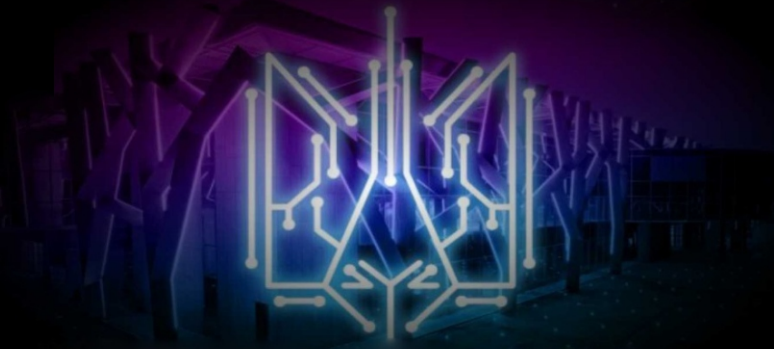

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

ББК 32.81+78.362

Інформаційна безпека та інформаційні технології: збірник тез доповідей VII Всеукраїнської науково-практичної конференції, м. Львів, 27 листопада 2025 року. Львів, ЛДУ БЖД, 2025, 493 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

УДК 004.934:004.056.5

МОНОКУЛЯРНА ОЦІНКА ГЛИБИНИ ЯК ЗАСІБ ПІДВИЩЕННЯ НАДІЙНОСТІ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Ростислав РОПНІЦКИЙ[1], Ростислав ТКАЧУК[1,2], Андрій ІВАНУСА[2]
[1]Національний університет «Львівська політехніка
[2]Львівський державний університет безпеки життєдіяльності

Анотація. *Біометрична автентифікація за зображенням обличчя широко використовується у цифрових сервісах, однак залишається вразливою до презентаційних атак через друковані фото, відеоповтори з екрана або прості маски. Наявність глибинних ознак суттєво підсилює перевірку живості, але у реальних системах спеціалізовані RGB-D або ІЧ сенсори доступні не завжди. Робота пропонує застосування монокулярної оцінки глибини з однієї RGB камери для формування додаткової 3D ознаки у каналі автентифікації. Ключова ідея полягає у прогнозуванні відносної карти глибини обличчя та інтеграції її у модуль прийняття рішення як просторового критерію живості і відповідності шаблону. Очікуваний ефект полягає у підвищенні стійкості до 2D атак без зміни апаратної платформи, зберігаючи вимоги реального часу і сумісність з наявними моделями розпізнавання.*

Ключові слова *біометрична автентифікація, перевірка живості, монокулярна глибина, карти глибини обличчя, презентаційні атаки, комп'ютерний зір*.

Abstract. *Face based biometric authentication is widely adopted in digital services, yet it remains vulnerable to presentation attacks such as printed photos, screen replays, or simple masks. Depth cues significantly strengthen liveness detection, but dedicated RGB-D or infrared sensors are not always available in practical deployments. This paper considers the use of monocular depth estimation from a single RGB camera to obtain an additional 3D cue within the authentication pipeline. The core idea is to predict a relative facial depth map and fuse it with the decision module as a spatial liveness and template consistency criterion. The anticipated outcome is improved resistance to 2D spoofing without changing the hardware platform, while preserving real time constraints and compatibility with existing face recognition models..*

Key words*: biometric authentication, liveness detection, monocular depth estimation, facial depth maps, presentation attacks, computer vision*.

Основний канал ризику у біометричній автентифікації за обличчям пов'язаний із тим, що класичні RGB-ознаки відображають переважно текстурні та фотометричні характеристики, які можуть відтворюватися на двовимірних носіях із високою точністю. Біометрична автентифікація в цілому базується на стабільних фізіологічних або поведінкових характеристиках людини, тоді як розпізнавання обличчя стало найбільш поширеним методом завдяки безконтактності та доступності стандартних камер як сенсорів. У типовому конвеєрі роботи таких систем виконуються етапи детекції та вирівнювання обличчя, формування ембеддингу та його порівняння з еталонними представленнями за метричними критеріями. Ця процедура забезпечує високу точність на контрольованих наборах даних, проте одночасно підвищує чутливість системи до реальних спотворень і атак на біометричні ознаки.

Сучасні методи перевірки живості базуються на аналізі мікротекстур, природних мікрорухів та оптичних артефактів, проте їх ефективність знижується при зміні освітлення, ракурсу та якості зображення. Додаткові фактори, такі як макіяж, аксесуари або висока зовнішня подібність між особами, ускладнюють класифікацію та підвищують ризик помилкових допусків і відмов. Найбільш критичними залишаються презентаційні атаки з використанням фотографій і відео, оскільки вони експлуатують плоску природу RGB-зображень. Застосування просторових ознак, зокрема глибини або альтернативних каналів, підвищує надійність автентифікації, дозволяючи відрізняти реальну тривимірну геометрію обличчя від плоских підробок та формувати незалежний від текстури критерій живості [1].

