КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ЖАБСЬКА ЄЛИЗАВЕТА ОЛЕГІВНА

УДК 004.4

ДИСЕРТАЦІЯ

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ НА ОСНОВІ ЛОКАЛЬНО-ТЕКСТУРНИХ ДЕСКРИПТОРІВ

121 Інженерія програмного забезпечення
12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Є.О. Жабська

Науковий керівник: Меркулова Катерина Володимирівна,
кандидат технічних наук, доцент

Київ – 2025

АНОТАЦІЯ

Жабська Є.О. Математичне та програмне забезпечення біометричної ідентифікації на основі локально-текстурних дескрипторів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 121 «Інженерія програмного забезпечення» (12 – Інформаційні технології). – Київський національний університет імені Тараса Шевченка, Київ, 2025.

Більшість сучасних досліджень щодо розробки програмних рішень біометричної ідентифікації за зображенням обличчя ґрунтується на використанні алгоритмів штучного інтелекту. Проте ці підходи мають певні обмеження, зокрема низьку адаптивність до змінних умов реального середовища через потребу у великій кількості якісних навчальних даних і значних ресурсів для підтримки їхньої роботи. Альтернативою методам штучного інтелекту є локально-текстурні дескриптори, які, попри неоціненність у сучасних дослідженнях, демонструють низку переваг при використанні у програмному забезпеченні, а саме не потребують значних обсягів даних, потужних апаратних можливостей чи тривалого навчання, і за певних обставин можуть перевершувати методи на основі штучного інтелекту за ефективністю.

Дане дисертаційне дослідження присвячено вирішенню актуального наукового завдання підвищення ефективності програмного забезпечення біометричної ідентифікації за зображенням обличчя на основі локально-текстурних дескрипторів.

У першому розділі представлено огляд програмних рішень задачі біометричної ідентифікації за зображенням обличчя, у межах якого встановлено переваги використання обличчя як біометричної ознаки, зокрема її неінвазивність і високу прийнятність користувачами; здійснено огляд сучасних досліджень і виявлено, що основною причиною помилок при ідентифікації є різниця в якості еталонних і тестових зображень; проаналізовано проблеми розпізнавання обличчя, зокрема оклюзію, неоднорідність, старіння, розпізнавання за одним зразком та у

відеопотоці; досліджено процес біометричної ідентифікації та визначено потребу у ретельному підборі методів, покладених в його основі; сформульовано завдання дисертаційного дослідження, яке полягає у створенні комплексного методу біометричної ідентифікації на основі локально-текстурних дескрипторів з метою підвищення ефективності програмного забезпечення біометричної ідентифікації.

Другий розділ присвячено дослідженню та розробці математичного забезпечення для програмного рішення біометричної ідентифікації за зображенням обличчя. У межах цього розділу здійснено вибір методів для розв'язання задачі біометричної ідентифікації. Описано математичне забезпечення, що включає методи Віола-Джонса на основі каскадів Гаара, анізотропну дифузію, вейвлет-перетворення Ґабора, комбінацію дескрипторів 1DLBP (локальні бінарні шаблони в одновимірному просторі) і HOG (гістограм орієнтованих градієнтів) та квадратну евклідову відстань для обробки та класифікації зображень. На основі визначеного математичного підґрунтя розроблено комплексний метод біометричної ідентифікації та здійснено підбір його параметрів.

У третьому розділі описано процес створення програмної компоненти рішення задачі біометричної ідентифікації за зображенням обличчя, у межах якого визначено функціональні можливості програмного забезпечення, проаналізовано сценарії його використання, спроєктовано архітектуру та компоненти програмного рішення, розроблено структуру бази даних з урахуванням вимог до інтеграції в існуючі інформаційні системи, а також реалізовано вебзастосунок із клієнт-серверною архітектурою, що втілює розроблений комплексний метод біометричної ідентифікації.

У четвертому розділі дисертації описано проведення експериментального дослідження ефективності розробленого комплексного методу біометричної ідентифікації за зображенням обличчя на основі локально-текстурних дескрипторів. У результаті експериментів встановлено, що найвищої точності у 95% комплексний метод досягає при одночасному застосуванні дескрипторів 1DLBP та HOG на зображеннях низької якості. Виявлено низку чинників, які впливають на ефективність методу. Експериментально доведено можливість

підвищення точності на 5–30% завдяки перетворенням властивостей вхідних зображень. Порівняльний аналіз показав перевагу запропонованого комплексного методу над традиційними підходами та сучасними алгоритмами на основі штучного інтелекту.

Наукова новизна отриманих результатів:

1. Вперше запропоновано комбіноване використання методів вилучення ознак із зображень на основі локально-текстурних дескрипторів 1DLBP (локальні бінарні шаблони в одновимірному просторі) та HOG (гістограми орієнтованих градієнтів), що дозволило підвищити точність програмного забезпечення біометричної ідентифікації порівняно з окремим застосуванням дескрипторів.

2. Вперше розроблено комплексний метод біометричної ідентифікації за зображенням обличчя, який поєднує метод Віола-Джонса на основі каскадів Гаара для виявлення обличчя на зображенні, анізотропну дифузію для попередньої обробки зображення, вейвлет-перетворення Ґабора для обробки зображення, комбінацію локально-текстурних дескрипторів 1DLBP (локальні бінарні шаблони в одновимірному просторі) та HOG (гістограми орієнтованих градієнтів) для вилучення векторів ознак із зображення та метрику квадратної евклідової відстані для класифікації вектору ознак, що підвищило ефективність біометричної ідентифікації при варіативності якості зображень та умов їх фіксації.

3. Удосконалено розроблений комплексний метод біометричної ідентифікації шляхом визначення оптимальних параметрів методу вейвлет-перетворення Ґабора, таких як розмір фільтрів, орієнтації нормалі до паралельних смуг функції Ґабора, довжина хвилі синусоїдальної складової, зсув фази синусоїдальної функції, стандартне відхилення огинаючої Ґауса та просторове співвідношення сторін, що підвищило ефективність комплексного методу в програмному забезпеченні біометричної ідентифікації за зображенням обличчя.

Практичне значення отриманих результатів:

1. Розроблено математичне забезпечення біометричної ідентифікації для програмних систем, на основі якого створено комплексний метод біометричної ідентифікації особи за зображенням обличчя, що забезпечує здійснення процесу

ідентифікації шляхом отримання зображення, локалізації обличчя на зображенні, попередньої обробки зображення обличчя, обробки зображення обличчя, формування вектору ознак із зображення та подальшої його класифікації.

2. Створено програмне забезпечення біометричної ідентифікації за зображенням обличчя, в якому реалізовано такі функціональні можливості, як здійснення ідентифікації суб’єкта, перегляд попередніх результатів ідентифікації, перегляд записів бази даних, здійснення експериментального дослідження комплексного методу біометричної ідентифікації та підбір його параметрів.

Ключові слова: програмне забезпечення, біометрія, біометрична ідентифікація, інформаційні технології, комп’ютерний зір, розпізнавання шаблонів, цифрове зображення, обробка зображень, виявлення об’єктів, розпізнавання облич, аналіз даних, вилучення ознак, ключова точка, оцінка схожості зображень, класифікація.

ABSTRACT

Zhabska Y.O. Mathematical and software framework for biometric identification based on local texture descriptors. – Qualification scientific work on the rights of the manuscript.

The PhD thesis on competition of a scientific degree of the Doctor of Philosophy in the specialty 121 “Software Engineering” (12 – Information Technologies). – Taras Shevchenko National University of Kyiv, Kyiv, 2025.

Most modern research on the development of software solutions for biometric identification by face images is based on the use of artificial intelligence algorithms. However, these approaches have certain limitations, in particular, low adaptability to variable real-world conditions due to the need for a large amount of high-quality training data and significant resources required to support their operation. An alternative to artificial intelligence methods is the use of local-texture descriptors, which, despite being underappreciated in contemporary studies, demonstrate a number of advantages in software applications. In particular, they do not require large volumes of data, powerful hardware capabilities, or prolonged training processes, and under certain conditions may outperform artificial intelligence based methods in terms of efficiency.

This dissertation research is devoted to solving the topical scientific problem of increasing the efficiency of biometric identification software based on face images using local-texture descriptors.

The first chapter presents a review of software solutions for the problem of biometric identification based on face images, within which the advantages of using the face as a biometric feature are established, in particular its non-invasiveness and high user acceptability; a review of modern studies is carried out, and it is revealed that the main cause of errors during identification is the difference in quality between etalon and test images; the problems of face recognition are analyzed, including occlusion, heterogeneity, aging, single-sample recognition, and recognition in video streams; the process of biometric identification is investigated, and the necessity of careful selection of the methods underlying it is identified; the objective of the dissertation research is

formulated, which consists in developing a complex method of biometric identification based on local-texture descriptors with the aim of increasing the efficiency of biometric identification software.

The second chapter is devoted to the research and development of the mathematical framework for the software solution of biometric identification based on face images. Within this chapter, the selection of methods for solving the biometric identification problem is carried out. The mathematical framework is described, which includes the Viola-Jones method based on Haar cascades, anisotropic diffusion, Gabor wavelet transform, a combination of 1DLBP (local binary patterns in one-dimensional space) and HOG (histograms of oriented gradients) descriptors, and squared Euclidean distance for image processing and classification. Based on the defined mathematical foundation, a comprehensive biometric identification method is developed and its parameters selected.

The third chapter describes the process of developing the software component of the biometric identification solution based on face images, within which the functional capabilities of the software are defined, its usage scenarios analyzed, the architecture and components of the software solution designed, the database structure developed considering the requirements for integration into existing information systems, and a web application with client-server architecture implementing the developed complex biometric identification method is implemented.

The fourth chapter of the dissertation describes the conduct of experimental research on the efficiency of the developed complex biometric identification method based on face images using local-texture descriptors. As a result of the experiments, it was established that the highest accuracy of 95% is achieved by the complex method when 1DLBP and HOG descriptors are simultaneously applied to low-quality images. A number of factors influencing the efficiency of the method were identified. It was experimentally proven that accuracy can be improved by 5–30% through transformations of the properties of input images. A comparative analysis demonstrated the advantage of the proposed method over traditional approaches and modern artificial intelligence based algorithms.

Scientific novelty of the obtained results:

For the first time, a combined use of feature extraction methods from images based on local texture descriptors 1DLBP (local binary patterns in one-dimensional space) and HOG (histograms of oriented gradients) was proposed, which allowed to increase the accuracy of biometric identification software compared to the separate application of the descriptors.

For the first time, a comprehensive biometric identification method was developed, which combines the Viola-Jones method based on Haar cascades for face detection, anisotropic diffusion for image preprocessing, Gabor wavelet transform for image processing, a combination of local-texture descriptors 1DLBP (local binary patterns in one-dimensional space) and HOG (histograms of oriented gradients) for feature vector extraction from the image, and squared Euclidean distance metric for feature vector classification, which increased the efficiency of biometric identification under conditions of variability in image quality and capture conditions.

The developed complex biometric identification method was improved by determining the optimal parameters of the Gabor wavelet transform method, such as filter size, orientation of the normal to the parallel bands of the Gabor function, wavelength of the sinusoidal component, phase offset of the sinusoidal function, standard deviation of the Gaussian envelope, and spatial aspect ratio, which improved the efficiency of the comprehensive method in biometric identification software based on face images.

Practical significance of the obtained results:

The mathematical foundation for solving the biometric identification problem in software systems was developed, on the basis of which a complex method of biometric identification by face image was created, providing the identification process by acquiring an image, localizing the face in the image, preprocessing the face image, processing the face image, forming a feature vector from the image, and further classifying it.

A software component for solving the biometric identification problem based on face images was developed, which implements such functional capabilities as subject identification, viewing previous identification results, browsing database records,

conducting experimental research of the comprehensive biometric identification method, and selecting its parameters.

Keywords: software, biometrics, biometric identification, information technology, computer vision, pattern matching, digital image, image processing, object detection, face recognition, data analysis, feature extraction, interest point, image similarity evaluation, classification.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. O. Bychkov, K. Merkulova and Y. Zhabska, “Software Application for Biometrical Person’s Identification by Portrait Photograph Based on Wavelet Transform,” 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 253-256, doi: 10.1109/ATIT49449.2019.9030462.

2. Бичков О., Меркулова К., Жабська Є. Створення системи розпізнавання облич на основі вейвлет-перетворень. Проблеми інформаційних технологій, №26, 2019, с. 32-43, doi: 10.35546/2313-0687.2019.26.32-43.

3. G. P. Dimitrov, O. Bychkov, P. Petrova, K. Merkulova, Y. Zhabska et al., “Creation of Biometric System of Identification by Facial Image,” 2020 3rd International Colloquium on Intelligent Grid Metrology (SMAGRIMET), Cavtat, Croatia, 2020, pp. 29-34, doi: 10.23919/SMAGRIMET48809.2020.9263995.

4. O. Bychkov, K. Merkulova and Y. Zhabska, “Information Technology for Person Identification by Occluded Face Image,” 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2022, pp. 147-151, doi: 10.1109/TCSET55632.2022.9766867.

5. V. Martsenyuk, O. Bychkov, K. Merkulova and Y. Zhabska, “Exploring Image Unified Space for Improving Information Technology for Person Identification,” in IEEE Access, vol. 11, pp. 76347-76358, 2023, doi: 10.1109/ACCESS.2023.3297488.

6. K. Merkulova and Y. Zhabska, “Input Data Requirements for Person Identification Information Technology,” Proceedings of the 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023), CEUR Workshop Proceedings, 2023, pp. 24-37. [Online]. Available: https://ceur-ws.org/Vol-3468/paper3.pdf

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. O. Bychkov, K. Merkulova and Y. Zhabska, “Information Technology of Person’s Identification by Photo Portrait,” 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020, pp. 786-790, doi: 10.1109/TCSET49122.2020.235542.

2. O. Bychkov, K. Merkulova, Y. Zhabska and A. Shatyrko, “Development of information technology for person identification in video stream”, Proceedings of the II International Scientific Symposium “Intelligent Solutions” (IntSol-2021), CEUR Workshop Proceedings, 2021, pp. 70-80. [Online]. Available: https://ceur-ws.org/Vol-3018/Paper_7.pdf

3. O. Bychkov, K. Merkulova and Y. Zhabska, “Improvement of Information Technology for Person Identification for Usage in Energy Smart Systems,” 2022 IEEE 8th International Conference on Energy Smart Systems (ESS), Kyiv, Ukraine, 2022, pp. 199-203, doi: 10.1109/ESS57819.2022.9969307.

4. K. Merkulova and Y. Zhabska, “Investigating Methods of Input Data Preparation for Person Identification Information Technology,” 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2022, pp. 495-498, doi: 10.1109/CSIT56902.2022.10000539.

5. O. Bychkov, O. Ivanchenko, K. Merkulova and Y. Zhabska, “Enhancement of Information Technology for Person Identification Based on Image Quality Features,” Selected Papers of the IX International Scientific Conference “Information Technology and Implementation” (IT&I-2022), CEUR Workshop Proceedings, vol. 3347, 2022, pp. 1-10. [Online]. Available: https://ceur-ws.org/Vol-3347/Paper_1.pdf

6. O. Bychkov, Y. Zhabska, K. Merkulova and M. Merkulov, “Research and Comparative Analysis of Person Identification Information Technology,” Selected Papers of the III International Scientific Symposium “Intelligent Solutions” (IntSol-2023), CEUR Workshop Proceedings, vol. 3538, 2023, pp. 54-64. [Online]. Available: https://ceur-ws.org/Vol-3538/Paper_6.pdf

7. O. Bychkov, K. Merkulova, Y. Zhabska, “Exploring Conditions of Image Samples Formation for Person Identification Information Technology”, Selected Papers of the X International Scientific Conference “Information Technology and Implementation" (IT&I 2023), CEUR Workshop Proceedings, vol. 3646, 2023, pp. 33-42. [Online]. Available: https://ceur-ws.org/Vol-3646/Paper_4.pdf

Наукові праці, які додатково відображають наукові результати дисертації:

1. O. Bychkov, O. Ivanchenko, K. Merkulova and Y. Zhabska, “Mathematical Methods for Information Technology of Biometric Identification in Conditions of Incomplete Data”, Proceedings of the 7th International Conference "Information Technology and Interactions" (IT&I-2020), CEUR Workshop Proceedings, vol. 2845, 2020, pp. 336-349. [Online]. Available: https://ceur-ws.org/Vol-2845/Paper_31.pdf

2. Жабська Є. Інформаційна технологія ідентифікації особи за зображенням обличчя в умовах оклюзії. Енергетика і автоматика, 0(1), 2023, с. 136-149, doi: 10.31548/energiya1(65).2023.136.

3. O. Bychkov, K. Merkulova, Y. Zhabska, “Preprocessing Methods Study to Improve Information Technology for Person Identification by Occluded Image,” Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), CEUR Workshop Proceedings, vol. 3309, 2022, pp. 66-76. [Online]. Available: https://ceur-ws.org/Vol-3309/paper6.pdf

4. O. Bychkov, K. Merkulova and Y. Zhabska, “Research of Image Preprocessing Methods for Enhancement of Information Technology for Person Identification,” 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 293-296, doi: 10.1109/PICST57299.2022.10238550.

5. Жабська Є. О. Дослідження параметрів вхідних зображень для вдосконалення інформаційної технології ідентифікації особи. Зв'язок, №4, 2023, с. 7-12. doi: 10.31673/2412-9070.2023.042030.

ЗМІСТ

ВСТУП

Актуальність теми. Програмні рішення задачі розпізнавання обличчя дедалі більше інтегруються в критично важливі системи, що підкреслює їхню ключову роль у сучасних системах безпеки. Завдяки ефективним і неінвазивним можливостям ідентифікації та автентифікації, такі програми стають незамінними в багатьох галузях. Наразі найпоширенішою сферою використання програмних засобів розпізнавання облич є розблокування телефонів, ноутбуків та персональних комп'ютерів, яке охоплює 68% випадків. Проте відомо, що на сьогоднішній день майже 80% країн використовують програмне забезпечення розпізнавання обличчя у банківських і фінансових установах, приблизно 60% – в аеропортах, приблизно 40% – на робочих місцях, близько 20% – в школах, близько 20% – у автобусах, а 30% – у поїздах і метро. Більшість експертів, а саме близько 45%, прогнозують, що програмні рішення для розпізнавання облич лідируватимуть в зростанні використання, випереджаючи мультимодальне розпізнавання, найбільше розповсюдження якого прогнозують лише 16% експертів [1-5].

Очікується, що ринок програмного забезпечення розпізнавання облич продовжуватиме зростати в найближчі роки завдяки кільком ключовим факторам. Одним із основних факторів зростання є підвищення попиту на програмні засоби безпеки та відеоспостереження, особливо в громадських місцях, таких як аеропорти, торгові центри та урядові будівлі. Іншим важливим фактором є розширення застосування програм розпізнавання обличчя в різних секторах, таких як роздрібна торгівля, банківська справа та охорона здоров'я. Третім фактором зростання є технологічний прогрес у галузі розпізнавання облич, зокрема розробка програмного забезпечення, яке забезпечує більш точні та надійні результати, особливо в складних умовах, таких як слабке освітлення та часткова видимість рис обличчя.

Прогнози свідчать, що ринок програмного забезпечення розпізнавання облич буде зростати значними темпами до 2030 року. Очікується, що ринок

збільшуватиметься зі зведеним річним темпом зростання (CAGR) на 11,1% протягом прогнозованого періоду, а до 2032 року ринковий дохід від програмних рішень розпізнавання облич сягне 19,3 млрд доларів [1].

Хоча програмні засоби розпізнавання обличчя мають величезний потенціал для підвищення безпеки, зручності та ефективності в багатьох сферах, вони також породжують значні проблеми та викликають серйозні питання щодо своєї надійності та безпеки. Зокрема, нещодавні дослідження виявили вразливість програм на основі методів розпізнавання облич до змагальних (наприклад, атаки протилежних патчів) і бекдор (наприклад, отруєння навчальних даних) атак. Крім того, згідно з дослідженнями програмних рішень розпізнавання, зосередженими на природних атаках із видаванням себе за іншу особу та атаках ухилення в реальних сценаріях, наведеними у роботі [6], незважаючи на заяви багатьох постачальників послуг розпізнавання облич про точність, що перевищує 99%, з помилковою ідентифікацією або повною відмовою програм біометричної ідентифікації стикалися 47,95% і 80,82% користувачів відповідно.

Таким чином, наведені аналітичні дані та результати досліджень вказують на те, що актуальність розробки нового програмного забезпечення розпізнавання облич і потреба в удосконаленні існуючого лише зростатиме протягом найближчого десятиліття.

Більшість актуальних досліджень програмних рішень завдання біометричної ідентифікації за зображенням обличчя базуються на використанні штучного інтелекту. Однак такі підходи мають обмежену гнучкість і не завжди здатні швидко адаптуватися до динамічних умов реального світу, оскільки вимагають чималої кількості високоякісних навчальних даних і значних витрат на підтримку.

На противагу методам штучного інтелекту у програмному забезпеченні біометричної ідентифікації можуть використовуватися локально-текстурні дескриптори. Проте у сучасних роботах недостатньо розкрите питання можливості їх застосування, незважаючи на те, що такі методи не потребують великих обсягів даних, потужного обладнання або тривалого навчання, а за певних умов їхня ефективність перевершує ефективність методів штучного інтелекту. Відповідно,

дану роботу присвячено вирішенню актуального наукового завдання щодо дослідження умов удосконалення програмного забезпечення біометричної ідентифікації на основі комплексного методу, що містить локально-текстурні дескриптори.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційна робота виконана відповідно до поточних і перспективних планів наукової та науково-технічної діяльності кафедри програмних систем і технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Здобувач брала участь як виконавець у проєкті Erasmus+ №2020-1-PL01-KA203-082197 «Innovations for Big Data in a Real World (iBIGworld)» у 2020-2022 роках.

