the use of adaptive video stream processing and multi-level analysis of spoofing attacks allows to increase the accuracy of spoofing detection by 25–35% and reduce the development time of the system based on open models by at least 1.5 times.

Keywords: biometric authentication; biometric authentication method; facial recognition; facial image; iris; neural network; critical infrastructure facility.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Abraham J., Paul V. "An imperceptible spatial domain color image watermarking scheme". Journal of King Saud University – Computer and Information Sciences. 2019. Vol. 31 (1), pp. 125-133.
2. Adithya U., Nagaraju C. "Object Motion Direction Detection and Tracking for Automatic Video Surveillance", International Journal of Education and Management Engineering (IJEME), Vol.11, No.2, pp. 32-39, 2021. DOI: 10.5815/ijeme.2021.02.04.

3. Badrinarayanan V., Kendall A., Cipolla R. “SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation”. URL: http://arxiv.org/abs/1511.0051 (accessed October 12, 2022).
4. Cherrat, Rachid Alaoui, Hassane Bouzahir. “Score Fusion of Finger Vein and Face for Human Recognition Based on Convolutional Neural Network Model”. International Journal of Computing, 2020. 19, 11-19.
5. Dai, J., He, K., & Sun, J. (2016). Instance-aware semantic segmentation via multi-task network cascades. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 3150-3158). https://doi.org/10.48550/arXiv.1512.04412.
6. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., ... & Houlsby, N. An image is worth 16x16 words: Transformers for image recognition at scale. 2020. arXiv preprint arXiv:2010.11929. https://doi.org/10.48550/arXiv.2010.11929
7. Jun Shen. “Motion detection in color image sequence and shadow elimination”. Visual Communications and Image Processing. 2014. Vol. 5308, pp. 731-740.
8. Keresh, A., & Shamoi, P. Liveness detection in computer vision: Transformer-based self-supervised learning for face anti-spoofing. 2024. IEEE Access. https://doi.org/10.48550/arXiv.2406.13860
9. Kong T., et al. “FoveaBox: Beyound Anchor-Based Object Detection”, IEEE Trans. Image Process. 29 (2020), pp. 7389–7398.
10. Korchenko O., & Tereikovskyi O. Semantic segmentation of facial images in biometric authentication systems of personnel of critical infrastructure facilities . Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique». 2025. 4(28), 385–399. https://doi.org/10.28925/2663-4023.2025.28.816
11. Korchenko O., Tereikovskyi I., Ziubina R., Tereikovska L., Korystin O., Tereikovskyi O., Karpinskyi V. Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images. Applied Sciences. 2025, 15, 2553. https://doi.org/10.3390/app15052553.
12. 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. Information security. 2024. V. 26, № 1, pp. 157-170. DOI: https://doi.org/10.18372/2410-7840.26.18839
13. Liu, X.-P., Li, G., Liu, L., Wang, Z. “Improved YOLOV3 target recognition algorithm based on adaptive eged optimization”. Microelectron. Comput. 2019. Vol. 36, pp. 59–64.
14. Prilianti, K. R et al. “Non-destructive Photosynthetic Pigments Prediction using Multispectral Imagery and 2D-3HM”. International Journal of Computing. 2021. 20(3), pp. 391-399.
15. Reja, S. A., Rahman, M. M. “Sports Recognition using Convolutional Neural Network with Optimization Techniques from Images and Live Streams”. International Journal of Computing, 2021. 20(2), pp. 276-285.
16. Ronneberger O., Fischer P., Brox T. “U-Net: Convolutional Networks for Biomedical Image Segmentation”. Medical Image Computing and Computer-Assisted Intervention (MICCAI), 2015. Vol.9351, pp. 234-241.
17. Senocak A. et al. “Part-based player identification using deep convolutional representation and multi-scale pooling”. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018, pp. 1732-1739.
18. Shkurat O. et al. “Image Segmentation Method Based on Statistical Parameters of Homogeneous Data Set”. Advances in Intelligent Systems and Computing. 2020. Vol. 902, pp. 271–281.
19. Simonyan K., Zisserman A. “Very deep convolutional networks for large-scale image recognition”. ArXiv1409.1556 Cs. (2019). http://arxiv.org/abs/1409.1556 (accessed October 11, 2022).
20. Tereikovska L., Tereikovskyi I. Evaluation and correction of visual characteristics of images. Science, technology and innovation in the context of global transformation : Scientific monograph. Riga, Latvia : Baltija Publishing, 2024. P. 205-225. ISBN 978-9934-26-499-3 DOI: https://doi.org/10.30525/978-9934-26-499-3-11
21. Tereikovskyi I., Korchenko O., Bushuyev S., Tereikovskyi O., Ziubina R. & Veselska O. A Neural Network Model for Object Mask Detection in Medical Images. International Journal of Electronics and Telecommunication. 2023. Vol. 69(1), pp. 41–46. https://doi.org/10.24425/ijet.2023.144329
22. Tereikovskyi I., Hu Z., Chernyshev D., Tereikovska L., Korystin O., & Tereikovskyi O.. The method of semantic image segmentation using neural networks. International Journal of Image, Graphics and Signal Processing. 2022. Vol. 10(6), 1,14(6), pp. 1–14. https://doi.org/10.5815/ijigsp.2022.06.0110.

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.