Інструменти прогнозування глибини з одиночного кадру останніми роками еволюціонували від задач загального сценного аналізу до прикладних сценаріїв, де необхідно відновлювати відносні карти глибини локальних об'єктів. У контексті біометричної автентифікації, така карта для обличчя відтворює його просторовий профіль і надає додаткову, комплементарну інформацію про форму, яка є більш стійкою до змін освітлення, макіяжу, аксесуарів або текстури шкіри, оскільки базується на геометрії, а не на фотометричних характеристиках. У практичних реалізаціях використовуються моделі на кшталт MiDaS, здатні формувати відносні глибинні поля з RGB кадру та адаптувати їх під обличчя як окремий сценний підоб'єкт. Результати попередніх досліджень і прикладних експериментів демонструють, що перехід у простір глибини відкриває нові дискримінативні ознаки, які не можуть бути повністю виловлені традиційним RGB описом. Спільне використання фотометричних та глибинних сигналів підвищує надійність і робастність біометричної автентифікації, забезпечуючи додатковий рівень захисту від презентаційних атак та інших спроб компрометації системи.

Роботи у сфері підвищення презентаційної стійкості демонструють, що комбінування RGB та глибинних ознак у двогілкових або багатозадачних нейронних мережах значно покращує розділення справжніх зразків від атак [1]. Дослідження, присвячені відновленню та уточненню глибинних даних обличчя, підтверджують придатність однокадрових глибинних реконструкцій як джерела 3D-критерію у біометричних та захисних модулях [2].

Запропонований підхід передбачає інтеграцію монокулярної глибини як додаткового рівня ознак у стандартній системі автентифікації. На вхід подається RGB кадр обличчя, з якого одночасно формуються 2D ембеддинги та прогнозується відносна карта глибини. Через масштабну неоднозначність монокулярної оцінки використовується відносний профіль, який зберігає стабільні просторові співвідношення між ключовими зонами обличчя, забезпечуючи перевірку живості. Глибинний опис нормалізується та узгоджується з 2D областю інтересу, формуючи спільний просторово-фотометричний вектор. Новизна підходу полягає у використанні відносної геометричної ознаки як критерію живості в умовах відсутності апаратних глибинних сенсорів, коли канал RGB є єдиним джерелом спостереження.

Модель прийняття рішення одночасно оцінює ідентичність за ембеддингом та узгодженість 3D профілю, суттєво знижуючи ймовірність проходу більшості 2D підробок навіть при наближенні фотометричних характеристик до реальних (рис. 1).

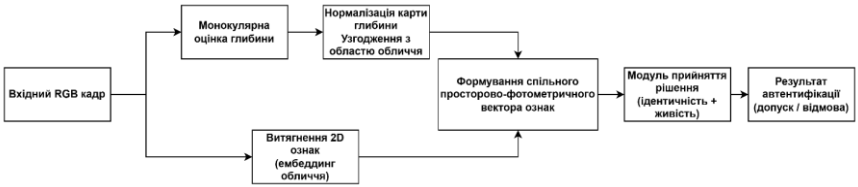

Рисунок 1 – Схема інтеграції монокулярної карти глибини у конвеєр біометричної автентифікації

Ключовим прикладним результатом запропонованого підходу є істотне підвищення стійкості біометричної автентифікації до презентаційних атак, зокрема друкованих фотографій і відеоповторів, завдяки інтеграції просторового контролю на основі монокулярної оцінки глибини без потреби додаткового апаратного обладнання. Практична реалізація підходу передбачає використання компактних моделей прогнозування відносної глибини та оптимізованого злиття 2D і 3D ознак, що забезпечує збереження швидкодії та відповідності вимогам реального часу. Така архітектура є придатною для мобільних і вбудованих платформ із обмеженими обчислювальними ресурсами та не потребує модифікацій існуючих конвеєрів розпізнавання. Отже, запропоноване рішення забезпечує ефективне поєднання доступності апаратних засобів, високої надійності перевірки живості та практичної придатності для сучасних систем біометричної автентифікації.

Література

1. SA-UNet for face anti-spoofing with depth estimation / J. Chen et al. Proceedings of the conference on face anti-spoofing. 2022. P. 9. DOI: https://doi.org/10.1117/12.2623137.

2. Schlett T., Rathgeb C., Busch C. Deep learning-based single image face depth data enhancement. Computer vision and image understanding. 2021. Vol. 210. P. 103247. DOI: https://doi.org/10.1016/j.cviu.2021.103247.

3. Мних М., Ткачук Р. Л., Федина Б. І. Організація оперативного управління кібербезпекою компанії. Інформаційна безпека та інформаційні технології : зб. тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022. (Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 30–32.

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

Відповідальні за випуск **Назарій БУРАК**
Олександр ХЛЕВНОЙ

Оригінал-макет **Юлія НАЗАР, Ольга СМОТР, Роман ГОЛОВАТИЙ, Діана РАЙТА, Віра ДОВБНЯК, Іван РОВЕЦЬКИЙ, Наталія ЖЕЗЛО-ХЛЕВНА**

Підписано до друку 12.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.