Здобувач брала участь як виконавець у науково-дослідній роботі кафедри програмних систем і технологій по темі №0121U113611 «Математичні методи та програмне забезпечення аналітики великих даних у реальному світі» у 2020-2024 роках.

Здобувач брала участь у науково-дослідній роботі факультету інформаційних технологій як виконавець по темі №24БП064-01М «Бездротова захищена система мінування/розмінування та моніторингу з інтелектуальним управлінням» у 2024 році.

Здобувач брала участь як виконавець у проєкті Erasmus+ №2023-2-PL01-KA220-HED-000179445 «TransLeader: The transferable training model – the best choice for training IT business leaders» у 2024-2025 роках.

Мета і завдання дослідження. Мета дисертаційної роботи полягає у підвищенні ефективності програмного забезпечення біометричної ідентифікації за зображенням обличчя на основі локально-текстурних дескрипторів при варіативності якості зображень та умов їх фіксації.

Для досягнення поставленої мети в дисертаційному дослідженні пропонується вирішення таких ключових завдань дослідження:

- Здійснити огляд та аналіз програмних рішень у сфері біометричної ідентифікації, виявити виклики, що постають при розв’язанні задачі біометричної ідентифікації за зображенням обличчя, та обґрунтувати доцільність застосування локально-текстурних дескрипторів для підвищення точності процесу біометричної ідентифікації.
- Розробити математичне підґрунтя розв’язання задачі біометричної ідентифікації, що включає вибір методів виявлення обличчя на зображенні, попередньої обробки, обробки зображення, вилучення вектору ознак і його класифікації, а також розробити на основі цих методів комплексний метод біометричної ідентифікації за зображенням обличчя.
- Виконати проєктування та реалізацію програмної компоненти на основі розробленого комплексного методу біометричної ідентифікації за зображенням обличчя, визначивши її функціональні можливості, сценарії функціонування, архітектуру та інформаційне забезпечення відповідно до принципів програмної інженерії.
- Здійснити експериментальне дослідження розробленого комплексного методу біометричної ідентифікації за зображенням обличчя, оцінити його ефективність на зображеннях з варіативністю якості та умов фіксації, порівняти результати з існуючими рішеннями та сформулювати вимоги до вхідних даних.

Об’єкт дослідження – процес біометричної ідентифікації за зображенням обличчя.

Предмет дослідження – методи й алгоритми проєктування та реалізації програмного рішення задачі біометричної ідентифікації за зображенням обличчя.

Методи дослідження: при виконанні завдань, поставлених у дисертаційному дослідженні, використовувалися загальні методи (аналіз, синтез, моделювання), емпіричні методи (експеримент, опис), а також методи та алгоритми аналізу й обробки зображень.

Наукова новизна отриманих результатів:

1. Вперше запропоновано комбіноване використання методів вилучення ознак із зображень на основі локально-текстурних дескрипторів 1DLBP (локальні бінарні шаблони в одновимірному просторі) та HOG (гістограми орієнтованих градієнтів), що дозволило підвищити точність програмного забезпечення біометричної ідентифікації порівняно з окремим застосуванням дескрипторів.

2. Вперше розроблено комплексний метод біометричної ідентифікації за зображенням обличчя, який поєднує метод Віола-Джонса на основі каскадів Гаара для виявлення обличчя на зображенні, анізотропну дифузію для попередньої обробки зображення, вейвлет-перетворення Ґабора для обробки зображення, комбінацію локально-текстурних дескрипторів 1DLBP (локальні бінарні шаблони в одновимірному просторі) та HOG (гістограми орієнтованих градієнтів) для вилучення векторів ознак із зображення та метрику квадратної евклідової відстані для класифікації вектору ознак, що підвищило ефективність біометричної ідентифікації при варіативності якості зображень та умов їх фіксації.

3. Удосконалено розроблений комплексний метод біометричної ідентифікації шляхом визначення оптимальних параметрів методу вейвлет-перетворення Ґабора, таких як розмір фільтрів, орієнтації нормалі до паралельних смуг функції Ґабора, довжина хвилі синусоїдальної складової, зсув фази синусоїдальної функції, стандартне відхилення огинаючої Ґауса та просторове співвідношення сторін, що підвищило ефективність комплексного методу в програмному забезпеченні біометричної ідентифікації за зображенням обличчя.

Практичне значення отриманих результатів:

1. Розроблено математичне забезпечення біометричної ідентифікації для програмних систем, на основі якого створено комплексний метод біометричної ідентифікації особи за зображенням обличчя, що забезпечує здійснення процесу ідентифікації шляхом отримання зображення, локалізації обличчя на зображенні, попередньої обробки зображення обличчя, обробки зображення обличчя, формування вектору ознак із зображення та подальшої його класифікації.

2. Створено програмне забезпечення біометричної ідентифікації за зображенням обличчя, в якому реалізовано такі функціональні можливості, як здійснення ідентифікації суб'єкта, перегляд попередніх результатів ідентифікації, перегляд записів бази даних, здійснення експериментального дослідження комплексного методу біометричної ідентифікації та підбір його параметрів.

Особистий внесок здобувача. Дисертаційне дослідження є самостійною науковою працею здобувача, у якій представлені ідеї та розробки, що дали змогу вирішити поставлені завдання. У публікаціях здобувачеві належать наступні результати: у статтях [7-9] досліджено методи обробки зображень облич на основі вейвлет-перетворень у комбінації з різними методами формування векторів ознак зображень і їх класифікації (вклад у статтю [7] складає 75%, у статтю [8] – 80%, у статтю [9] – 83%); у роботі [10] представлено концептуальну модель та математичні методи обробки зображень облич на основі вейвлет-перетворення Ґабора, проаналізовано етапи обробки зображень та формування векторів ознак за допомогою обчислення статистичних характеристик (вклад у статтю складає 60%); у роботі [11] досліджено математичні методи біометричної ідентифікації за зображенням обличчя в умовах неповних даних (вклад у статтю складає 75%); у статті [12] вперше запропоновано комплексний метод біометричної ідентифікації за зображенням обличчя, який включає такі методи, як анізотропна дифузія, вейвлет-перетворення Ґабора, локальні бінарні шаблони в одновимірному просторі та гістограми орієнтованих градієнтів (вклад у статтю складає 75%); у роботах [13-14] досліджено та проаналізовано запропонований метод біометричної ідентифікації в умовах неповної видимості рис обличчя на зображеннях (вклад у статтю [13] складає 80%, у статтю [14] – 100%); у роботі [15] досліджено запропонований метод біометричної ідентифікації для використання в розумних енергетичних системах (вклад у статтю складає 77%); у роботах [16-18] описані дослідження методів попередньої обробки зображень облич з метою покращення ефективності запропонованого методу біометричної ідентифікації (вклад у статтю [16] складає 82%, у статтю [17] – 90%, у статтю [18] – 85%); у статтях [19-21] досліджено умови та підбір параметрів запропонованого методу біометричної

ідентифікації для створення уніфікованого за властивостями простору зображень облич, що подаються на вхід методу (вклад у статтю [19] складає 75%, у статтю [20] – 75%, у статтю [21] – 100%); у статті [22] сформульовано вимоги до зображень, що подаються на вхід запропонованого методу біометричної ідентифікації, до яких застосування методу є найбільш ефективним (вклад у статтю складає 90%); у статті [23] описано дослідження та порівняльний аналіз запропонованого методу біометричної ідентифікації з підходами на основі методів штучного інтелекту (вклад у статтю складає 73%); у статті [24] проаналізовано ефективність запропонованого методу біометричної ідентифікації при застосуванні його до зображень, зафіксованих у контрольованих і неконтрольованих умовах навколишнього середовища (вклад у статтю складає 85%).

Апробація матеріалів дисертації. Основні результати дисертаційного дослідження доповідалися та обговорювалися на наукових семінарах кафедри програмних систем і технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, на міжнародних і національних наукових і науково-практичних конференціях, семінарах:

- 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT 2019, Київ, 18-20 грудня 2019 року);
- 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET 2020, Львів-Славське, 25-29 лютого 2020 року);
- 3rd International Colloquium on Intelligent Grid Metrology (SMAGRIMET 2020, Дубровнік, 20-23 жовтня 2020 року);
- 7th International Conference “Information Technology and Interactions” (IT&I 2020, Київ, 2-3 грудня 2020 року);
- 2nd International Scientific Symposium “Intelligent Solutions” (IntSol 2021, Київ-Ужгород, 28-30 вересня 2021);

- 16th IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET 2022, Львів-Славське, 22-26 лютого 2022 року);
- 8th IEEE International Conference on Energy Smart Systems (ESS 2022, Київ, 12-14 жовтня 2022 року);
- 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022, Тернопіль, 22-24 листопада 2022 року);
- 17th IEEE International Conference on Computer Science and Information Technologies (CSIT 2022, Львів. 10-12 листопада 2022 року);
- 4th International Scientific Conference "Information Technology and Implementation" (IT&I 2022, Київ, 30 листопада – 2 грудня 2022 року);
- 9th IEEE International Conference on Problems of Infocommunications Science and Technology (PICS&T 2022, Харків, 10-12 жовтня 2022 року);
- 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023, Тернопіль, 14-16 червня 2023 року);
- 3rd International Scientific Symposium "Intelligent Solutions" (IntSol 2023, Київ, 27-28 вересня 2023 року);
- 10th International Scientific Conference "Information Technology and Implementation" (IT&I-WS 2023, Київ, 20-21 листопада 2023 року).

Публікації. Основні результати дисертаційного дослідження опубліковано у 18 наукових роботах, з яких 14 – у матеріалах міжнародних науково-технічних конференцій, 1 – у міжнародному реферованому журналі віднесеному до першого квартиля (Q1) відповідно до класифікації Scimago Journal & Country Rank, 3 – у вітчизняних фахових виданнях (15 публікацій проіндексовано в наукометричній базі даних Scopus, 4 – у Web of Science).

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи складає 205 сторінок, з них 172 основного тексту; робота містить 27 таблиць, 61 рисунок, 2 додатки, список використаних джерел зі 122 найменувань.

РОЗДІЛ 1. ОГЛЯД ПРОГРАМНИХ РІШЕНЬ ЗАДАЧІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

1.1 Програмні рішення задачі біометричної ідентифікації

Біометричне розпізнавання спрямоване на встановлення зв'язку між особистим ідентифікатором та конкретною особою шляхом аналізу її фізичних або поведінкових ознак [25]. На відміну від традиційних програмних засобів біометричної ідентифікації, робота яких ґрунтується на знаннях (наприклад, паролі) або фізичних носіях (наприклад, токени, смарт-карти), біометричне програмне забезпечення використовує унікальні біологічні та поведінкові характеристики особи.

Впровадження біометричних систем у різноманітних сферах підкреслює значущість розробки масштабних програмних систем ідентифікації, здатних забезпечувати стабільну точність в умовах змінного середовища. Зі зростанням кількості зареєстрованих користувачів критичною є підтримка високої точності розпізнавання. Програмне забезпечення біометричної ідентифікації має відповідати вимогам щодо точності, швидкості обробки, ефективного використання ресурсів, безпеки та прийнятності для користувачів і стійкості до шахрайських атак [26].

Технологія розпізнавання облич набула значного поширення за останні десятиліття завдяки своїй відносній простоті в аналізі зображень і розпізнаванні образів, а також доступності у сучасних цифрових пристроях [27]. Розпізнавання обличчя визначається як процес встановлення особи людини на основі її характеристик обличчя. Ця технологія передбачає порівняння двох зображень для встановлення їхньої відповідності. Попри здатність людини розпізнавати обличчя за різних умов, автоматизовані програмні рішення стикаються з викликами, пов'язаними зі змінами віку, пози, освітлення, виразів обличчя, а також наявністю зовнішніх факторів, таких як макіяж чи аксесуари. Складність розробки таких рішень зумовлена недостатнім розумінням когнітивних і нейронних механізмів, що лежать в основі людського сприйняття обличчя [28].

Попри певні обмеження, розпізнавання облич є одним із найпоширеніших біометричних методів через низку переваг [27]: обличчя природно використовується для ідентифікації; зображення обличчя можна отримати безконтактним способом без спеціальних датчиків; мінімальна взаємодія з користувачем; висока соціальна прийнятність, зважаючи на публічний доступ до зображень облич в соцмережах.

Розвиток технологій розпізнавання облич сприяв їх впровадженню в різні сфери. Програмні рішення, такі як Face++ [29], активно застосовуються для ідентифікації осіб в аеропортах, банківських установах і системах відеоспостереження. Система Amazon Rekognition [30] використовується для аналізу відеозаписів і фотографій у комерційних застосунках з метою підвищення рівня безпеки у торгових центрах і на масових заходах. Azure AI Vision [31] забезпечує безконтактну ідентифікацію в корпоративному секторі та медичних установах, зокрема для контролю доступу до приміщень і підтвердження особи пацієнтів.

До інших прикладів програмного забезпечення належать FaceFirst [32], яке застосовується в торговельних мережах для ідентифікації клієнтів і забезпечення безпеки, а також NEC Face Recognition [33], що використовується для безконтактної перевірки осіб на масових заходах та в системах громадської безпеки.

Постійне вдосконалення методів розпізнавання сприяло підвищенню їхньої точності та доступності, що зумовило їх широке використання в більш складних умовах. Наприклад, IARPA розробляє технології для ідентифікації облич у відеоспостереженні за ускладнених умов, спеціальні програми застосовуються військовими та правоохоронними органами, зокрема в безпілотниках для збору розвідданих, рятувальних операцій і контролю безпеки [34, 35].

Програмне забезпечення розпізнавання облич Clearview AI широко використовується під час російсько-української війни для пошуку та ідентифікації біженців, викриття неправдивих повідомлень про війну в соціальних мережах, підвищення безпеки та встановлення особи загиблих військовослужбовців [36].

1.2 Огляд програмних рішень біометричної ідентифікації за зображенням обличчя

У статті [27] аналізується сучасний стан інженерії програмного забезпечення для розпізнавання облич на основі 180 наукових праць. Незважаючи на досягнутий прогрес, автори висвітлюють ключові проблеми, з якими стикаються дослідники в цій галузі, такі як оклюзія, старіння та розпізнавання за єдиним зразком зображення обличчя. Наголошується на необхідності подолання цих викликів з урахуванням високих вимог до точності та безпеки програм розпізнавання обличчя.

Аналізуючи сучасні дослідження у галузі розпізнавання облич, можна відзначити, що хоча дані, отримані за допомогою відповідних програмних засобів, застосовуються у багатьох сферах, однак зображення, зафіксовані камерами відеоспостереження, автофіксації чи мобільними пристроями, часто мають низьку якість, тоді як бази даних містять високоякісні знімки, отримані під час оформлення документів. Різниця у якості порівнюваних зображень часто стає причиною збою процесу ідентифікації у програмному забезпеченні. Тому необхідним є дослідження можливості підвищення ефективності програмних засобів біометричної ідентифікації шляхом зміни властивостей зображень, які вони обробляють.

У дослідженні [37] описано програмний засіб розпізнавання облич у реальному часі, що використовує надвисоку роздільну здатність для покращення процесу обробки зображень та виявлення облич. Підхід спрямований на збільшення кількості дескрипторів і зменшення шуму, реалізований на основі паралельної архітектури для підвищення ефективності алгоритму.

У статті [38] запропоновано програмне забезпечення на основі моделі розпізнавання облич із низькою роздільною здатністю, що ґрунтується на співставленні ознак. Модель включає ідентифікаційну функцію втрати, яка поєднується з втратою ознак і втратою вмісту зображення для спільного навчання.

Автори статті [39] аналізують відмінності між зображеннями зі зниженою дискретизацією та реальними зображеннями низької роздільної здатності. Встановлено, що продуктивність програмних засобів розпізнавання залежить не

лише від обсягу інформації у зображенні, а й від вирівнювання, що є критичним чинником за відсутності змін пози та освітлення.

У роботі [40] запропоновано програмне рішення щодо покращення ідентифікації зображень облич у навчальних наборах даних шляхом використання норми ознак як показника якості. Автори адаптивно змінювали функцію відстані залежно від норми ознак, що дозволило контролювати масштаб градієнта для зображень різної якості.

У дослідженні [41] представлено програмне рішення на основі словникового методу для розпізнавання облич із різними рівнями розмитості. Метод продемонстрував підвищену надійність при обробці зображень низької якості.

У роботі [42] для усунення розбіжностей між зображеннями високої та низької роздільної здатності запропоновано програмне рішення на основі багатовимірного масштабування. Дискримінативні властивості покращено шляхом введення міжкласового обмеження, що збільшує відстань між різними суб'єктами у підпросторі. Дослідження розширено в [43], де цей метод застосовано для навчання матриці відображення, що перетворює зображення обох типів у спільний підпростір, забезпечуючи кращу розрізнювальну здатність.

Більш обчислювально ефективний варіант багатовимірного масштабування, заснований на референсах, запропоновано у роботі [44]. Програмне рішення порівнює тестові зображення лише з вибраними референсними зображеннями, а не з усією базою даних. Для вирівнювання зображень побудовано два ортогональні словники в областях низької та високої роздільної здатності, використовуючи зіставлення дводольних графів.

У роботі [45] запропоновано програмне рішення, засноване на дискримінантному кореляційному аналізі (DCA), що покращує відмінності між класами та має переваги над канонічним кореляційним аналізом.

Автори [46] виявили, що оклюзії на тестових зображеннях із низькою роздільною здатністю часто ігноруються. Для виявлення оклюзії та вилучення глобальних структур зображень застосовано програмний засіб на основі методу представлення зображень подвійною низькорівневою ранговою матрицею.

У статті [47] запропоновано програмне рішення на основі безцентрової регуляризації, яке зближує зразки внутрішнього класу у просторі представлення. Робота [48] описує додаткову розгалужену мережу поверх основної, використовуючи функцію втрат на основі парного відображення для покращеного навчання у домені ознак.

Аналіз тенденцій у сучасних дослідженнях свідчить про те, що, незважаючи на високу ефективність методів розпізнавання облич у різних програмних рішеннях, вони залишаються вразливими до атак противника, що підриває їхню надійність у реальних сценаріях використання.

Дослідження [49] висвітлює, як зображення природного вигляду можуть вводити в оману системи розпізнавання обличчя, призводячи до помилкових прогнозів. Більш того, у роботі [50] описано фізичну атаку, яка використовує тканинні маски з візерунками для уникнення програм розпізнавання обличчя. Маски, спроєктовані для ідеального злиття з обличчям носія, викликають помилкову ідентифікацію за різних умов і в різних середовищах.

У роботі [51] досліджено вразливість глибоких нейронних мереж (DNN) до атак на програмне забезпечення розпізнавання обличчя. Встановлено їхню сприйнятливість цих методів до збурень, що вимагає розробки безпечних програмних систем, особливо в критичних для безпеки сферах.

У статті [52] розглянуто модель загроз для програмних засобів розпізнавання облич у контексті поширеності DNN та аутсорсингу. Визначено бекдор-атаки як загрозу, що виникає через маніпуляції навчанням або розгортанням DNN, що порушує цілісність системи. Огляд досліджень щодо бекдор-атак та методів захисту підкреслює необхідність розробки стратегій протидії.

Очікується, що світовий ринок програмного забезпечення для розпізнавання облич зросте з 3,72 млрд доларів США у 2020 році до 11,62 млрд доларів США до 2026 року, згідно зі звітом Mordor Intelligence [53]. Інший звіт від Grand View Research [54] також передбачає значне зростання попиту на програмне забезпечення для розпізнавання облич, особливо в сегменті безпеки, з високими темпами зростання в найближчі роки.

Результати вищенаведеного аналізу свідчать про те, що наразі існує критична потреба в розробці програмних рішень біометричної ідентифікації за зображенням обличчя, стійких до новітніх вразливостей та агресивних атак, а також у дослідженні існуючого програмного забезпечення для підвищення ефективності ідентифікаційного процесу. Відповідно, важливо детально проаналізувати проблеми програмних рішень, які можуть обмежувати їхню ефективність та точність у реальних умовах використання.

1.3 Проблеми програмних рішень задачі біометричної ідентифікації за зображенням обличчя

У більшості біометричних застосунків зміни зовнішнього вигляду, викликані необмеженим середовищем, створюють проблеми для програмного забезпечення розпізнавання облич. Розглянемо проблеми, які необхідно вирішити найближчим часом [27]:

1. Оклюзія зображення. Оклюзія спотворює риси обличчя, за якими можливо розпізнати особу, та збільшує відстань у просторі ознак між двома зображеннями одного суб’єкта. Варіації всередині класу більші, ніж варіації між класами, що призводить до низьких результатів роботи програмних засобів розпізнавання [55].

Прикладом реального прецеденту, коли умови зовнішнього середовища можуть впливати на результати роботи програмних рішень для розпізнавання за зображенням обличчя є пандемія COVID-19 [56]. Всесвітня організація охорони здоров’я рекомендувала використання медичних масок як частину стратегії комплексних заходів із придушення передачі захворювання. Проте маски, що повністю закривають нижню половину обличчя людини, ускладнюють процес ідентифікації. У липні 2020 року Національний інститут стандартів і технологій провів дослідження точності розпізнавання облич з масками, використовуючи програмне забезпечення на основі алгоритмів, що існували до пандемії [57]. Результати показали значне зниження точності ідентифікації — найбільш точні алгоритми не змогли ідентифікувати особу в 20-50% випадків. Поява маски на зображенні обличчя призвела до неможливості виділення рис обличчя, що

порушило роботу алгоритмів. У дослідженні також вивчали три рівні закриття носа маскою (низький, середній, високий), і встановлено, що точність знижується з більшим покриттям носа: помилкові невідповідності збільшувалися в 10, 25 і 36 разів для медіанних алгоритмів [58].

У листопаді 2020 року NIST оновив свої дослідження щодо точності розпізнавання облич з масками за допомогою алгоритмів, удосконалених після початку пандемії. Встановлено, що точність алгоритмів все ще знижується при покритті 70% обличчя маскою. Попри заяви розробників про покращену ефективність, деякі алгоритми не ідентифікують особу в 10-40% випадків, а точність розпізнавання таких програмних рішень порівнянна з алгоритмами середини 2017 року [59].

2. Розпізнавання неоднорідних облич. Це завдання полягає у встановленні програмним рішенням кореляції між двома зображеннями обличчя, які були створені за допомогою різних методів візуалізації, що дуже корисно в юридичних цілях. Наприклад, інфрачервоне зображення [60, 61] може бути єдиним способом отримати корисне зображення підозрюваного в нічних умовах, тоді як поліцейські файли є зображеннями у видимому спектрі. Або, у випадку відсутності зображення підозрюваного, може бути створений юридичний ескіз на основі опису очевидця. Зіставлення таких ескізів із фотографіями облич є важливим у юридичних запитах. Також можливі ситуації, коли зображення, на яких необхідно ідентифікувати особу, та зображення, що зберігаються в базі даних, мають різну якість, наприклад, коли зображення з камер відеоспостереження, що зазвичай характеризуються низькою якістю, порівнюються із високоякісними зображеннями, збереженими в урядових базах даних. Таке співставлення неоднорідних зображень облич може призвести до некоректної або хибно коректної ідентифікації програмним забезпеченням. Тому дослідження програмних рішень на основі методів уніфікації таких зображень є актуальним і необхідним.

3. Розпізнавання обличчя та старіння. Старіння обличчя – це складний процес, який впливає на форму та текстуру обличчя (наприклад, тон шкіри або зморшки). Типовий сценарій застосування програмних засобів розпізнавання облич

проти ефекту старіння полягає у виявленні присутності конкретної особи в раніше зареєстрованій базі даних (наприклад, ідентифікація зниклих дітей або контроль підозрюваних у списку спостереження). Оскільки віковий проміжок між зображенням запиту та еталонним зображенням тієї самої особи збільшується, точність розпізнавання у програмних рішеннях зазвичай знижується [62].

4. Розпізнавання обличчя за єдиним зразком є однією з найбільш реалістичних та складних задач у галузі розпізнавання обличчя [63]. У цьому випадку для навчання системи доступне лише одне зображення обличчя особи. У реальних застосунках (наприклад, в імміграційних системах) зазвичай в базі даних зареєстрована і доступна для розпізнавання лише одна модель для кожної особи [64]. Проте деякі програмні засоби розпізнавання вимагають величезних навчальних даних для забезпечення коректної роботи [63]. Таким чином, розпізнавання обличчя за єдиним зразком залишається актуальною і невирішеною проблемою, яка є однією з основних напрямків наукових досліджень.

5. Розпізнавання облич у відеоспостереженні. Програмні засоби розпізнавання облич широко використовуються в системах відеоспостереження [65]. Їхня ефективність залежить від умов зйомки, таких як зміна пози та артефакти, спричинені методами отримання зображень. В основному існують проблеми з фокусуванням камери, які можуть призвести до розмиття зображення, помилок із низькою роздільною здатністю або стисненням і ефектів блокування. Завданням програмних засобів розпізнавання облич є ідентифікація особи на зображеннях з низькою якістю або змінними позами. Ця проблема залишається актуальною та потребує подальших досліджень.

З урахуванням наведених проблем, важливо зазначити, що ефективність програмних рішень біометричної ідентифікації безпосередньо залежить від методів, що лежать в основі ідентифікаційного процесу. Тому необхідно детально дослідити процес біометричної ідентифікації за зображенням обличчя та методи, які забезпечують його реалізацію.

1.4 Процес біометричної ідентифікації та методи, покладені в його основу

Процес автоматизованої ідентифікації обличчя складається з трьох ключових етапів. Перший етап – виявлення обличчя на зображенні, яке подається на вхід методу ідентифікації. Вихідне зображення сканується вікном змінного розміру, при застосуванні якого відбувається визначення ступеня схожості сканованої області з шаблоном, що відповідає обличчю.

Другий етап – вилучення вектору ознак з області зображення, що містить обличчя. Часто для покращення результатів на даному етапі можуть застосовуватись методи попередньої обробки зображення.

Останній етап — ідентифікація особи, яка включає визначення унікального ідентифікатора особи, обличчя якої виявлено на зображенні, або позначення особи як невідомої, якщо зразок не знайдений у базі даних [66].

Ефективність методу біометричної ідентифікації визначається точністю, яка залежить від методів, покладених в основу ідентифікаційного процесу. Тому доцільним є здійснення аналізу та експериментальних досліджень для вибору таких методів.

Для виконання першого етапу процесу біометричної ідентифікації застосовуються методи виявлення обличчя, які дозволяють локалізувати ділянку зображення, що з високою ймовірністю містить риси обличчя. Ефективність цього етапу значною мірою впливає на точність подальших процедур, оскільки помилки локалізації можуть спричинити втрату критично важливої інформації. Існують кілька підходів для виявлення облич на зображеннях, більшість з яких засновані на виділенні локально-текстурних ознак та застосуванні бінарних класифікаторів для виявлення області зображення, що містить обличчя. Розглянемо деякі з них.

Перший підхід, запропонований Віола та Джонсом, базується на використанні фільтрів Гаара для виявлення облич. Метод Віола-Джонса широко застосовується у різних дослідженнях через можливість використання у реальному часі, швидкість виявлення, високу точність і доступність програмного забезпечення з відкритим кодом [67]. Однак цей метод схильний до хибнопозитивних (обличчя

виявлено, якщо його немає на зображенні) і хибнонегативних (обличчя не виявлено, хоча воно міститься на зображенні) помилок.

Для задач детекції та класифікації облич у комп'ютерному зорі може бути використано метод опорних векторів (SVM). Цей метод створює максимальну граничну гіперплощину, яка відокремлює два класи даних [68]. Позитивні зразки представляють класи об'єктів, а негативні – класи, що не містять об'єктів. SVM є ефективним для виявлення облич з різними позами та умовами освітлення, забезпечуючи високу точність і низький рівень помилок. Однак основним недоліком є потреба в значній кількості тренувальних даних для досягнення високої точності, що робить метод обчислювально вимогливим та ресурсозатратним.

Метод послідовного перетворення середнього квантування (SMQT) та класифікатор розрідженої мережі елементів просіювання (SNOW) [69] використовуються для випадків класифікації, коли кількість важливих характеристик об'єктів може бути великою та завчасно невідомою. Цей підхід є швидким і ефективним з точки зору обчислень, проте потребує великої кількості навчальних даних.

Для виявлення облич широко використовуються нейронні мережі, що складаються з персептронів, з'єднаних у кілька шарів. Мережа сканує зображення малим вікном без необхідності навчання на зображеннях без обличчя, що зменшує обчислювальне навантаження [70]. Однак для налаштування мережі потрібні великі обсяги зображень, що містять обличчя.

У роботі [71] проведено експериментальне дослідження для порівняння вищенаведених методів виявлення обличчя. Результати порівняльного аналізу наведено в Таблиці 1.1. Точність вказує на кількість коректно класифікованих позитивних екземплярів серед усіх визначених як позитивні, повнота – на частку коректно визначених позитивних екземплярів серед усіх дійсно позитивних.

Таблиця 1.1 – Результати порівняльного аналізу методів виявлення обличчя

Метод виявлення обличчя	Точність	Повнота
Метод виявлення Віола-Джонса	0.27321	0.27321
Метод опорних векторів	0.26792	0.26792
Ознаки SMQT та класифікатор SNOW	0.339450	0.037582
Нейромережеві методи	0.01392850	0.00835708

На основі результатів експериментів найвище значення відносно таких метрик оцінки, як точність та повнота, має метод Віола-Джонса на основі каскадів Гаара. Отже, доцільним є використання цього методу у подальших дослідженнях.

Після виявлення обличчя зображення потребує попередньої обробки для покращення якості вхідних даних, яка є важливим фактором, що впливає на ефективність методів розпізнавання обличчя. Низька роздільна здатність або наявність шумів на зображеннях можуть призвести до помилок у процесі ідентифікації [72]. Попередня обробка зображень покращує їхні локальні й глобальні характеристики, сприяючи ефективнішому вилученню ознак і підвищенню точності розпізнавання. Основними методами для цього є нормалізація, фільтрація, вирівнювання гістограми, зміна розміру і кадрування зображень.

Кадрування виділяє область виявленого на зображенні обличчя, усуваючи деталі, що не є суттєвими для процесу ідентифікації або йому перешкоджають. Подальша зміна розміру зображення після виділення області обличчя сприяє зменшенню обсягу даних, пришвидшенню обробки та уніфікації вхідних даних для ідентифікації. Проте надмірне зменшення масштабу може призвести до втрати важливих ознак обличчя, особливо текстурних. Тому визначення оптимального розміру зображення залишається актуальним завданням дослідження можливості підвищення ефективності процесу ідентифікації.

Зміна яскравості є базовим методом попередньої обробки, що коригує загальну освітленість зображення шляхом додавання або віднімання постійного

значення до кожного пікселя. Цей процес дозволяє виділити особливості зображення обличчя, важливі для ідентифікації [73].

Змінність освітлення ускладнює розпізнавання облич, оскільки неконтрольовані умови освітлення при фіксації зображення призводять до нерівномірного розподілу яскравості. Для вирівнювання розподілу застосовуються методи корекції, зокрема техніки вирівнювання гістограм [74].

Методи нормалізації яскравості зображень обличчя забезпечують їх коректне порівняння шляхом приведення до стандартного рівня яскравості. Найпоширенішими підходами є вирівнювання гістограми, специфікація гістограми та логарифмічне перетворення.

Вирівнювання гістограми (HE) покращує контрастність зображення шляхом перерозподілу рівнів яскравості, роблячи їх рівноймовірними. Логарифмічне перетворення (LOG) моделює чутливість людського ока до світла, а корекція інтенсивності гами (GIC) нормалізує яскравість до канонічного вигляду, зменшуючи вплив освітлення. Однак ці методи можуть спотворювати риси обличчя, знижуючи точність розпізнавання у випадках незначних змін освітлення. Дослідження [75] показало, що HE є найбільш ефективним, оскільки не потребує складних обчислень і полегшує розпізнавання при варіаціях освітлення.

Анізотропна дифузія може використовуватися як метод попередньої обробки зображень для зменшення шуму та розмиття, зберігаючи висококонтрастні межі. Зазвичай метод анізотропної дифузії використовується для покращення медичних зображень, проте в межах даного дослідження вирішено застосувати даний метод для попередньої обробки зображень облич з метою подальшої їх ідентифікації. Альтернативним підходом є вирівнювання гістограми, яке покращує якість зображення, розширюючи його динамічний діапазон. Цей метод дозволяє рівномірно розподілити яскравість, що підвищує візуальну якість і деталізацію зображення. Оскільки обидва методи виконують різні функції в обробці зображень, доцільно провести дослідження їх ефективності для покращення результатів біометричної ідентифікації при застосуванні як окремо, так і в комбінації.

Наступним кроком виконання процесу біометричної ідентифікації є обробка зображень. Методи обробки спрямовані на забезпечення максимальної узгодженості між зразками зображень, що містять обличчя. У задачах обробки зображення часто розглядаються як випадкові поля через наявність шумів. Для стаціонарних сигналів ефективним є перетворення Фур'є, однак для нестаціонарних сигналів необхідна локалізація частотних змін у часі. Вейвлет-перетворення забезпечує таку локалізацію, використовуючи базисні функції з обмеженою областю визначення [76].

Загальний принцип вейвлет-перетворення ґрунтується на масштабних перетвореннях і зсувах, що дозволяє аналізувати характеристики сигналу на різних рівнях деталізації. Представлення зображення через вейвлет-функції сприяє зменшенню ентропії, що полегшує його кодування [77].

Сигнали, до яких застосовується вейвлет-перетворення, зазвичай представлені квадратично-інтегрованими функціями на множині дійсних чисел. Ортонормовані вейвлети з компактним носієм для нескінченної дійсної осі були розроблені Добеші [78]. Їхня масштабувальна та вейвлет-функції є асиметричними, оскільки побудовані з використанням мінімальних фазових квадратних коренів для концентрації енергії біля початкової точки компактного носія.

Симлети – це модифікація вейвлетів Добеші з меншою асиметричністю. Вони використовують єдиний набір коренів фази для забезпечення більшої симетричності з лінійною комплексною фазою. Конструкція симлетів оптимізована для максимізації кількості нульових моментів на всій довжині носія [76].

Окремим випадком вейвлетів Добеші є койфлети, які формуються шляхом накладання умови нульового моменту на вейвлет-функцію та функцію масштабування, що призводить до збільшення кількості коефіцієнтів [76].

Біортогональні вейвлети – клас вейвлетів, що не є ортогональними до функцій масштабування, але зберігають властивості напівортогональних базисів. Їхня побудова ґрунтується на розрідженні матриць аналізу та синтезу, що підвищує швидкодію розкладу та відновлення сигналів [79]. У біортогональній системі

функції вейвлету та масштабування використовуються окремо для аналізу й синтезу сигналу, що забезпечує одночасну роботу в часовій і частотній областях.

При зворотному біортогональному вейвлет-перетворенні функції синтезу застосовуються для аналізу та навпаки. Зворотні біортогональні вейвлети використовуються як у часовій, так і у частотній областях, формуючи прості хвильові структури. Вейвлет-функція завжди адаптується до розміру області перегляду, що вирішує проблему узгодження часової та частотної роздільної здатності.

Широкого поширення в галузі вейвлет-перетворень набули функції, вперше запропоновані Ґабором, який сформулював «квантовий принцип» інформації: об'єднана частотно-часова область для одномірних сигналів обов'язково має квантуватися таким чином, щоб жоден сигнал або фільтр не захоплював у цій області значення, менші за певні мінімальні пороги [80]. Представлення зображень вейвлетами Ґабора використовується в обробці зображень через їх біологічну значимість та технічні властивості. Вейвлети Ґабора мають форму, подібну до рецептивних полів простих клітин первинної зорової кори, отже представлення зображень засноване на принципах представлення зображень в людському мозку.

Альтернативою є функція лог-Ґабора, запропонована Філдом [81]. Фільтри лог-Ґабора мають довільну пропускну здатність, а їхня смуга пропускання оптимізується для мінімізації просторової міри. Вейвлет-перетворення лог-Ґабора зберігає математичні властивості функцій Ґабора, забезпечуючи точну реконструкцію сигналу. Порівняно з іншими методами, лог-Ґабор-вейвлети ефективно відокремлюють корисну інформацію від некогерентного ґауссівського шуму завдяки жорсткому порогу та здатності кодувати елементи зображення з мінімальним числом значущих коефіцієнтів.

З огляду на те, що кожен з розглянутих методів вейвлет-перетворення має свої переваги та недоліки, необхідним є подальше проведення порівняльного аналізу методів обробки зображень на основі вейвлет-перетворення.

Одним з ключових етапів процесу біометричної ідентифікації є вилучення вектору ознак, що відображає індивідуальні особливості обличчя. За допомогою

спеціалізованих методів, зображення перетворюється на вектор ознак – компактне числове представлення, придатне для подальшої класифікації. Якість цього представлення безпосередньо впливає на точність розпізнавання.

Методи двовимірного розпізнавання облич класифікуються за підходом до вилучення ознак на чотири групи: холістичні, локальні (геометричні), методи на основі локально-текстурних дескрипторів і глибокого навчання [27]. Локально-текстурні методи є ключовими для комп'ютерного зору та класифікації зображень, забезпечуючи високу швидкість аналізу, розпізнавання та інваріантність до масштабу й зміщення. Вони стійкі до змін градації сірого, освітлення та яскравості й не потребують сегментації. На відміну від глобальних дескрипторів, що аналізують зображення загалом, локальні дескриптори описують окремі фрагменти, що підвищує їхню ефективність у варіативних умовах.

У роботі [82] проведено дослідження та порівняння локально-текстурних дескрипторів для розпізнавання виразу обличчя. Ефективність методів оцінювалася на стандартних наборах даних, що містять зображення з різними умовами освітлення, позами та виразами обличчя. Встановлено, що локально-текстурні дескриптори шаблонів є стійкими до випадкового шуму, змін пози, віку та виразу обличчя. Результати експерименту підтвердили їхню високу ефективність у задачах розпізнавання облич.

Згідно з дослідженням [83], метод локальних бінарних шаблонів (LBP) є одним із найефективніших для розпізнавання облич. У роботі проаналізовано LBP та чотири похідні дескриптори з метою оцінки їх продуктивності. Встановлено, що ефективність цих методів знижується в середньому на 40% при застосуванні до зображень із шумами.

У дослідженні [84] проаналізовано 18 локально-текстурних дескрипторів, застосованих окремо та в комбінації до різних наборів зображень облич. Експериментальні результати підтвердили, що поєднання кількох дескрипторів суттєво підвищує ефективність розпізнавання облич.

У статті [85] проаналізовано підхід до комбінування гістограм орієнтованих градієнтів (HOG) і локальних бінарних шаблонів (LBP) для розпізнавання облич.

Автори зазначають, що поєднання дескрипторів HOG із LBP дозволяє ефективніше виділяти структурні особливості зображення. Експериментальні результати показали, що застосування комбінованих дескрипторів підвищує точність класифікації в середньому на 8%, що підтверджує перевагу комплексного підходу над використанням окремих дескрипторів.

У статті [86] запропоновано комбінування гістограми орієнтованих градієнтів (HOG) та ортогональної комбінації локальних бінарних шаблонів (OC-LBP) — модифікації LBP, що зменшує розмірність дескриптора й підвищує його дискримінативну здатність. У ході експериментів дескриптори LBP, OC-LBP і HOG застосовувалися окремо та в поєднанні (OC-LBP + HOG) для вилучення ознак облич на зображеннях із трьох наборів даних. Результати показали, що комбінований підхід забезпечує вищу надійність порівняно з використанням окремих дескрипторів.

У дослідженні [87] проведено порівняльний аналіз методів вилучення ознак зображень, зокрема гістограм орієнтованих градієнтів (HOG), локальних бінарних шаблонів (LBP), методу головних компонент (PCA), прискорених стійких ознак (SURF) та ознак Гаара (Haar). За результатами експериментів алгоритм HOG продемонстрував найвищу ефективність з точністю розпізнавання 85%. Високих показників також досягнуто при використанні методу LBP і його комбінації з HOG.

У статті [88] запропоновано алгоритм розпізнавання обличчя, що поєднує метод центросиметричних локальних бінарних шаблонів із середньо-зваженими околицями (CS-NWALBP) та гістограм об’єднаних градієнтів (HOG). Автори порівняли його з поширеними методами локально-текстурного аналізу. Результати дослідження показали, що алгоритм CS-NWALBP-HOG забезпечує найвищу точність розпізнавання серед розглянутих підходів.

У дослідженні [89] запропоновано алгоритм на основі локальних бінарних шаблонів і гістограм орієнтованих градієнтів (LBPH) для біометричної системи контролю відвідуваності. Його ефективність порівняно з методами Eigenface і Fisherface. Результати показали, що LBPH значно перевершує традиційні підходи до розпізнавання облич.

У статті [55] запропоновано локально-текстурний дескриптор 1DLBP для автоматизованої ідентифікації особи, що базується на методі локальних бінарних шаблонів (LBP) та відображає двовимірне зображення в одновимірний простір. LBP вирізняється стійкістю до змін освітлення й обертання, а також низькою обчислювальною складністю, проте має обмеження через великий розмір вектора ознак і відсутність глобальної інформації. Дескриптор 1DLBP усуває цей недолік, поєднуючи локальні та глобальні особливості зображення обличчя. Експериментальне порівняння показало, що точність розпізнавання для LBP становить 85.2%–94.3%, а для 1DLBP – 92%–98.3%. Коефіцієнти помилково позитивного розпізнавання: для LBP – 3.1%–3.62%, для 1DLBP – 1.1%–2.36%. У порівнянні з класичними алгоритмами 1DLBP показав найвищу точність: PCA – 83.1%, LDA – 83.6%, POEM – 90.2%, LGBP – 93.6%, 1DLBP – 97.2%. Отже, 1DLBP демонструє вищу продуктивність порівняно з традиційними підходами.

У дослідженні [27] проведено аналіз і порівняння сучасних алгоритмів розпізнавання облич на основі глибинного навчання. Оцінювання здійснювалося за показниками точності на наборі даних LFW із використанням нейромережевих архітектур CNN, VGGNet, GoogleNet, LeNet, ResNet тощо. Загальна точність розпізнавання варіюється від 97.35% до 99.86%. Встановлено, що глибокі згорткові нейронні мережі забезпечують вищу точність порівняно з холістичним, геометричним і локально-текстурним підходами завдяки здатності виявляти дискримінаційні ознаки на великих наборах даних. Водночас ефективне навчання таких моделей потребує значних обчислювальних ресурсів і великих обсягів високоякісних даних.

У статті [90] описано порівняння алгоритму LBPH з нейромережею CNN на основі літературних даних. Встановлено, що LBPH є більш стійким до поворотів голови, тоді як точність CNN може знижуватися до 37.5% за аналогічних умов. Також зазначено, що нейромережеві методи вимагають значних обсягів навчальних даних, що ускладнює їх використання без ефективних механізмів збору даних.

У роботі [91] проаналізовано ефективність локально-текстурних дескрипторів (LBP, HOG) та згорткової нейронної мережі (CNN) для виявлення та

розпізнавання облич. Встановлено, що LBP і HOG забезпечують вищу швидкість розпізнавання, тоді як CNN потребує більше часу на обробку. Водночас, зі збільшенням складності зображень усі методи демонстрували подібний рівень точності.

У статті [92] запропоновано два методи: LCMoG-CNN, який використовує неглибоку згорткову нейронну мережу (CNN) для проєктування коваріаційних матриць вейвлетів Ґабора у вектор ознак, та LCMoG-LWPZ, що застосовує матрицю-логарифм і аналіз головних компонент із відбілюванням (WPCA) для вилучення рис обличчя. Точність цих методів порівнювалася з поширеними алгоритмами на основі локально-текстурних дескрипторів і нейромереж. Дослідження показало, що вейвлет-перетворення Ґабора та LBP ефективні для вилучення детальних рис, тоді як нейромережеві підходи демонструють високу надійність за складних умов, але вимагають значних обчислювальних ресурсів та великого обсягу навчальних даних.

Таким чином, методи розпізнавання обличчя на основі нейронних мереж демонструють високі показники точності розпізнавання, стійкість до варіацій пози, орієнтації, часткової оклюзії, зміщення та виразів обличчя. Проте використання таких методів не є ефективним для задач розпізнавання обличчя на низькоякісних зображеннях або в умовах, коли у базі даних існує лише одне зображення обличчя на людину, оскільки навчання нейронних мереж потребує великомасштабних високоякісних навчальних даних.

У статті [93] запропоновано комплексний метод вилучення ознак, що поєднує вейвлет-декомпозицію Гаара з методами BSIF (бінаризовані статистичні ознаки зображення) та HOG (гістограми орієнтованих градієнтів). Дослідження спрямоване на вилучення ознак відбитків долоні. На основі отриманих результатів у цьому дисертаційному дослідженні вирішено застосувати подібну комбінацію методів для біометричної ідентифікації за зображенням обличчя.

На основі проведеного аналізу локально-текстурних дескрипторів та їх порівняння з методами штучного інтелекту для проведення подальших досліджень обрано дескриптори локальних бінарних шаблонів в одновимірному просторі

(1DLBP) та гістограм орієнтованих градієнтів (HOG). Основна ідея підходу полягає у застосуванні цих дескрипторів до вейвлет-перетворених зображень з метою ефективного вилучення ключових ознак обличчя. Далі розглянемо методи 1DLBP і HOG детальніше.

Метод LBP, запропонований у [94], використовується для аналізу текстури, демонструючи високу стійкість до змін кута огляду та освітлення. Він кодує значення кожного пікселя вікна 3×3 у двійкову форму на основі його оточення. Проте маска 3×3 не враховує великі текстурні структури. Для подолання цього обмеження запропоновано модифікації з розширеними масками. В роботі [95] представлено дескриптор 1DLBP, що усуває цей недолік та адаптує LBP для розпізнавання облич, використовуючи його одновимірну версію.

Форма зображення кодується у гістограмах границь об’єктів, що знаходяться в піддіапазонах зображень після вейвлет-перетворення. Метод HOG застосовується до таких зображень для виділення ознак форми, де кожен інтервал гістограми відображає кількість границь із певною орієнтацією. Об’єднання гістограм усіх піддіапазонів дозволяє сформувати дескриптор HOG, який містить інформацію про текстуру та форму, необхідну для реконструкції вихідного зображення. Використання спрямованого двійкового коду та вейвлет-перетворення Гаара покращує високочастотні характеристики, зокрема деталізацію границь.

Враховуючи результати аналізу досліджень локально-текстурних дескрипторів, необхідним є дослідження як окремого використання кожного з обраних методів у процесі біометричної ідентифікації, так і використання цих методів у комбінації.

Завершальним етапом процесу біометричної ідентифікації є класифікація вектору ознак зображення. Для цього використовуються методи, які порівнюють вхідний вектор із шаблонами в базі даних, визначаючи ступінь відповідності. Для вирішення проблеми класифікації векторів ознак зображень обличчя зазвичай використовуються ті самі підходи, що і для автоматичної класифікації даних у галузі інтелектуального аналізу даних, де використовуються принципи групування

даних у класи таким чином, щоб дані одного класу були якомога подібнішими, а класи – якомога більш відмінними один від одного.

Для класифікації векторів ознак у методах розпізнавання та ідентифікації використовуються підходи, що належать до двох категорій [96]. Перша категорія – це підходи до порівняння векторів ознак, які ґрунтуються на обчисленні відстаней між векторами ознак, які потрібно класифікувати, та векторами, які зберігаються в базі даних. Такі підходи зазвичай використовують метричні відстані – математичний спосіб вимірювати відстань між двома векторами у векторному просторі. У такому випадку межі розрізнення між класами векторів визначаються на етапі ідентифікації.

До другої категорії належать підходи, які спочатку використовуються на етапі реєстрації суб'єкта в базі даних шляхом контрольованого навчання класифікатора для того, щоб апріорно визначити межі розрізнення між класами векторів ознак, що містяться в базі даних. Повторно такі методи застосовуються на етапі ідентифікації, щоб визначити клас суб'єкта, якого необхідно ідентифікувати. До даної категорії належать методи на основі нейронних мереж та метод опорних векторів.

Якщо порівнювати наведені методи класифікації векторів ознак, то з точки зору точності класифікації методи на основі нейронних мереж та опорних векторів є більш ефективними, ніж метричні відстані. Порівнюючи за швидкістю класифікації, слід зазначити, що метричні відстані виконують класифікацію за менший проміжок часу. Тим не менш, методи класифікації на основі нейронних мереж та опорних векторів характеризуються серйозним недоліком, який виникає під час реєстрації в базі даних нової особи. У цьому випадку дані підходи, на відміну від метричних відстаней, вимагають повторення всього процесу навчання. Методами метричних відстаней класифікація здійснюється без повторного проходження етапу навчання. Таким чином, для розробки комплексного методу біометричної ідентифікації за зображенням обличчя вирішено використати саме метричні відстані для класифікації векторів ознак зображень обличчя.

Отже, метричні відстані використовуються, коли потрібно порівняти два вектори ознак, отримані в результаті етапу вилучення ознак із зображення, шляхом

обчислення ступеня розбіжності між цими двома векторами. Існує декілька найбільш поширених методів обчислення метричної відстані, які демонструють різну ефективність при їх застосуванні до різного типу задач. Тому доцільним є здійснення порівняльного аналізу таких методів.

1.5 Постановка завдання

Сучасні програмні рішення біометричної ідентифікації за зображенням обличчя стикаються з низкою критичних викликів, враховуючи які необхідне проведення ґрунтовного дослідження методів, що покладені в основі ідентифікаційного процесу.

Основні технології розпізнавання облич наразі базуються на методах штучного інтелекту, зокрема на нейронних мережах. Однак такі підходи мають обмежену гнучкість і не можуть швидко адаптуватися до змінних умов реального світу, оскільки потребують великої кількості якісних даних для навчання, вдосконалення обладнання та значних витрат на обслуговування, як зазначено в [27, 90, 92]. Крім того, дослідження [51] і [52] показують, що методи розпізнавання облич на основі нейронних мереж можуть бути скомпрометовані через атаки, коли зловмисники маніпулюють навчанням або розгортанням нейромережі для впровадження зловмисної поведінки, порушуючи цілісність системи.

У сучасних дослідженнях недостатньо уваги приділяється використанню локально-текстурних дескрипторів у завданнях розпізнавання облич. Такі методи, на відміну від нейронних мереж, не вимагають великої кількості даних, високої обчислювальної потужності обладнання та тривалого часу на навчання. Оскільки локально-текстурні методи не потребують навчання, їх неможливо скомпрометувати через маніпуляції з навчальними даними або розгортанням нейромережі. Більше того, на зображеннях, отриманих у неконтрольованих умовах, ефективність таких методів майже дорівнює ефективності методів штучного інтелекту, а в деяких контрольованих умовах навіть перевищує її [90, 91]. Таким чином, методи, що базуються на локально-текстурних дескрипторах, потребують подальших досліджень та вдосконалення.

Відповідно, завданням даної дисертаційної роботи є розробка комплексного методу біометричної ідентифікації за зображенням обличчя, що базується на локально-текстурних дескрипторах, та дослідженні розробленого комплексного методу з метою підвищення ефективності процесу біометричної ідентифікації. Реалізація поставленого завдання вимагає вирішення ряду важливих задач, таких як здійснення вибору методів детектування обличчя на зображенні, попередньої обробки зображення обличчя, обробки зображення, вилучення векторів ознак із зображення обличчя, обчислення відстані між векторами ознак; опис математичного забезпечення біометричної ідентифікації за зображенням обличчя у вигляді комплексного методу, що охоплює всі етапи ідентифікаційного процесу, та підбір параметрів методу, що лежать в основі комплексного методу біометричної ідентифікації; проєктування та реалізація програмного забезпечення біометричної ідентифікації на основі розробленого комплексного методу; визначення вимог до інформаційного та технічного забезпечення процесу біометричної ідентифікації; проведення експериментального дослідження розробленого комплексного методу біометричної ідентифікації; оцінка результатів експериментів і порівняльний аналіз результатів дослідження з роботами інших дослідників.

Висновки до розділу 1

У першому розділі представлено огляд програмних рішень задачі біометричної ідентифікації, у ході якого отримано такі результати:

1. Здійснено аналіз програмних рішень біометричної ідентифікації, за результатами якого встановлено, що така біометрична ознака, як обличчя, має ряд переваг, серед яких неінвазивність і висока прийнятність користувачами.

2. Проведено огляд сучасних досліджень у сфері розпізнавання облич, встановлено, що різниця в якості еталонних та тестових зображень є однією з основних причин помилок у процесі ідентифікації. Визначено необхідність дослідження можливості підвищення ефективності програмних засобів біометричної ідентифікації шляхом зміни властивостей зображень, які вони обробляють.

3. Здійснено аналіз проблем, пов’язаних із розпізнаванням обличчя. Результати аналізу свідчать про значну кількість викликів, що потребують подальших досліджень, ключовими з яких є проблеми, пов’язані з оклюзією, неоднорідністю зображень облич, процесом старіння, розпізнаванням за єдиним зразком та у відеопотоці.

4. Досліджено процес біометричної ідентифікації та методи, покладені в його основу. Визначено необхідність проведення досліджень для вибору методів попередньої обробки зображень, вилучення векторів ознак та обчислення відстані між ними.

5. Поставлено завдання дисертаційного дослідження, що полягає у розробці комплексного методу біометричної ідентифікації на основі локально-текстурних дескрипторів та дослідженні розробленого комплексного методу з метою підвищення ефективності процесу біометричної ідентифікації.

РОЗДІЛ 2. МАТЕМАТИЧНЕ ПІДҐРУНТЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

2.1 Обґрунтування вибору методів розв'язання задачі біометричної ідентифікації

Розв'язання задачі біометричної ідентифікації передбачає формування ефективного математичного та алгоритмічного забезпечення, яке охоплює повний цикл обробки зображення – від вхідного кадру до класифікаційного рішення. Ключовим етапом цього процесу є вибір методів, що використовуються на кожній стадії обробки даних.

З метою формування обґрунтованого вибору методів детектування обличчя, попередньої обробки, обробки зображень, вилучення векторів ознак та обчислення відстаней між векторами, здійснимо порівняльний аналіз відповідних підходів. Цей аналіз базується на результатах огляду літературних джерел, представлених у Розділі 1, а також на експериментальних дослідженнях із використанням набору даних The Database of Faces.

Для забезпечення об'єктивного порівняння методів сформовано тестову вибірку зі 120 зображень облич та еталонну вибірку з 40 зображень, що належать 40 різним суб'єктам. Зображення варіювалися за рядом характеристик, зокрема розміром, умовами освітлення, положенням голови, виразом обличчя, а також відстанню до камери, що дозволяє оцінити ефективність методів в умовах різноманітних характеристик вхідних даних.

Вибір методу попередньої обробки зображень здійснено на основі порівняльного аналізу результатів застосування до зображень облич методів анізотропної дифузії та вирівнювання гістограми, як окремо кожного, так і в комбінації. Крім того, методи застосовувалися як до зображень з чітко видимими рисами обличчя (неоклюзивних), так і до зображень з неповністю видимими рисами (оклюзивних). Результати цих досліджень наведені на Рисунку 2.5.

У результаті експерименту отримано показник точності ідентифікації 92,5% при застосуванні методу анізотропної дифузії та 90% при застосування методу

вирівнювання гістограми та комбінації методів одночасно. Різниця результатів складає 2,5%, що не є досить переконливим результатом для того, аби надати перевагу одному з розглянутих методів. Тому вирішено провести експерименти в більш складних умовах, а саме за наявності оклюзії на зображеннях. У результаті найвищий показник точності ідентифікації, що складає 82,5%, отримано при застосуванні методу анізотропної дифузії. Отриманий показник перевищує результати застосування комбінації методів і методу вирівнювання гістограми окремо на 10% і 12,5% відповідно. Результати описаних експериментів наведені у Таблиці 2.1.

Таблиця 2.1 – Результати порівняльного аналізу методів попередньої обробки зображень облич

Метод попередньої обробки	Всього зображень / суб'єктів	Показник ідентифікації		Кількість ідентифікованих суб'єктів	
		Точність	Помилка	Коректно	Некоректно
Неоклюзивні зображення					
Анізотропна дифузія	160 / 40	92,5%	7,5%	37	3
Вирівнювання гістограми		90%	10%	36	4
Комбінація методів		90%	10%	36	4
Оклюзивні зображення					
Анізотропна дифузія	160 / 40	82,5%	17,5%	33	7
Вирівнювання гістограми		70%	30%	28	12
Комбінація методів		72,5%	27,5%	29	11

Згідно з отриманими результатами метод анізотропної дифузії є більш ефективним в складних умовах ідентифікації, таких як наявність оклюзії на зображеннях, що надає йому перевагу для подальшого використання у комплексному методі біометричної ідентифікації.

Вибір методу обробки зображень облич виконувався на основі порівняльного аналізу результатів експериментального дослідження із застосуванням до зображень облич методів вейвлет-перетворень, розглянутих у Розділі 1. Оскільки деякі вейвлети характеризуються чутливістю до зсувів та мають обмежену селективність орієнтації, для проведення даного дослідження окремо сформовано вибірки статичних (фронтальні зображення без варіації виразів обличчя) і динамічних (змінні вирази облич і положення голови суб'єкта ідентифікації) зображень. Крім того, методи застосовувалися як до зображень з чітко видимими рисами обличчя, так і до зображень з неповністю видимими рисами.

При застосуванні до статичних зображень найвищий показник точності ідентифікації 97,5% отримано під час проведення експерименту із використанням зворотніх біортогональних вейвлетів. Оскільки класу біортогональних вейвлетів властивий такий недолік як погана селективність орієнтації, відповідно ефективність зворотніх біортогональних знизилася до 62,5% при застосуванні до динамічних зображень та 75% при застосуванні до оклюзивних зображень. Крім того при використанні біортогональних вейвлетів отримано показники точності 85% при застосуванні до статичних зображень, 62,5% – до динамічних зображень і 60% – до оклюзивних зображень.

При застосуванні до статичних зображень фільтрів Добеші отримано точність ідентифікації 92,5%. Проте вейвлети Добеші не мають вбудованої інваріантності до зсуву, що означає, що невеликі зміни в вхідному зображенні можуть призвести до значних змін у коефіцієнтах вейвлету. Відповідно ефективність даного методу знизилася при застосуванні до динамічних зображень до 77,5% та при застосування до оклюзивних зображень до 72,5%. При використання похідних від фільтрів Добеші методів койфлетів і симлетів отримано низькі результати точності від 57,5% до 67,5% при застосуванні до всіх вибірок зображень.

Під час використання фільтрів лог-Ґабора також отримано результат у 92,5% при застосуванні до статичних зображень, проте ефективність методу також значно знизилася при застосуванні до динамічних і оклюзивних зображень, становлячи 72,5% і 70% відповідно. Крім того, процес обробки зображень фільтрами лог-

Ґабора може бути обчислювально складним завданням, особливо при обробці великої кількості зображень, що обмежує можливість використання методів на основі цих вейвлетів у застосунках, що працюють в реальному часі. Фільтри лог-Ґабора можуть виділяти текстурні особливості, але у деяких випадках вони можуть викликати перекриття текстур, що робить важчим розрізнення між об’єктами на зображенні.

Показник точності ідентифікації у 87,5%, отримано під час застосування фільтрів Ґабора до статичних зображень, 82,5% – до динамічних зображень і 77,5% – до оклюзивних зображень. Порівнюючи з результатами вищезгаданих методів, ефективність фільтрів Ґабора при застосуванні до динамічних і оклюзивних зображень є найвищою серед результатів усіх експериментів. Крім того, вейвлети Ґабора мають властивості інваріантності до зміни масштабу та орієнтації, що робить їх найбільш придатними для роботи з обличчями під різними ракурсами і в різних масштабах. Вейвлети Ґабора мають здатність відображати як низькочастотні, так і високочастотні компоненти, що дозволяє отримувати більш детальний набір ознак обличчя для подальшого аналізу та розпізнавання. Враховуючи переваги фільтрів Ґабора та його високу ефективність при застосуванні до зображень з варіацією виразів обличчя та положення голови суб’єкта, вирішено використовувати саме цей метод обробки зображень для подальшої роботи.

З метою встановлення найбільш ефективної комбінації методів проведено експериментальне дослідження з використанням одного методу вилучення ознак (HOG або 1DLBP) і використанням комбінації методів вилучення ознак (HOG і 1DLBP) у поєднанні з раніше обраними методами виявлення обличчя на зображенні, попередньої обробки та обробки зображення обличчя. Експерименти проводилися з використанням набору даних The Database of Faces, який представлений зображеннями облич 40 різних суб’єктів. Результати експериментів представлені в Таблиці 2.2.

Таблиця 2.2 – Результати експериментального дослідження методів вилучення ознак на зображеннях з набору даних The Database of Faces

	HOG		1DLBP		HOG + 1DLBP	
	Точність	Помилка	Точність	Помилка	Точність	Помилка
Всього суб'єктів	40		40		40	
Кількість суб'єктів	26	14	17	23	28	12
Показник ідентифікації	65%	35%	42,5%	57,5%	70%	30%

З порівняльної діаграми результатів на Рисунку 2.1 випливає, що при використанні лише одного методу вилучення ознак, окремо HOG або 1DLBP, відсоток коректно ідентифікованих зображень коливається від 42,5% до 65%. Найвищий показник точності ідентифікації 70% отримано при застосуванні комбінації методів вилучення векторів ознак 1DLBP і HOG. Це підтверджує доцільність одночасного використання двох методів вилучення ознак при застосуванні комплексного методу біометричної ідентифікації.

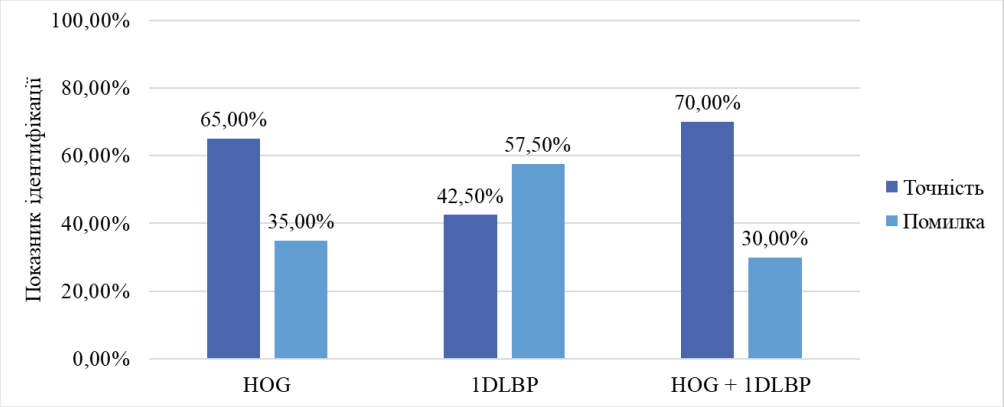


Рисунок 2.1 – Порівняльна діаграма результатів ідентифікації із застосуванням методів вилучення ознак до зображень з набору даних The Database of Faces

Отже, поєднання методів локальних бінарних шаблонів в одновимірному просторі та гістограм орієнтованих градієнтів демонструє найвищі результати точності ідентифікації, відповідно комбінацію цих методів обрано для подальшого використання.

У процесі вибору методів обчислення відстані між векторами ознак використано наступні метричні відстані: Брея-Кертіса, Канберра, Чебишева, Мангеттенську, кореляційну, косинусну, Евкліда, Дженсена-Шеннона, Міньковського, квадратичну Евкліда.

Після проведення експериментів для порівняльного аналізу метрик обчислення відстані між векторами ознак зображень отримано показники точності ідентифікації для кожної з метрик, наведені на Рисунку 2.2.

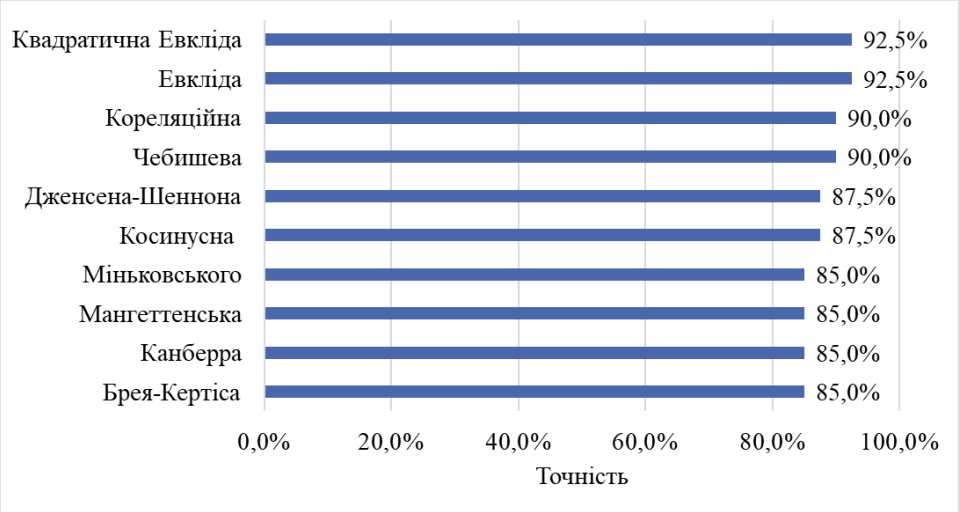


Рисунок 2.2 – Порівняльна діаграма результатів аналізу методів класифікації векторів ознак зображень облич

За результатами експериментального дослідження встановлено, що для класу задач, поставлених в даній роботі, найбільш ефективним є використання метрики обчислення відстані Евкліда та квадратичної відстані Евкліда. Обираючи між цими двома метриками, необхідно враховувати, що квадратична евклідова відстань обчислюється без використання операції визначення квадратного кореня із числа, яка є обчислювально витратною операцією, а визначається простою сумою квадратів відстаней. Тому для класифікації векторів ознак зображень облич в процесі біометричної ідентифікації вирішено використовувати квадратичну відстань Евкліда.

2.2 Математичне забезпечення для програмного рішення біометричної ідентифікації

Формування ефективного рішення задачі біометричної ідентифікації потребує комплексного математичного забезпечення, що охоплює весь процес обробки зображення – від моменту надходження вхідного зображення до прийняття рішення про ідентичність особи, обличчя якої зафіксоване на зображенні. Успішна реалізація такого рішення залежить від правильного вибору математичного підґрунтя виконання кожного з етапів ідентифікаційного процесу: виявлення обличчя, попередньої обробки зображення, обробки зображення, вилучення векторів ознак та здійснення класифікації.

На основі проведеного в підрозділі 2.1 аналізу обґрунтовано вибір методів, які є найбільш ефективними в умовах розв'язання задачі біометричної ідентифікації за зображенням обличчя. Зокрема, обрано метод Віола–Джонса на основі каскадів Гаара для виявлення обличчя, метод анізотропної дифузії для попередньої обробки зображення, метод вейвлет-перетворення Ґабора для обробки зображення, методи локальних бінарних шаблонів в одновимірному просторі (1DLBP) та гістограм орієнтованих градієнтів (HOG) для вилучення векторів ознак із зображення та метрику квадратичної відстані Евкліда для класифікації векторів ознак. Розглянемо математичний апарат виконання кожного з цих методів.

За результатами порівняльного аналізу методів виявлення обличчя на зображеннях обрано метод Віола–Джонса на основі каскадної структури ознак Гаара. Розглянемо алгоритм виконання даного методу:

1. На вхід методу подається зображення I, на якому необхідно ідентифікувати особу.

2. Перетворення зображення у відтінки сірого. Для зменшення обчислювальної складності та забезпечення коректного обчислення ознак Гаара, вхідне зображення I перетворюється у відтінки сірого, у результаті чого формується матриця яскравостей зображення у відтінках сірого. Значення елементу матриці яскравостей зображення I_g з індексами (i, j) обчислюється за формулою:

$$I_g(i,j) = 0.299 \cdot R(i,j) + 0.587 \cdot G(i,j) + 0.114 \cdot B(i,j), \quad (2.1)$$

де *R(i, j)*, *G(i, j)* і *B(i, j)* – значення червоної, зеленої та синьої компонент пікселя зображення *I* з індексами *(i, j)*.

3. Визначення параметрів методу. Для коректної роботи методу визначаються значення таких параметрів: τ – порогове значення, що використовується для прийняття рішення про наявність обличчя у заданій області зображення; ω – параметр, який визначає мінімальну кількість суміжних областей матриці зображення, віднесених до класу областей, що містять риси одного обличчя, щоб область матриці зображення, яка перевіряється, була визначена такою, що містить риси цього ж обличчя; $(\alpha_{min}, \beta_{min})$ – мінімальний розмір вікна сканування зображення. Мінімальний розмір вікна $(\alpha_{min}, \beta_{min})$, що забезпечує достатню деталізацію для розпізнавання ознак обличчя, становить 24×24 пікселі [97].

4. Обчислення матриці інтегрального зображення. Інтегральне зображення – це перетворене зображення, в якому кожен піксель має значення, яке визначається шляхом обчислення суми значень всіх пікселів в області, що починається з верхнього лівого кута до поточного пікселя зображення, поданого на вхід алгоритму. Позначимо матрицю інтегрального зображення як I_{int}. Значення елементів матриці інтегрального зображення I_{int} з індексами (i, j) обчислюється за рекурентною формулою:

$$I_{int}(i,j) = I_g(i,j) + I_{int}(i-1,j) + I_{int}(i,j-1) - I_{int}(i-1,j-1), \quad (2.2)$$

де $I_g(i, j)$ – значення елемента матриці яскравостей I_g зображення з індексами (i, j).

5. Обчислення значень каскаду класифікаторів на основі ознак Гаара. Каскад класифікаторів утворюється з послідовності окремих класифікаторів, кожен із яких перевіряє певну область матриці яскравостей зображення на наявність ознак обличчя. На ранніх етапах класифікатори можуть відсіювати області, які не містять ознак обличчя, що зменшує обсяг подальших обчислень. У процесі перевірки класифікатори використовують ознаки Гаара – фільтри розміру (α, β), що складаються зі світлих і темних прямокутних областей та обчислюють різницю яскравостей між ділянками матриці зображення, що підпадають під ці області [67].

Матриця інтегрального зображення сканується ковзним вікном розміру *(α, β)*, в якому обчислюються значення послідовності ознак Гаара. Початкові значення *(α, β)* визначаються як відношення ширини та висоти вхідного зображення до параметра *ω*. Позначимо розміри прямокутних областей ознаки Гаара як $\alpha'_u \times \beta'_u$, де *u* – індекс прямокутної області в загальній послідовності *u = [1, 2, ..., U]*, а *U* – кількість прямокутних областей, при цьому сума площ прямокутних областей дорівнює розміру ковзного вікна ознаки Гаара *(α, β)* [67]:

$$\sum_{u=1}^{U} (\alpha'_u \times \beta'_u) = \alpha \times \beta. \quad (2.3)$$

Значення Гаара Ω_a для окремої прямокутної області розміру $\alpha' \times \beta'$, індекси лівого верхнього кута якої позначаються як *(i', j')*, що відповідає елементу $I_{int}(i', j')$ матриці інтегрального зображення I_{int} з індексами *(i', j')*, обчислюється за формулою:

$$\Omega_a = I_{int}(i' + \alpha', j' + \beta') - I_{int}(i', j' + \beta') - I_{int}(i' + \alpha', j') + I_{int}(i', j'), \quad (2.4)$$

де $I_{int}(i' + \alpha', j' + \beta')$, $I_{int}(i', j' + \beta')$, $I_{int}(i' + \alpha', j')$, $I_{int}(i', j')$ – елементи матриці інтегрального зображення I_{int} з індексами $(i' + \alpha', j' + \beta')$, $(i', j' + \beta')$, $(i' + \alpha', j')$, (i', j').

Окремо обчислюються значення для світлих Ω_{aw} і темних Ω_{ad} прямокутних областей ознак Гаара. Результуюче значення ознаки Гаара Ω обчислюється як різниця суми значень елементів матриці інтегрального зображення I_{int} в прямокутних світлих і темних областях ознак Гаара:

$$\Omega = \Omega_{aw} - \Omega_{ad}. \quad (2.5)$$

Для кожної області розміру *(α, β)* матриці I_{int} обчислюються значення ознак Гаара $[\Omega_1, \Omega_2, ..., \Omega_\varphi]$, де *φ* – індекс ознаки в загальній послідовності $\varphi = [1, 2, ..., \Phi]$, а *Φ* – кількість ознак.

При цьому на кожному етапі каскаду класифікаторів обчислюється зважена сума *Ψ* значень ознак Гаара $[\Omega_1, \Omega_2, ..., \Omega_\varphi]$:

$$\Psi = \sum_{\varphi=1}^{\Phi} w_\varphi \cdot \Omega_\varphi, \quad (2.6)$$

де w_φ – ваги відповідних ознак, алгоритм обчислення яких наведено в дослідженні [97].

Якщо на певному етапі зважена сума значень ознак не перевищує порогове значення τ, тобто $\Psi < \tau$, обчислення для поточної області (α, β) матриці зображення припиняються, і вона класифікується як така, що не містить ознак обличчя. Якщо область зображення успішно проходить всі етапи каскаду, вона класифікується як така, що потенційно містить ознаки обличчя.

6. Формування загальної області матриці зображення, що містить обличчя. Позначимо множину областей матриці зображення, які були віднесені до класу областей, що потенційно містять ознаки обличчя, як $A = \{A_1, A_2, \ldots, A_l\}$, де l – індекс області в загальній послідовності $l = [1, 2, \ldots, L]$, а L – кількість областей. Для кожної області A_l з множини A визначається кількість її суміжних областей, які також належать до множини A. Позначимо множину таких суміжних областей як $Y_l = \{A_y \in A: A_l \cap A_y \neq \emptyset\}$. Якщо кількість суміжних до A_l областей, що віднесені до класу областей, які потенційно містять ознаки обличчя, тобто належать до множини Y_l, перевищує значення параметру ω, тобто $|Y_l| \geq \omega$, то область A_l утворює частину загальної матриці зображення, що містить обличчя. Таким чином перевіряються усі L областей множини A. Позначимо результуючу матрицю зображення, що містить лише область обличчя, як I_{Haar}. Матриця I_{Haar} утворюється шляхом об'єднання всіх областей, що віднесені до класу таких, що потенційно містять ознаки обличчя, та мають більше ω суміжних областей, що віднесені до того ж класу:

$$I_{Haar} = \bigcup_{A_l \in A:\, |Y_l| \geq \omega} A_l. \tag{2.7}$$

7. Масштабування вікна сканування. У випадку, якщо не вдалося сформувати матрицю I_{Haar}, а саме $I_{Haar} = \emptyset$, виконується масштабування розміру вікна сканування (α, β) пропорційно параметру s, після чого виконання кроків 5-6 алгоритму повторюється, доки не сформується матриця I_{Haar}. Якщо в результаті масштабування розміри вікна сканування сягнули мінімальних значень, а саме $(\alpha, \beta) \leq (\alpha_{min}, \beta_{min})$, і при жодній зі змін розміру вікна не вдалося сформувати матрицю I_{Haar}, виконується крок 8 алгоритму.

8. Масштабування зображення. У випадку, якщо не вдалося сформувати матрицю I_{Haar}, а саме $I_{Haar} = \emptyset$, при цьому $(\alpha, \beta) \leq (\alpha_{min}, \beta_{min})$, виконується масштабування матриці яскравостей зображення I_g пропорційно параметру s, після чого виконання кроків 4-7 алгоритму повторюється, доки не сформується матриця I_{Haar}. Якщо в результаті масштабування розміри зображення стали меншими за мінімальні значення вікна сканування $(\alpha_{min}, \beta_{min})$ і при жодній зі змін масштабів не вдалося сформувати матрицю I_{Haar}, то формується повідомлення про те, що обличчя на зображенні не виявлено.

За результатами експериментального дослідження методів попередньої обробки зображень обрано метод анізотропної дифузії. Розглянемо алгоритм виконання даного методу:

1. На вхід методу подається матриця яскравостей зображення обличчя I_{Haar}, отримана в результаті застосування класифікатору Гаара до вхідного зображення.

2. Визначення параметрів анізотропної дифузії. Для застосування методу анізотропної дифузії до матриці вхідного зображення необхідно визначити значення таких параметрів, як μ — кількість ітерацій застосування методу, κ — коефіцієнт провідності, η — швидкість дифузії.

3. Обчислення градієнтів яскравості. Значення градієнтів матриці яскравості зображення визначаються за допомогою односторонньої різницевої схеми, яка враховує значення сусіднього елемента матриці у напрямку обчислення. Зокрема, горизонтальний градієнт кожного елемента матриці обчислюється як різниця між його правим сусідом та самим елементом, а вертикальний градієнт — як різниця між нижнім сусідом та самим елементом. Позначимо градієнт яскравості у горизонтальному напрямку елемента вхідної матриці I_{Haar} з індексами (i, j) як $\delta_i(i, j)$, а градієнт у вертикальному напрямку – $\delta_j(i, j)$ [98]. Значення градієнтів яскравості обчислюються за такими формулами:

$$\delta_i(i,j) = I_{Haar}(i,j+1) - I_{Haar}(i,j), \quad (2.8)$$

$$\delta_j(i,j) = I_{Haar}(i+1,j) - I_{Haar}(i,j). \quad (2.9)$$

4. Обчислення градієнтів провідності. Градієнти провідності визначають зміну коефіцієнта провідності залежно від градієнта яскравості матриці

зображення. В однорідних областях матриці із низьким градієнтом яскравості провідність залишається високою, що сприяє інтенсивнішому згладжуванню. Натомість на межах об'єктів, де градієнт яскравості вищий, провідність зменшується, що запобігає розмиттю важливих деталей, таких як риси обличчя та текстурні особливості зображення. Градієнт провідності ρ елемента вхідної матриці I_{Haar} з індексами *(i, j)* обчислюється за формулою [99]:

$$\rho(i,j) = \exp\left(-\left(\frac{\delta_i(i,j)}{\kappa}\right)^2\right) + \exp\left(-\left(\frac{\delta_j(i,j)}{\kappa}\right)^2\right), \quad (2.10)$$

де $\delta_i(i, j)$ – градієнт яскравості елемента матриці I_{Haar} в горизонтальному напрямку, $\delta_j(i, j)$ – градієнт яскравості елемента матриці I_{Haar} у вертикальному напрямку, κ — коефіцієнт провідності.

5. Обчислення потоку дифузії. Потік дифузії описує, як змінюються значення яскравості елементів в різних напрямках матриці зображення в залежності від значень їхніх градієнтів. Оскільки метою застосування анізотропної дифузії є збереження контурів, на яких є різкі зміни в градієнті яскравості (наприклад, риси обличчя), потік дифузії буде малим на межах таких контурів і більшим в однорідних областях матриці зображення [100]. Потік дифузії $J(i, j)$ елемента матриці з індексами *(i, j)* обчислюється за формулою:

$$J(i,j) = \eta \cdot \rho(i,j), \quad (2.11)$$

де η – швидкість дифузії, $\rho(i, j)$ – градієнт провідності елемента матриці I_{Haar} з індексами *(i, j)*.

6. Обчислення значень елементів результуючої матриці. Позначимо матрицю, що формується в результаті застосування методу анізотропної дифузії до вхідної матриці I_{Haar}, як I_{AD}. Значення елемента результуючої матриці I_{AD} з індексами *(i, j)* обчислюється за формулою [101]:

$$I_{AD}(i,j) = I_{Haar}(i,j) + J(i,j), \quad (2.12)$$

де $I_{Haar}(i, j)$ – елемент вхідної матриці I_{Haar} з індексами *(i, j)*, $J(i, j)$ – значення потоку дифузії елемента матриці I_{Haar} з індексами *(i, j)*.

7. Оновлення параметру кількості ітерацій. Кроки 3-5 алгоритму повторюються протягом μ ітерацій, при цьому з кожною ітерацією значення μ зменшується на 1, доки не досягне 0.

За результатами експериментального дослідження методів обробки зображень обрано метод вейвлет-перетворення Ґабора. Розглянемо алгоритм виконання даного методу:

1. На вхід методу подається матриця I_{AD}, отримана в результаті попередньої обробки матриці зображення обличчя методом анізотропної дифузії.

2. Визначення параметрів фільтрів Ґабора. Для генерування фільтрів Ґабора необхідно визначити значення таких параметрів, як λ — довжина хвилі синусоїдальної складової, θ — орієнтація нормалі до паралельних смуг функції Ґабора в градусах, ψ — зсув фази синусоїдальної функції, σ — стандартне відхилення ядра Ґауса, γ — просторове співвідношення сторін, що визначає еліптичність носія функції Ґабора. На даному кроці алгоритму встановлюються початкові значення цих параметрів.

3. Генерування фільтрів Ґабора. Оптимальна формула для генерування фільтрів Ґабора повинна мати низьке значення постійної компоненти для мінімізації шуму, а також високу селективну здатність для більш чіткого виділення меж на перепадах яскравості [80]. Позначимо матрицю фільтру Ґабора як $Г$. Елементи $Г(i_Г, j_Г)$ матриці $Г$ з індексами $(i_Г, j_Г)$ обчислюються за формулою:

$$Г(i_Г, j_Г) = exp\left(-\frac{1}{2}\left[\frac{i_Г'^2 + \gamma^2 j_Г'^2}{\sigma^2}\right]\right)\cos(2\pi\frac{i_Г'}{\lambda} + \psi), \quad (2.13)$$

де $i_Г' = i_Г\cos\theta + j_Г\sin\theta$ та $j_Г' = -i_Г\sin\theta + j_Г\cos\theta$.

4. Застосування фільтрів Ґабора до вхідної матриці. На даному кроці алгоритму виконується згортка вхідної матриці I_{AD} з фільтрами Ґабора $[Г_1, Г_2, ..., Г_f]$, де f – індекс фільтру в загальній послідовності $f = [1, 2, ..., F]$, а F – кількість фільтрів. У результаті застосування фільтру до вхідної матриці утворюється результуюча матриця I_{Gabor}:

$$I_{Gabor} = I_{AD} * Г_f, \quad (2.14)$$

де * - операція згортки [102].

5. Формування вхідних даних для етапу вилучення векторів ознак. Результати застосування фільтрів Ґабора до вхідної матриці використовуються як вхідні дані для методів вилучення векторів ознак..

6. Оновлення параметрів фільтрів Ґабора. Набір з F фільтрів Ґабора Γ створюється шляхом варіювання значень параметрів фільтрів: довжини хвилі λ в діапазоні значень $[\Delta\lambda, \lambda_{max}]$ з кроком $\Delta\lambda$, орієнтації θ в діапазоні значень $[\Delta\theta, \theta_{max}]$ з кроком $\Delta\theta$ та стандартного відхилення σ в діапазоні значень $[\Delta\sigma, \sigma_{max}]$ з кроком $\Delta\sigma$ [103].

За результатами експериментального дослідження методів вилучення векторів ознак із зображень для подальшого використання обрано комбінацію методів локальних бінарних шаблонів в одновимірному просторі (1DLBP) та гістограм орієнтованих градієнтів (HOG). Розглянемо алгоритм виконання методу 1DLBP:

1. На вхід методу подається матриця зображення I_{Gabor}, отримана в результаті виконання методу вейвлет-перетворення Ґабора.

2. Декомпозиція матриці I_{Gabor} на N блоків B_k:

$$I_{Gabor} = \bigcup_{k=1}^{N} B_k, \tag{2.15}$$

де k – індекс блоку в загальній послідовності $k = [1, 2, ..., N]$, N – кількість блоків, B_k – блок декомпозованої вхідної матриці [55]. При цьому блоки не перетинаються, а $\bigcup_{k=1}^{N} B_k$ охоплює всю площу матриці I_{Gabor}.

3. Вертикальна проєкція кожного блоку матриці в одновимірний простір.

Для здійснення проєкції блоку B_k матриці в одновимірний простір спочатку виконується інверсія матриці яскравості блоку B_k. Позначимо яскравість пікселя з індексами (i, j) матриці блоку B_k як $B(i, j)$. Яскравість пікселя визначена у діапазоні [0, 255] яскравості у відтінках сірого. Інвертоване значення яскравості пікселя $B_{inv}(i, j)$ матриці інвертованих значень яскравості B_{inv} визначається таким чином:

$$B_{inv}(i, j) = 255 - B(i, j). \tag{2.16}$$

Далі обчислюється сума значень яскравостей пікселів уздовж рядків інвертованої матриці яскравостей блоку B_{inv} [55]. Сума яскравостей S_i в кожному i-му рядку визначається як:

$$S_i = \sum_{j=1}^{M} B_{inv}(i,j), \tag{2.17}$$

де j – індекс стовпців матриці в загальній послідовності $j = [1, 2, ..., M]$, а M – кількість стовпців інвертованої матриці яскравостей B_{inv} блоку B.

Зі значень сум яскравостей інвертованої матриці яскравостей B_{inv} формується вектор проєкції V_{pr}:

$$V_{pr} = (S_1, S_2, \dots, S_M) = \left(\sum_{j=1}^{M} B_{inv}(1,j), \sum_{j=1}^{M} B_{inv}(2,j), \dots, \sum_{j=1}^{M} B_{inv}(M,j) \right). \tag{2.18}$$

4. Застосування дескриптора 1DLBP до кожного вектора вертикальної проєкції блока. Для цього кожний елемент вектора проєкції V_{pr} порівнюється з 8 сусідніми значеннями. Усі сусіди отримують значення 1, якщо вони більші або рівні центральному елементу, і 0 в іншому випадку [95].

Нехай $V_{pr} = [v_1, v_2, ..., v_M]$, де M – кількість елементів у векторі. Поточний елемент вектора позначимо як v_p, де $p = [1, 2, ..., M]$. Для кожного елемента v_p розглядаємо 8 сусідів, позначених як v_{p-4}, v_{p-3}, v_{p-2}, v_{p-1}, v_{p+1}, v_{p+2}, v_{p+3}, v_{p+4}, де індекси, що виходять за межі $[1, M]$ обробляються циклічно, тобто $r = [-4, -3, -2, -1, 1, 2, 3, 4]$, а $v_{p+r} = v_{(p + r - 1) \bmod M+1}$. Поточний елемент v_p порівнюється із сусідами v_{p+r}, використовуючи функцію $C(x)$, яку можна описати так:

$$C(x) = \begin{cases} 1, v_{p+r} \geq v_p, \\ 0, v_{p+r} < v_p. \end{cases} \tag{2.19}$$

Результати порівняння утворюють $\vec{c}$ для елемента v_p, де $\vec{c} = [c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7]$, тобто $\vec{c}$ містить 8 елементів, які були отримані в результаті застосування функції $C(x)$ до кожного з 8 пікселів, сусідніх із v_p.

Далі формуються вагові коефіцієнти, що задаються як $w_n = 2^n$, де $n = [0, 1, ..., 7]$, і відповідають позиціям елементів $\vec{c}$ [95]. Окреме значення результуючого $\vec{E}$ обчислюється за формулою:

$$e = \sum_{n=0}^{7} c_n \cdot w_n. \quad (2.20)$$

Відповідно, дескриптор 1DLBP блоку матриці визначається результуючим вектором ознак $\vec{E}$, що має вигляд $\vec{E} = [e_1, e_2, \ldots, e_M]$, де M – кількість елементів у векторі, що дорівнює кількості стовпців у блоці B.

5. Формування вектору ознак 1DLBP.

Вектор ознак V_{1DLBP}, що є дескриптором 1DLBP матриці зображення, поданої на вхід алгоритму, формується таким чином:

$$V_{1DLBP} = [E_1, E_2, \ldots, E_N], \quad (2.21)$$

де N – кількість блоків вхідної матриці, утворених в результаті декомпозиції.

Схематичний приклад формування значення вектору ознак 1DLBP представлено на Рисунку 2.3.

Розглянемо алгоритм виконання методу HOG:

1. На вхід методу подається матриця зображення I_{Gabor}, отримана в результаті виконання методу вейвлет-перетворення Ґабора.

2. Обчислення градієнтів першого порядку. Градієнти першого порядку фіксують текстурну інформацію, забезпечуючи додаткову стійкість до варіацій освітлення. Значення градієнтів обчислюються за допомогою схеми центральної різниці, тобто для обчислення значення градієнта поточного пікселя матриці зображення враховуються значення обох його сусідніх пікселів (лівого та правого для обчислення горизонтального градієнта, верхнього та нижнього – вертикального градієнта) [85]. Позначимо градієнт у горизонтальному напрямку пікселя вхідної матриці I_{Gabor} з індексами (i, j) як $G_i(i, j)$, а градієнт у вертикальному напрямку – $G_j(i, j)$. Значення градієнтів обчислюються за такими формулами:

$$G_i(i,j) = |I_{Gabor}(i, j+1) - I_{Gabor}(i, j-1)|, \quad (2.22)$$

$$G_j(i,j) = |I_{Gabor}(i+1, j) - I_{Gabor}(i-1, j)|. \quad (2.23)$$

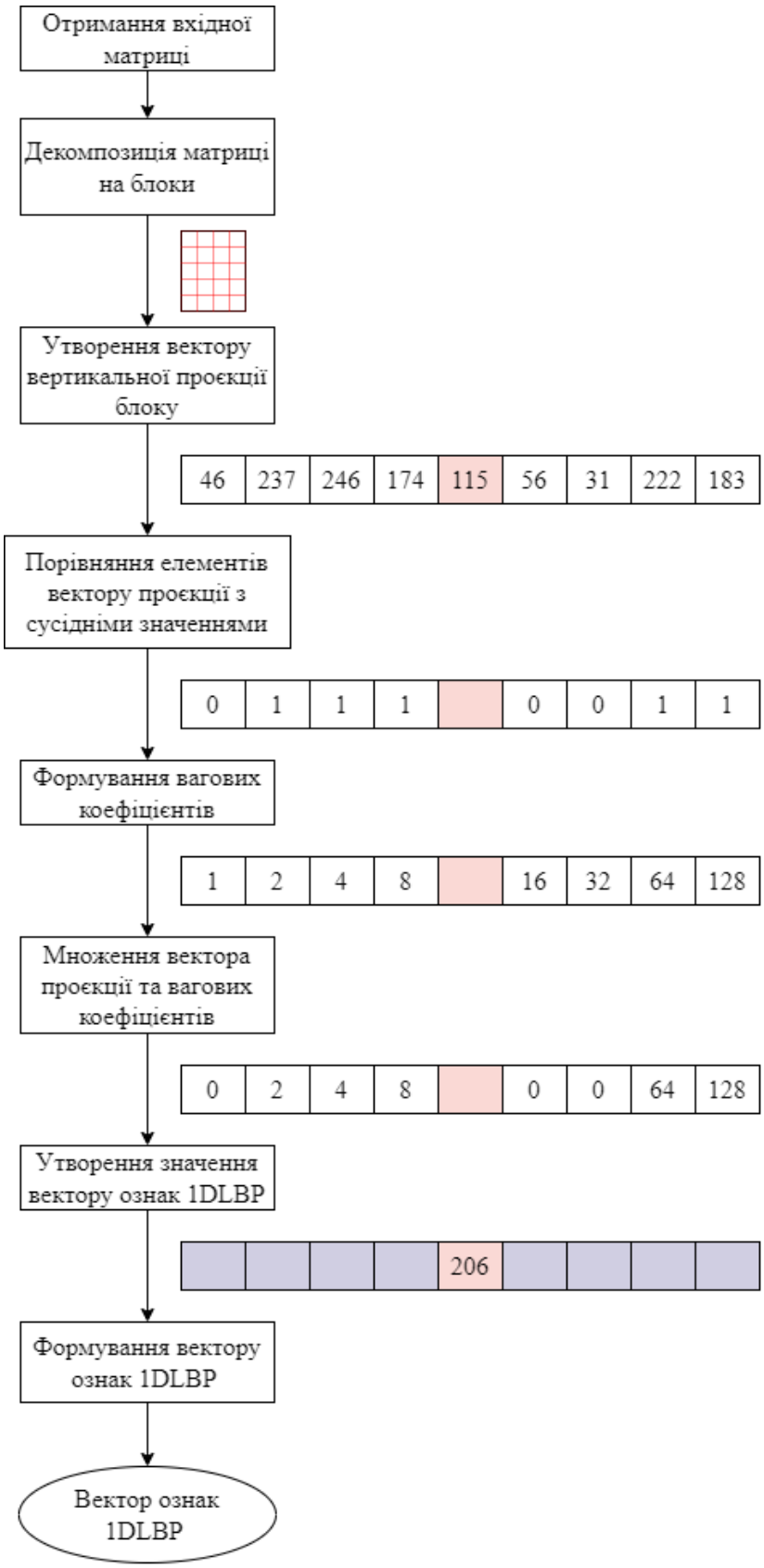


Рисунок 2.3 – Схематичний приклад формування значення результуючого вектору дескриптора локальних бінарних шаблонів в одновимірному просторі (1DLBP)

3. Обчислення величини та орієнтації градієнта.

Величина $m(i, j)$ та орієнтація $\theta(i, j)$ градієнта у пікселі з індексами (i, j) обчислюються за формулами:

$$m(i,j) = \sqrt{G_i^2(i,j) + G_j^2(i,j)}, \tag{2.24}$$

$$\theta(i,j) = arctg\left(\frac{G_j(i,j)}{G_i(i,j)}\right) \cdot \frac{180°}{\pi}\ mod\ 180°, \tag{2.25}$$

де $G_i(i, j)$ та $G_j(i, j)$ – значення градієнтів пікселя з індексами (i, j) у горизонтальному та вертикальному напрямках відповідно. $\theta(i, j)$ обмежується інтервалом [0, 180°), тобто у подальших обчисленнях використовується лише напрямок градієнта, незалежно від його знаку [86].

4. Розбиття вхідної матриці на комірки. Матриця I_{Gabor} розбивається на малі просторові області (комірки). Розбиття матриці I_{Gabor} на D комірок C_d описується формулою:

$$I_{Gabor} = \bigcup_{d=1}^{D} C_d, \tag{2.26}$$

де d – індекс комірки в загальній послідовності $d = [1, 2, ..., D]$, D – кількість комірок, C_d – комірка матриці, тобто частина вхідної матриці I_{Gabor}, утворена в результаті її розбиття.

5. Групування орієнтацій за інтервалами. Даний крок алгоритму спрямований на створення кодування, яке чутливе до локального вмісту матриці зображення, але стійке до невеликих змін розташування або зовнішнього вигляду. Для кожної комірки акумулюється локальна одновимірна гістограма орієнтацій градієнтів для всіх пікселів у межах комірки. Діапазон орієнтацій [0, 180°) розбивається на T інтервалів, при цьому інтервал кроку $\Delta\theta$ обчислюється як $\Delta\theta = \frac{180°}{T}$, а окремий інтервал позначається як t, що змінюється в межах послідовності $t = [0, 1, 2, ..., T]$. Кожен t-ий інтервал має межі $[\Delta\theta \cdot t, \Delta\theta \cdot (t+1)]$, а центральне значення обчислюється як $c'_t = \Delta\theta(t + ½)$. Кожна орієнтація $\theta(i, j)$ градієнта у пікселі з індексами (i, j) потрапляє в межі одного з T інтервалів. Для орієнтації градієнта в

комірці спочатку обчислюється *t*-ий інтервал, а потім значення, яке буде надано *t*-му та *(t+1)*-му інтервалам відповідно. Для кожної комірки гістограма створюється як масив з *T* значень, де кожне значення h_t відповідає сумі величин градієнтів *m(i, j)* пікселів у комірці, орієнтація яких потрапляє у відповідний *t*-ий інтервал, з урахуванням вагового значення μ_t для пікселя з індексами *(i, j)* у *t*-му інтервалі, яке визначається на основі орієнтації *θ(i, j)* пікселя [88]:

$$h_t = \sum_{(i,j)\in C} m(i,j) \cdot \mu_t(i,j), \tag{2.27}$$

При цьому вагові коефіцієнти μ_t визначаються за формулою:

$$\mu_t(i,j) = 1 - \frac{|\theta(i,j) - c'_t|}{\Delta\theta}. \tag{2.28}$$

Відповідно, гістограма комірки *C* визначається вектором $\overrightarrow{H_C}$, що має вигляд $\overrightarrow{H_C} = [h_1, h_2, \dots, h_T]$, де *T* – кількість інтервалів орієнтацій.

6. Утворення блоків комірок та нормалізація гістограм блоків. Нормалізація забезпечує кращу інваріантність до освітлення, тіней та контрасту меж. Вона виконується шляхом акумуляції локальних значень гістограми для груп комірок, які об'єднуються у блоки [88].

Позначимо блок, що складається з *r* комірок *C*, як $Q = [C_1, C_2, \dots, C_r]$. При цьому гістограма кожної комірки *C* має вигляд $H_C = [h_1, h_2, \dots, h_T]$, де *T* – кількість інтервалів орієнтацій. Відповідно, гістограма блоку *Q* матиме вигляд $H_Q = [H_{C1}, H_{C2}, \dots, H_{Cr}]$, де *r* – кількість комірок в блоці.

Для нормалізації гістограми блоку обчислюємо L2-норму:

$$x = \sqrt{H_{C1}^2 + H_{C2}^2 + \dots + H_{Cr}^2}. \tag{2.29}$$

Нормалізована гістограма H'_Q блоку обчислюється за формулою:

$$H'_Q = \left[\frac{H_{C1}}{x}, \frac{H_{C2}}{x}, \dots, \frac{H_{Cr}}{x}\right]. \tag{2.30}$$

7. Формування вектору ознак HOG матриці зображення. Після нормалізації гістограм блоків формується глобальна гістограма матриці зображення, поданої на вхід алгоритму. Ця глобальна гістограма є дескриптором HOG матриці зображення.

Вектор ознак V_{HOG} формується шляхом об'єднання нормалізованих гістограм блоків:

$$V_{HOG} = \left[H'_{Q1}, H'_{Q2}, \dots, H'_{Qz}\right], \quad (2.31)$$

де z – індекс гістограми блоку у загальній послідовності $z = [1, 2, \dots, Z]$, а Z – кількість блоків, утворених в результаті об'єднання комірок матриці зображення.

Схематичний приклад формування значення вектору ознак HOG представлено на Рисунку 2.4.

2.3 Комплексний метод біометричної ідентифікації

Після детального аналізу окремих методів, що описані в попередніх розділах, сформовано комплексний метод біометричної ідентифікації, який дозволяє максимально ефективно використовувати переваги кожного з методів, покладених його в основу, для досягнення високої точності ідентифікації.

Суть комплексного методу полягає в тому, що на кожному етапі обробки зображення використовуються найефективніші інструменти для виділення та аналізу ознак, що дозволяє значно підвищити точність порівняння та класифікації облич. Як вхідні дані комплексний метод використовує зображення, на якому необхідно ідентифікувати суб'єкт. Покрокове виконання комплексного методу можна описати так:

1. Виявлення обличчя на зображенні. На вхідному зображенні локалізується область обличчя методом Віола-Джонса на основі каскадів Гаара. Для подальшої обробки використовується лише зображення обличчя людини, оскільки це область інтересу для процесу біометричної ідентифікації.

2. Попередня обробка зображення. Зображення обличчя, що отримане в результаті виявлення, обробляється методом анізотропної дифузії, який дозволяє зберегти та покращити інформацію про риси обличчя на зображенні, а також видалити шум.

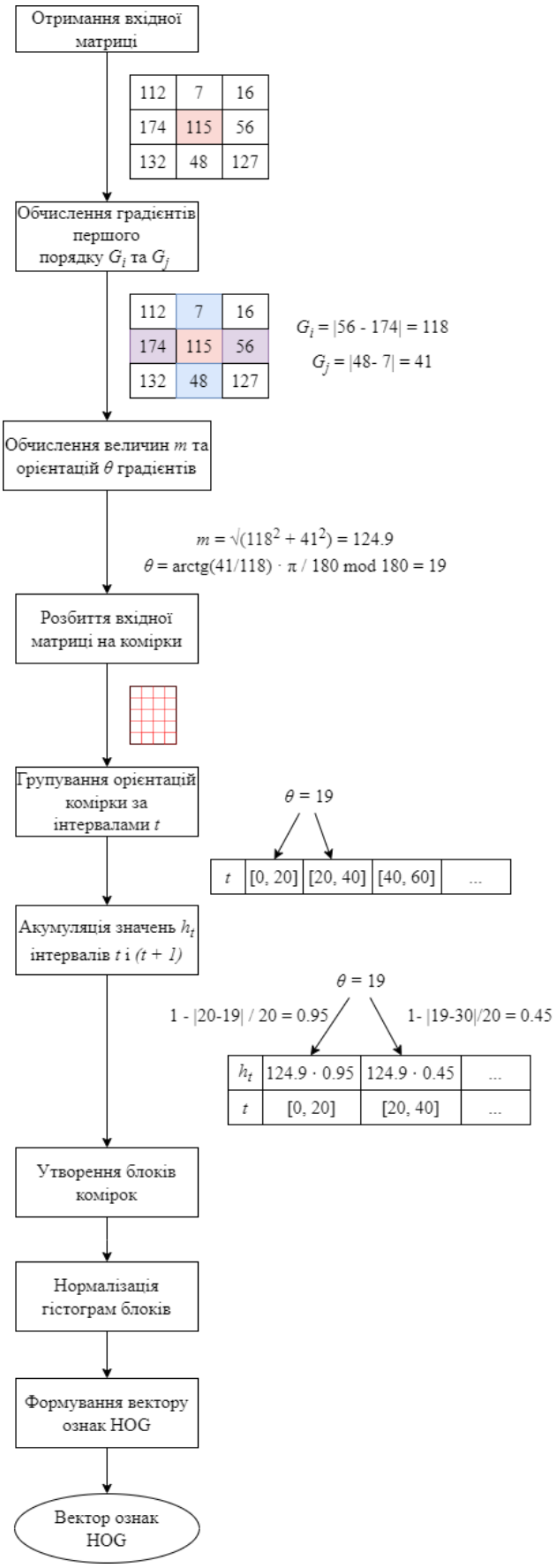


Рисунок 2.4 – Схематичний приклад формування значення результуючого вектору дескриптора гістограм орієнтованих градієнтів (HOG)

3. Обробка зображення. Зображення обличчя після застосування до нього анізотропної дифузії обробляється вейвлетами Ґабора з різними значеннями параметрів вейвлет-функції таким чином, щоб отримати 16 вейвлет-перетворених варіацій зображення обличчя. Кожне з вейвлет-перетворених зображень передається на вхід методів вилучення векторів ознак.

4. Вилучення векторів ознак. Зображення, сформовані в результаті застосування вейвлет-перетворення Ґабора, одночасно надходять на вхід двох окремих методів вилучення ознак – локальних бінарних шаблонів в одновимірному просторі (1DLBP) та гістограм орієнтованих градієнтів (HOG). В результаті вилучення ознак з вейвлет-перетворених зображень із застосуванням кожного з цих методів формуються два окремих 512-значних вектора ознак.

5. Формування глобального вектора та його класифікація. Через відхилення у векторних розподілах і діапазонах, вектори ознак, вилучені окремо з використанням методів 1DLBP і HOG, несумісні. Для покращення сумісності векторів і створення єдиного глобального вектора ознак використовується мінімально-максимальна нормалізація, яка перетворює вектори ознак у діапазоні [0, 1]. Позначимо вектор ознак 1DLBP як $V_{1DLBP} = [E_1, E_2, \ldots, E_{512}]$, а вектор ознак HOG як $V_{HOG} = [H_1, H_2, \ldots, H_{512}]$. Значення елементів нормалізованих векторів ознак обчислюються з використанням мінімально-максимальної нормалізації за допомогою формул:

$$E' = \frac{E_{i''} - min(V_{1DLBP})}{max(V_{1DLBP}) - min(V_{1DLBP})}, \tag{2.32}$$

$$H' = \frac{H_{i''} - min(V_{HOG})}{max(V_{HOG}) - min(V_{HOG})}, \tag{2.33}$$

де i'' – індекс елемента у векторі ознак, *min()* і *max()* – операції пошуку мінімального та максимального елементів вектора, відповідно.

Нормалізовані вектори ознак 1DLBP і HOG об’єднуються, щоб сформувати глобальний вектор ознак зображення обличчя, що складається зі 1024 значень. Позначимо нормалізовані вектори ознак 1DLBP як $V'_{1DLBP} = [E'_1; E'_2; \ldots; E'_{512}]$ для

1DLBP і HOG як $V'_{HOG} = [H'_1; H'_2; \ldots; H'_{512}]$. Таким чином, глобальний вектор ознак V_g можна представити у вигляді [93]:

$$V_g = [E'_1, E'_2, \ldots, E'_{512}, H'_1, H'_2, \ldots, H'_{512}]. \quad (2.34)$$

Отриманий вектор глобальних ознак використовується для подальшої класифікації з використанням метрики квадратичної відстані Евкліда. Глобальний вектор порівнюється із кожним вектором для зображень, що містяться у базі даних. Якщо один з еталонних векторів з бази даних позначити як V_e, то відстань між векторами обчислюватиметься наступним чином:

$$d^2(V_g, V_e) = \sum_{j''=1}^{1024} (V_{gj''} - V_{ej''})^2, \quad (2.35)$$

де j'' – індекс елемента у векторі ознак.

Кожен вектор, що міститься в базі даних, позначається відповідним ідентифікатором суб'єкта, якому він належить. Отже, результатом роботи розробленого комплексного методу біометричної ідентифікації є ідентифікатор особи, квадратична Евклідова відстань до вектору ознак зображення обличчя якої є найменшою.

Структурна схема розробленого комплексного методу біометричної ідентифікації на основі локально-текстурних дескрипторів представлена на Рисунку 2.5.

2.4 Підбір параметрів комплексного методу біометричної ідентифікації

З метою підвищення ефективності розробленого комплексного методу біометричної ідентифікації необхідно здійснити підбір параметрів для методів, що лежать в його основі. Вибір параметрів є важливим етапом, оскільки навіть незначні відхилення в їх значеннях можуть суттєво вплинути на результативність комплексного методу в цілому. Параметри кожного методу, що лежать в основі процесу біометричної ідентифікації, визначають, як саме будуть оброблятися дані, а отже – точність отриманих результатів.

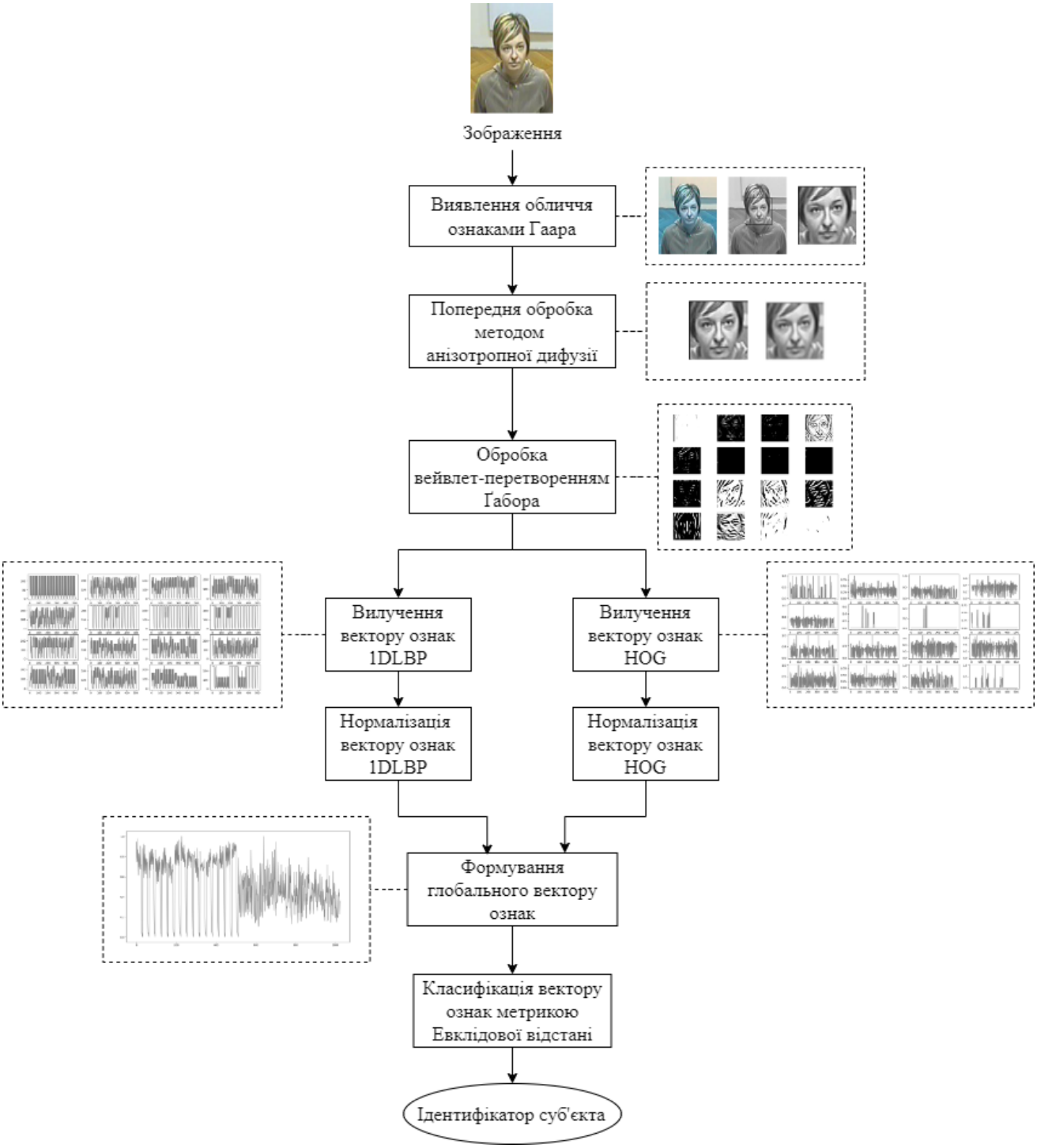


Рисунок 2.5 – Структурна схема комплексного методу біометричної ідентифікації на основі локально-текстурних дескрипторів

Коректний вибір параметрів дозволяє максимізувати ефективність кожного з методів і забезпечити оптимальну взаємодію між етапами ідентифікаційного процесу ідентифікації, що є ключем до досягнення високої точності ідентифікації при мінімальних обчислювальних витратах.

Найбільш суттєвим етапом процесу ідентифікації є обробка зображень облич, який в даній роботі здійснюється з використанням вейвлет-перетворення Ґабора. Відповідно, підбір параметрів комплексного методу біометричної ідентифікації варто почати з даного методу.

Як і під час попередніх досліджень методів, що лежать в основі комплексного методу біометричної ідентифікації, експерименти щодо підбору параметрів проводилися з використанням набору даних The Database of Faces, що містить зображення облич 40 суб'єктів.

Для здійснення найбільш повного аналізу зображень облич, необхідно використовувати набір фільтрів Ґабора з різними параметрами. Після застосування до зображення обличчя операції згортки з усіма фільтрами проводиться аналіз отриманих результатів. Оскільки операції дискретної згортки потребує часу, збільшується загальний час, необхідний для фільтрації з використанням набору ядер фільтрів.

Спершу необхідно визначити оптимальний розмір фільтру Ґабора. Вибір розміру ядра залежить від властивостей зображень, до яких буде застосовуватися фільтр. Використання ядра фільтру меншого розміру зображення дозволяє виявити дрібні деталі на зображеннях, і навпаки – ядра більшого розміру краще обробляють більші об'єкти. Розмір ядра може бути будь-якого розміру, наприклад 3×3, 5×5, 7×7, 9×9, . . ., 31×31, 33×33 і так далі. Проте, якщо розмір ядра перевищує 31×31, то у відфільтрованому зображенні не спостерігатиметься жодних змін, тобто в певний момент великі розміри ядра не показують відхилень у відфільтрованому зображенні (воно майже збігається з вхідним зображенням, що відомо як ефект розмиття Ґауса [104]. Тому для визначення розміру ядра фільтрів Ґабора, що лежать в основі розробленого комплексного методу біометричної ідентифікації, будуть використовуватися значення розмірів від 3×3 до 31×31. На виявлення деталей та, як

наслідок, на рівень шуму на зображеннях, впливає число орієнтацій, оскільки фільтр має чітко виражену орієнтаційну вибірковість. Згідно з даними, наведеними в літературі, присвяченій дослідженням, що використовуються фільтри Ґабора, для виявлення незначних деталей потрібно максимум 18 орієнтацій, про що свідчать також дослідження в області нейрофізіології [105, 106]. Тому для визначення розміру фільтрів, які застосовуватимуться для обробки зображень в даному дослідженні, створюємо набір з 18 фільтрів з орієнтаціями θ від 0 до π. Такий діапазон обрано через симетричність фільтрів Ґабора щодо напрямків, тому немає необхідності розрізняти орієнтації від 0 до 2π. На час дослідження значення решти параметрів фільтрів встановлюємо як середні значення діапазону можливих значень для кожного із параметрів.

З порівняльної діаграми результатів на Рисунку 2.6 випливає, що найбільше значення точності ідентифікації, яке становить 75%, отримано з використанням фільтрів з розміром 25×25. Проте такий розмір фільтру є завеликим для задачі розпізнавання облич, оскільки часто зображення облич мають низьку роздільну здатність, що призводить до врахування фільтром зайвої інформації та неможливості виділити важливі дрібні локальні особливості. Також використання фільтру такого розміру потребує більших обчислювальних ресурсів. Один із наступних за ефективністю результатів отримано за значень розміру фільтру 9×9, а саме показник точності складає 72.5%. Така розмірність фільтру є більш прийнятною, проте існує ймовірність, що при зміні значень решти параметрів точність ідентифікації за інших значень розмірів також зміниться. Тому для подальших досліджень вирішено обрати розмірність 9×9, як таку, що дозволила отримати один із найвищих результатів, а також попереднє та наступне значення розмірностей, що становлять 7×7 і 11×11.

Далі визначимо, які значення орієнтацій θ фільтрів є найбільш ефективними для вирішення поставленого завдання. Для цього перевіряємо кожне із значень θ в межах від 0 до π з кроком $\frac{\pi}{18}$, змінюючи значення довжини хвилі λ таким чином, щоб утворилося 18 фільтрів для кожного із значень орієнтації. При цьому немає

необхідно у перевірці значення π, оскільки через симетричність фільтрів будуть отримані ті самі результати, що і при $\theta = 0$.

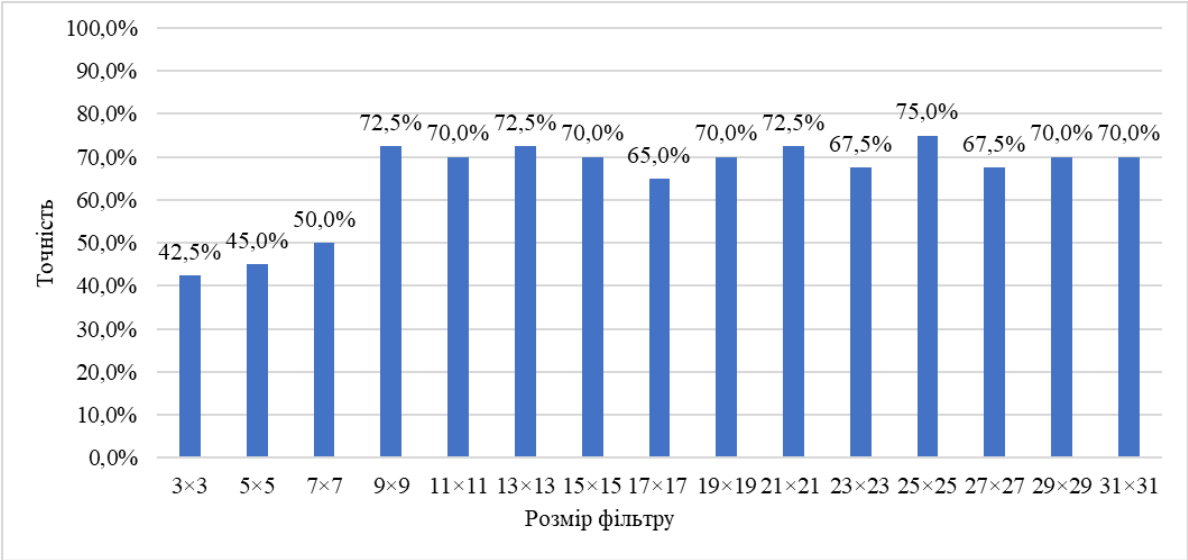
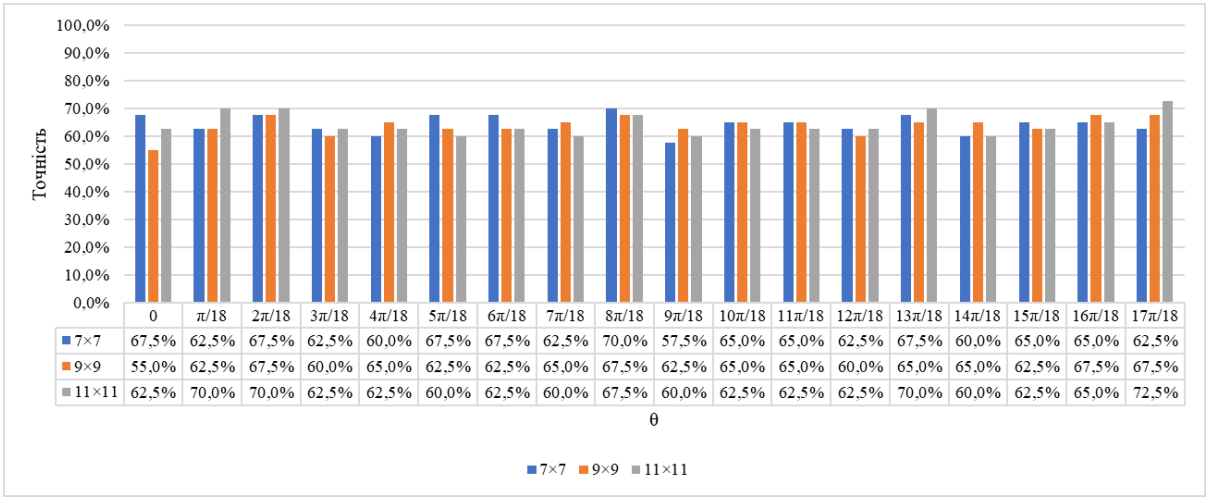


Рисунок 2.6 – Порівняльна діаграма експериментальних результатів підбору розміру фільтрів Ґабора

З результатів, представлених на Рисунку 2.7, випливає, що найбільшого значення точності 72.5% отримано при значенні орієнтації $\theta = \frac{7\pi}{18}$ і розмірі фільтру 11×11. Наступний результат точності 70% отримано при значеннях орієнтації $\theta = \frac{\pi}{18}, \frac{2\pi}{18}, \frac{8\pi}{18}, \frac{13\pi}{18}$ і розмірах фільтру 7×7 і 11×11. Для того, щоб визначитися з найбільш доцільним значенням орієнтації здійснимо підбір параметру довжини хвилі синусоїдальної складової λ.

Для визначення ефективних значень довжини хвилі синусоїдальної складової λ фільтрів встановлюємо константним значення орієнтації θ, а значення λ змінюємо в межах від 0 до π з кроком $\frac{\pi}{18}$. При цьому, виходячи з формули генерації фільтрів Ґабора, λ не може дорівнювати 0, тому початковим значенням діапазону є $\lambda = \frac{\pi}{18}$.



	0	π/18	2π/18	3π/18	4π/18	5π/18	6π/18	7π/18	8π/18	9π/18	10π/18	11π/18	12π/18	13π/18	14π/18	15π/18	16π/18	17π/18
7×7	67,5%	62,5%	67,5%	62,5%	60,0%	67,5%	67,5%	62,5%	70,0%	57,5%	65,0%	65,0%	62,5%	67,5%	60,0%	65,0%	65,0%	62,5%
9×9	55,0%	62,5%	67,5%	60,0%	65,0%	62,5%	62,5%	65,0%	67,5%	62,5%	65,0%	65,0%	60,0%	65,0%	65,0%	62,5%	67,5%	67,5%
11×11	62,5%	70,0%	70,0%	62,5%	62,5%	60,0%	62,5%	60,0%	67,5%	60,0%	62,5%	62,5%	62,5%	70,0%	60,0%	62,5%	65,0%	72,5%

Рисунок 2.7 – Порівняльна діаграма експериментальних результатів підбору параметру орієнтації θ фільтрів Ґабора

З результатів на Рисунку 2.8 слідує, що найбільша кількість пікових значень точності, що складає 72.5% отримано при значеннях $\lambda = \frac{2\pi}{18}, \frac{5\pi}{18}, \frac{17\pi}{18}$ та розмірі фільтру 7×7.

Оскільки в дисертаційному дослідженні поставлено завдання ідентифікації на зображеннях облич, важливо розуміти, що виконання методу потребує компромісу між точністю ідентифікації та кількістю обчислювальних ресурсів. Враховуючи це, а також вищенаведені результати підбору параметрів, для подальших досліджень вирішено обрати розмір фільтрів 7×7 і крок зміни параметрів орієнтації θ у $\frac{\pi}{18}$. Такий параметр орієнтації θ покриває кут у 180 градусів, що є достатнім для фільтрації зображення обличчя, враховуючи симетричність фільтрів.

Для 18 орієнтацій фільтрів необхідно підібрати такі параметри довжини хвилі, за яких точність комплексного методу біометричної ідентифікації є найвищою. Оскільки найбільш ефективний крок визначено, необхідно встановити початкове значення параметру. Враховуючи, що параметр довжини хвилі λ може приймати значення від 0 до π, здійснимо перевірку значень в цих межах з кроком $\frac{\pi}{5}$. Результати даного експерименту представлені на Рисунку 2.9.

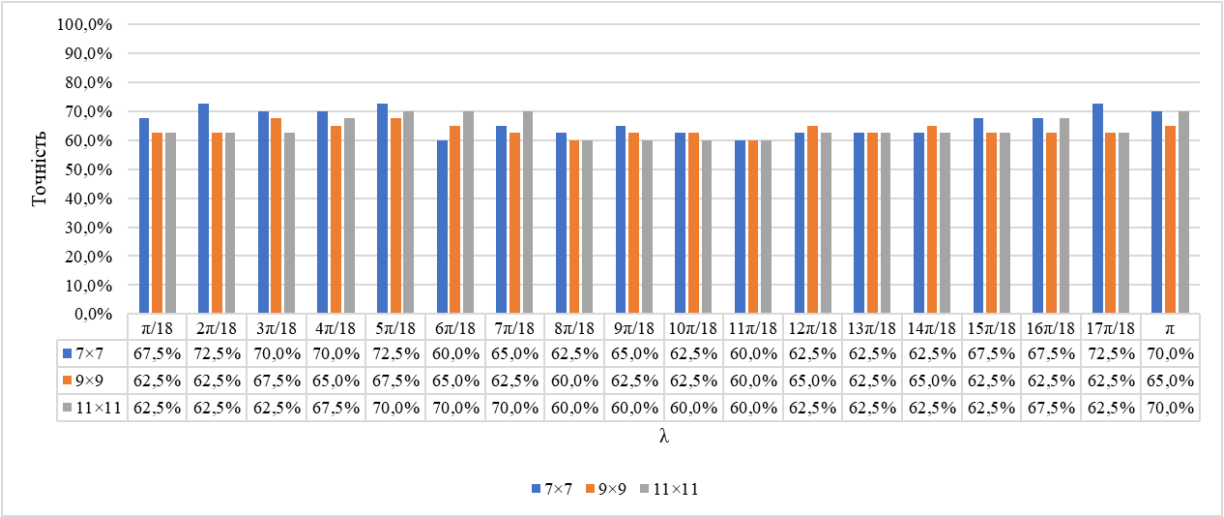


Рисунок 2.8 – Порівняльна діаграма експериментальних результатів підбору параметру довжини хвилі синусоїдальної складової λ фільтрів Ґабора

Перевіримо коректність підібраного параметру кроку $\frac{2\pi}{18}$, або $\frac{\pi}{9}$. Для цього візьмемо декілька значень, близьких до заданого, та які не були покриті при підборі параметру з кроком $\frac{\pi}{18}$. Для цього експерименту визначимо наступні значення $\lambda = \frac{\pi}{7}, \frac{\pi}{8}, \frac{\pi}{9}, \frac{\pi}{10}, \frac{\pi}{11}$.

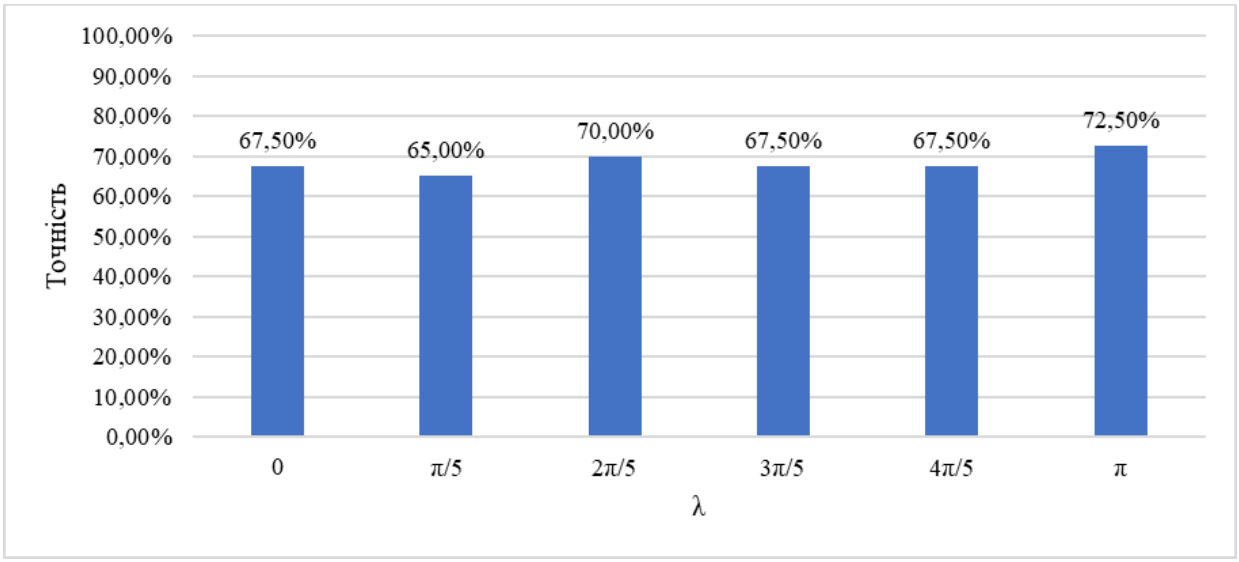


Рисунок 2.9 – Порівняльна діаграма експериментальних результатів підбору початкового значення параметру довжини хвилі λ фільтрів Ґабора

З порівняльної діаграми на Рисунку 2.9 випливає, що початкове значення $\lambda = \pi$ дозволяє отримати найвищий показник точності. Експерименти щодо встановлення коректності кроку зміни параметру довжини хвилі λ, результати яких наведені на Рисунку 2.10, продемонстрували, що крок $\frac{\pi}{9}$ дійсно є ефективним, проте той самий показник точності отримано і при значенні кроку $\frac{\pi}{10}$, що є більш прийнятним значенням з точки зору складності обчислень. Відповідно, у подальших дослідження для формування фільтрів Ґабора довжина хвилі λ змінюватиметься від значення π з кроком $\frac{\pi}{10}$.

Наступним етапом підбору параметрів комплексного методу біометричної ідентифікації є визначення значення стандартного відхилення ядра Ґауса σ. Для початку необхідно визначити діапазон, в якому змінювати значення параметру. У роботі [107] запропоновано значення σ, еквівалентне довжині хвилі λ, тобто $\sigma = \lambda$, тому у якості відправної точки для проведення досліджень обираємо таке ж значення параметру та стратегію параметру значень. Спершу змінюємо значення σ у діапазоні від 0 до π з кроком $\frac{\pi}{18}$, проте враховуємо, що перше значення не може дорівнювати 0 згідно з формулою побудови фільтра Ґабора.

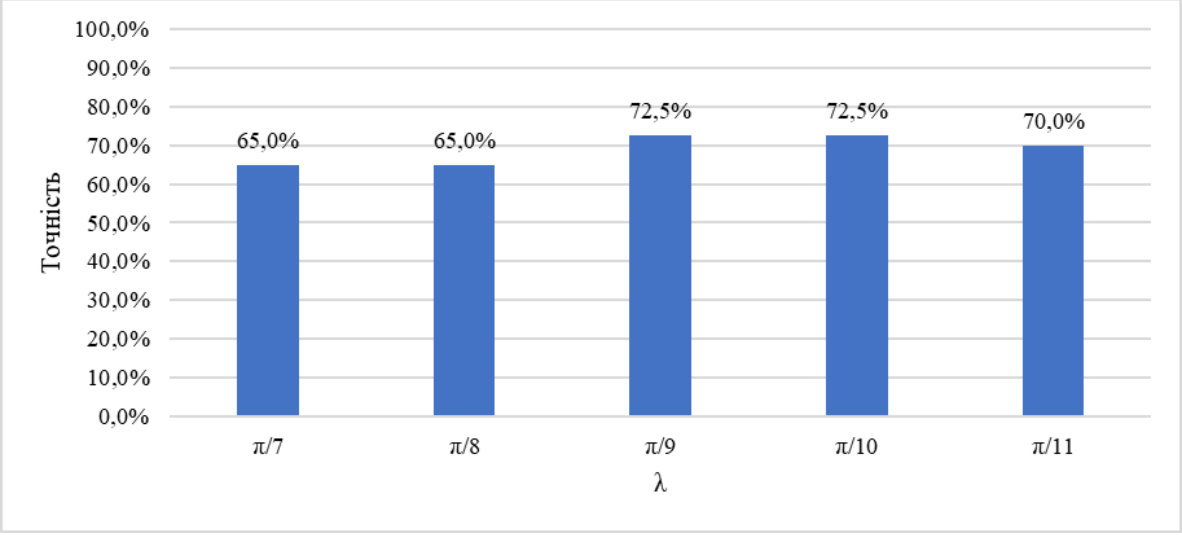


Рисунок 2.10 – Порівняльна діаграма експериментальних результатів підбору кроку зміни значення параметру довжини хвилі λ фільтрів Ґабора

Як видно з результатів, наведених на Рисунку 2.11, найвищий показник точності отримано при значенні параметру $\sigma = \frac{2\pi}{18}$, або $\frac{\pi}{9}$. Аналогічно до підбору параметру λ, визначимо початкове значення параметру σ, встановлюючи значення параметру від 0 до π з кроком $\frac{\pi}{5}$.

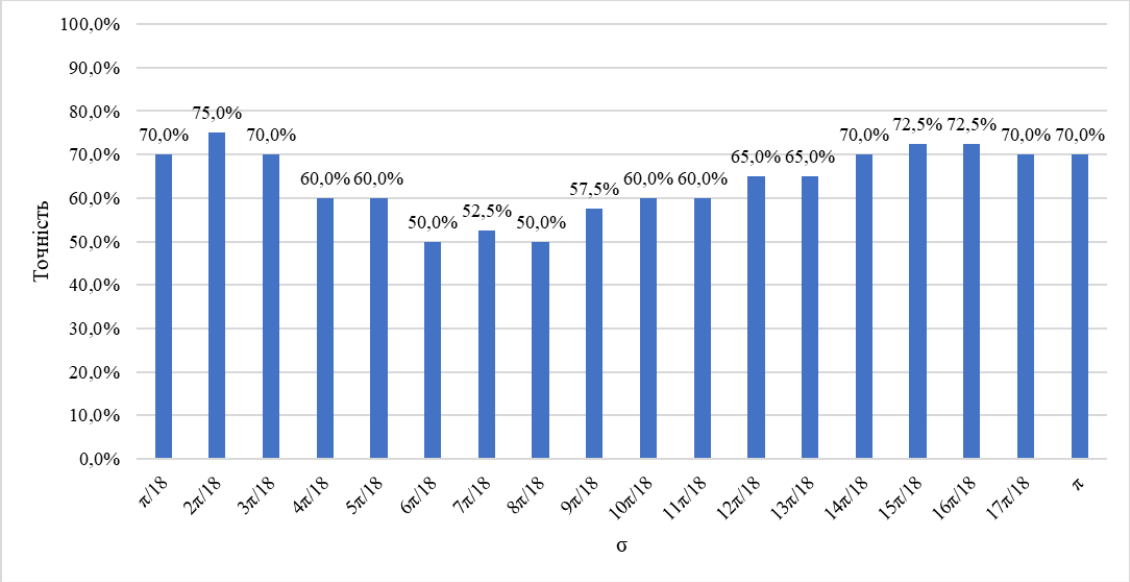


Рисунок 2.11 – Порівняльна діаграма експериментальних результатів підбору параметру стандартного відхилення ядра Ґауса σ фільтрів Ґабора

Результати, наведені на Рисунку 2.12, свідчать про те, що пікових значень параметр σ сягає при початкових значеннях $\sigma = 0, \frac{4\pi}{5}, \pi$.

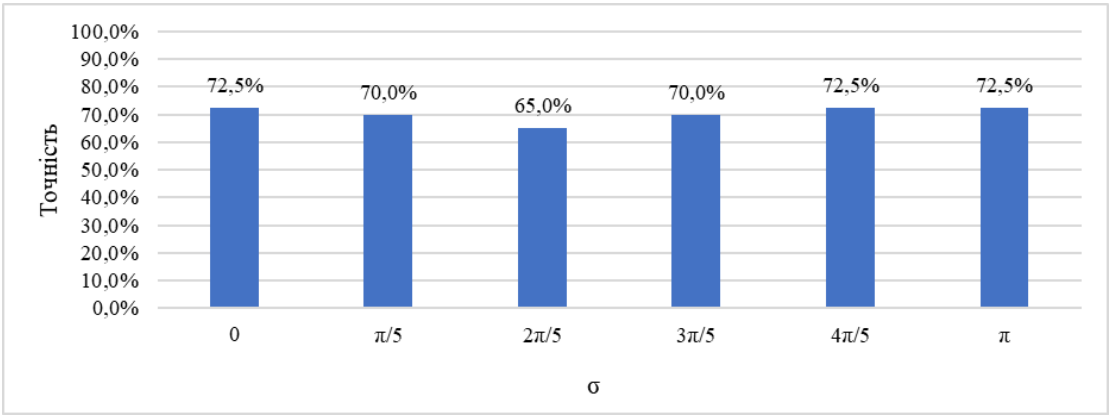
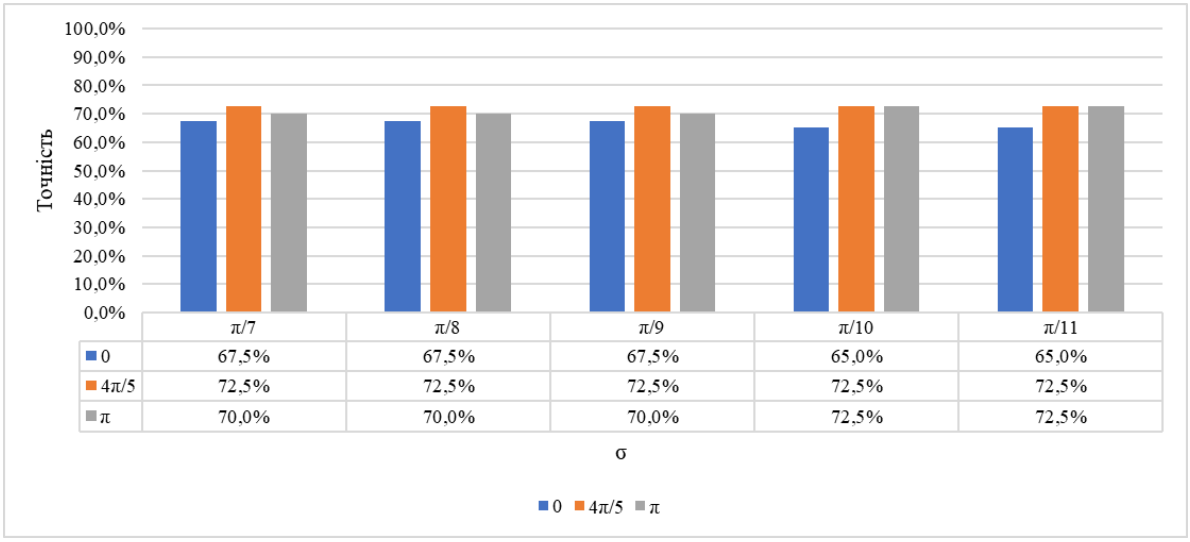


Рисунок 2.12 – Порівняльна діаграма експериментальних результатів підбору початкового значення стандартного відхилення ядра Ґауса σ фільтрів Ґабора

Аналогічно експериментів з підбору параметру λ, перевіримо коректність визначеного кроку зміни параметра $\sigma = \frac{\pi}{9}$. Встановимо значення σ, набором значень, близьких до заданого, що не були використані при підборі параметру з кроком $\frac{\pi}{18}$, а саме $\sigma = \frac{\pi}{7}, \frac{\pi}{8}, \frac{\pi}{9}, \frac{\pi}{10}, \frac{\pi}{11}$. При цьому також використаємо три визначених у попередньому експерименті початкових значення σ для встановлення найбільш ефективної комбінації параметрів.

Виходячи з результатів, представлених на Рисунку 2.13, найбільших показників точності розроблений метод сягає при початкових значеннях параметра $\sigma = \frac{4\pi}{5}$, π, та при зміні кроку $\frac{\pi}{10}, \frac{\pi}{11}$. З метою зменшення кількості математичних операцій при виконанні комплексного методу біометричної ідентифікації і відповідно часу виконання, початкове значення σ встановлюємо π. Оскільки для зміни параметру λ використовувалися значення від π з кроком $\frac{\pi}{10}$, що також є ефективною комбінацією в даному експерименті, для зменшення обчислювальної складності комплексного методу біометричної ідентифікації також вирішено встановити значення σ від π з кроком $\frac{\pi}{10}$.



	π/7	π/8	π/9	π/10	π/11
0	67,5%	67,5%	67,5%	65,0%	65,0%
4π/5	72,5%	72,5%	72,5%	72,5%	72,5%
π	70,0%	70,0%	70,0%	72,5%	72,5%

Рисунок 2.13 – Порівняльна діаграма експериментальних результатів підбору початкового значення та кроку зміни значення стандартного відхилення ядра Ґауса σ фільтрів Ґабора

Далі необхідно здійснити підбір параметрів фазового зсуву синусоїди ψ та еліптичності носія функції Ґабора γ. Параметр ψ впливає на симетричність ядра фільтру та введений у якості альтернативи квадратурній парі фільтрів. Він може приймати значення $-\frac{\pi}{2}$ або $\frac{\pi}{2}$ для виявлення асиметричних компонент і -π, 0 або π для симетричних компонент. Параметр γ приймає значення в діапазоні (0, 1] і визначає витягнутість ядра фільтру по вісі ординат. У роботі [105] наведено рекомендацію щодо вибору значення параметра з інтервалу $0.23 < \gamma < 0.92$, найчастіше приймають $\gamma = 0.5$.

Експерименти зі встановлення значення параметру фазового зсуву синусоїди ψ проводилися для заданих можливих значень параметру, а саме в діапазоні від -π до π з кроком $\frac{\pi}{2}$. Результати експериментів представлені на Рисунку 2.14. Найвищий показник точності отримано при значенні параметру $\psi = \frac{\pi}{2}$. Відповідно, таке значення використовувалося для проведення подальших досліджень.

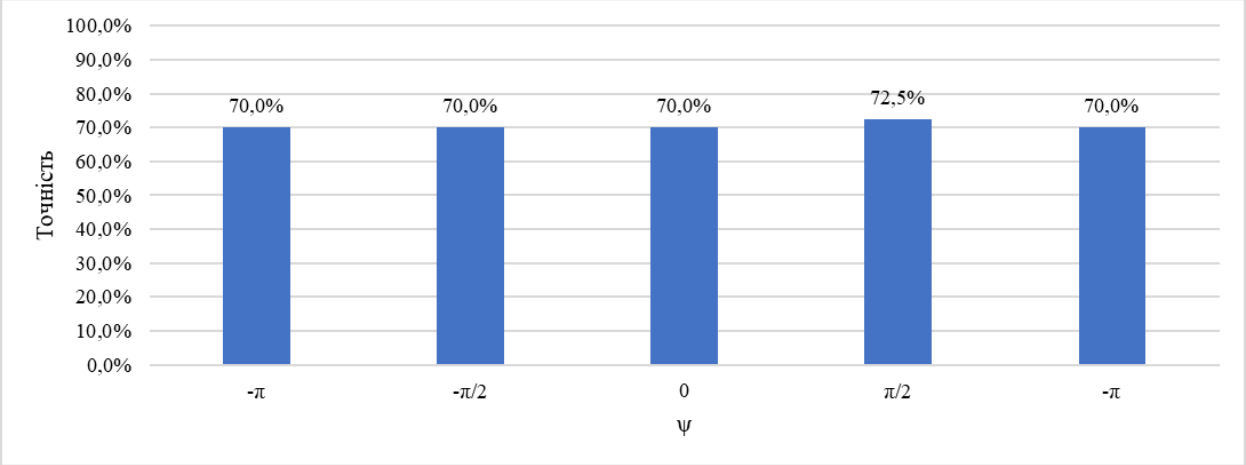


Рисунок 2.14 – Порівняльна діаграма експериментальних результатів підбору фазового зсуву синусоїди ψ фільтрів Ґабора

Для визначення значення параметру γ вирішено провести експерименти зі значеннями, що лежать в можливому діапазоні значень параметру, а саме від 0.3 до 0.9 з кроком 0.1. У результаті експерименту отримано значення точності 72.5% при всіх заданих значеннях γ. З цього випливає, що при використані розробленого

комплексного методу біометричної ідентифікації параметр γ значно не впливає на точність, відповідно значення γ встановлено як найменше з визначеного діапазону параметру, а саме $\gamma = 0.24$.

Також перевірено можливість зменшення кількості фільтрів шляхом експериментів зі зміною значення кількості орієнтацій θ. У результаті показник точності стабільно однаковий зі зміною θ з $\frac{\pi}{18}$ до $\frac{\pi}{11}$, що дозволяє змінити кількість фільтрів з 18 до 11. Проте, варто зазначити, що при зміні набору зображень, до яких застосовується розроблений комплексний метод ідентифікації, може змінитися і показник точності, оскільки більша кількість фільтрів дозволяє отримати більш повну інформацію про зображення, до яких вони застосовуються. Тому оптимальним є використання середнього значення кількості фільтрів. Таким чином, для подальших досліджень використовувалося значення зміни кількості орієнтацій $\frac{\pi}{16}$ і 16 фільтрів відповідно.

Наступним кроком підбору параметрів створеного комплексного методу біометричної ідентифікації є визначення параметрів методів вилучення ознак. У процесі здійснення вилучення ознак методом ідентифікації утворюється вектор із 1024 значень, який далі подається на вхід методу класифікації. Саме така розмірність вектору обрана для досягнення компромісу між збереженням детальних ознак зображень облич і обмеженням обчислювальної складності. Крім того, цей розмір є досить типовим у задачах комп'ютерного зору та машинного навчання, отже, за необхідності інтегрувати розроблений комплексний метод в будь-яку систему це буде простіше зробити зі стандартними значеннями розмірностей векторів ознак. Оскільки в даній роботі використовуються два методи вилучення ознак, 1DLBP і HOG, для векторів, що сформуються в результаті застосування кожного з них, відведено по 512 значень глобального вектору. Отже, параметри методів вилучення ознак підбиралися у відповідності з необхідною розмірністю вектору ознак.

Розмірність дескриптора 1DLBP залежить від роздільної здатності блоків, на які розбивається зображення, що подається на вхід методу. Щоб отримати вектор з

512 значень вирішено використовувати роздільну здатність блоків 16×32 пікселі. Параметри дескриптора HOG були встановлені емпірично у відповідності до необхідності сформувати вектор з 512 значень, що є іншою половиною глобального вектора ознак зображення обличчя з 1024 значень. Таким чином, для формування дескриптора HOG використовувалися наступні значення: число орієнтацій, на які розділено інформацію про градієнт на гістограмі – 8, розмір клітинки, для якої обчислюється кожна градієнтна гістограма – 16×36 пікселів, локальна область, у які нормалізується кількість гістограм у заданій комірці – 1×1 пікселі.

Останнім методом, що вимагає підбору параметрів, є метод попередньої обробки зображень облич з використанням анізотропної дифузії. Спершу здійснимо підбір параметру κ, що контролює провідність як функцію градієнта. Якщо κ низький – невеликі градієнти інтенсивності можуть блокувати провідність, а отже і дифузію, через різкі перепади меж об'єктів на зображеннях. Велике значення κ зменшує вплив градієнтів інтенсивності на провідність. Коефіцієнт провідності κ зазвичай змінюється в діапазоні від 20 до 100 одиниць. Для проведення експерименту з підбору даного параметра вирішено перевірити значення в цьому діапазоні з кроком 5. На час експерименту всі інші параметри встановлені в середні значення своїх діапазонів. Проте результат, отриманий у ході експерименту виявився однаковим для всіх значень κ, а саме коефіцієнт точності становив 72.5%. Щоб зменшити обчислювальну складність методу попередньої обробки, а відповідно і комплексного методу біометричної ідентифікації в цілому, параметр κ встановлено у найменше можливе значення, тобто $\kappa = 20$. Аналогічні результати були отримані й при підборі параметрів швидкості дифузії η і кількості ітерацій μ. Оскільки не отримано значних покращень продуктивності комплексного методу біометричної ідентифікації за рахунок використання методу попередньої обробки, значення параметрів були встановлені як найменш можливі. Таким чином були визначені наступні параметри: $\mu = 10$, $\eta = 0.1$.

Проте вирішено провести дослідження методу попередньої обробки з використанням зображень облич з іншого набору зображень – SCface. При цьому експерименті зміна параметрів κ і η не дала суттєвих змін результативності. Проте

розглянемо більш детально експеримент зі встановлення кількості необхідних ітерацій.

Як видно з порівняльної діаграми на Рисунку 2.15, зміна кількості ітерацій мала значний вплив на ефективність комплексного методу біометричної ідентифікації, а найвищий показник точності отримано при кількості ітерацій μ = 10. Відповідно, таке значення цього параметру використовуватиметься і в подальших дослідженнях.

У висновку до проведених досліджень слід зазначити, що завдяки ретельному підбору параметрів на кожному етапі виконання розробленого комплексного методу вдалося досягти високого рівня точності при раціональній обчислювальній складності. Зокрема, встановлено, що оптимальний розмір фільтрів Ґабора для обробки зображень — 9×9 пікселів — забезпечує найкращий баланс між ефективністю ідентифікації та продуктивністю обчислень. Додатково, параметри орієнтації, довжини хвилі, стандартного відхилення, фазового зсуву і витягнутості фільтрів були підібрані таким чином, щоб мінімізувати обчислювальні витрати без втрати точності методу.

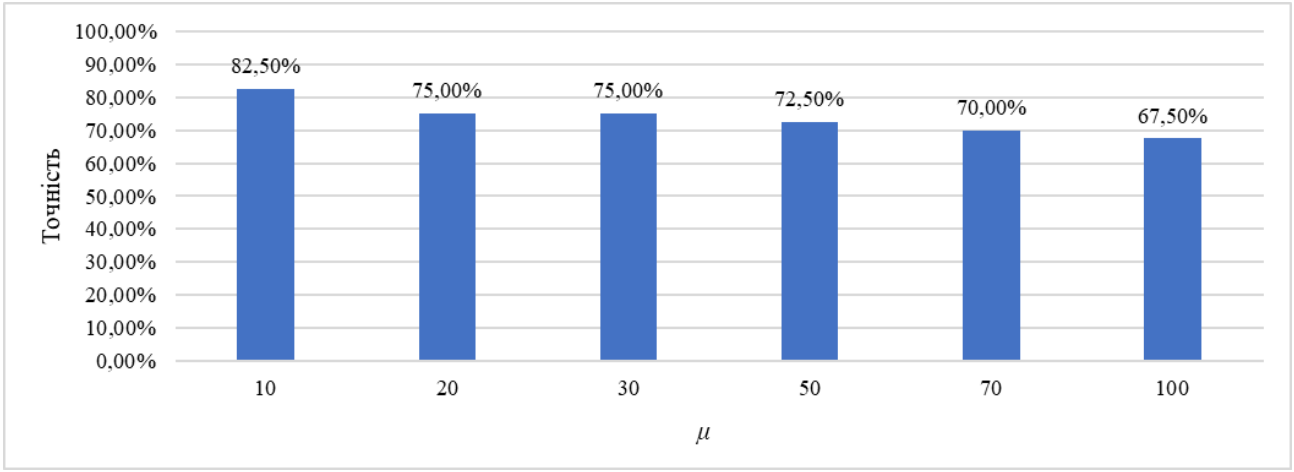


Рисунок 2.15 – Порівняльна діаграма експериментальних результатів підбору кількості ітерацій застосування методу анізотропної дифузії

Окрему увагу приділено підбору параметрів методів вилучення ознак, 1DLBP та HOG, де вдалося досягти необхідної розмірності вектора ознак для збереження

високого рівня точності. Параметри анізотропної дифузії для попередньої обробки зображень були встановлені на мінімально можливому рівні, що суттєво знижує обчислювальну складність загального методу.

Таким чином, комплексний метод біометричної ідентифікації завдяки підбору параметрів забезпечує точне розпізнавання облич при ефективному використанні обчислювальних ресурсів.

Висновки до розділу 2

Другий розділ присвячено дослідженню та розробці математичного забезпечення для програмного рішення біометричної ідентифікації за зображенням обличчя, під час яких отримані наступні результати:

1. Здійснено вибір методів для розв'язання задачі біометричної ідентифікації за зображенням обличчя, а саме для подальшого використання на основі результатів експериментів обрано метод анізотропної дифузії з показником точності 92,5%, метод вейвлет-перетворення Ґабора з показником точності 87,5%, локальні бінарні шаблони в одновимірному просторі (1DLBP) та гістограми орієнтованих градієнтів (HOG) з точністю 70% та метрику обчислення квадратичної відстані Евкліда з показником точності становить 92,5%.

2. Описано математичне забезпечення для програмного рішення біометричної ідентифікації за зображенням обличчя, що складається з методів Віола-Джонса на основі каскадів Гаара, анізотропної дифузії для попередньої обробки зображень, вейвлет-перетворення Ґабора для обробки зображень, локальних бінарних шаблонів в одновимірному просторі (1DLBP) та гістограм орієнтованих градієнтів (HOG) для вилучення векторів ознак із зображень та квадратичної відстані Евкліда для класифікації векторів ознак.

3. На основі створеного математичного забезпечення описано комплексний метод біометричної ідентифікації за зображенням обличчя, що містить вищезгадані методи.

4. Виконано підбір параметрів методів, що лежать в основі розробленого комплексного методу біометричної ідентифікації за зображенням обличчя.

РОЗДІЛ 3. ПРОГРАМНА КОМПОНЕНТА РОЗВ'ЯЗАННЯ ЗАДАЧІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

3.1 Аналіз варіантів використання програмної компоненти

З метою встановлення ефективності розробленого комплексного методу біометричної ідентифікації за зображенням обличчя, необхідно розробити програмне забезпечення, здатне здійснювати процес ідентифікації.

Перш ніж перейти безпосередньо до розробки програмного забезпечення, необхідно виділити основні функціональні особливості, що мають бути реалізовані у програмній системі. В отриманій у результаті проєктування та реалізації програмній системі мають бути доступні наступні мінімальні можливості для здійснення ідентифікації за допомогою запропонованого методу:

- Програма захоплює зображення людини з відеопотоку камери або користувач завантажує зображення, збережене на пристрої.
- Програма демонструє вихідне зображення користувачу на екрані.
- Програма передає зображення на вхід комплексного методу.
- Програма обробляє вхідне зображення за допомогою комплексного методу біометричної ідентифікації, формуючи в якості результату вектор ознак.
- Програма здійснює порівняння отриманого вектору ознак із зареєстрованими записами, що містяться в базі даних.
- Програма отримує із бази даних ідентифікатор, який належить суб'єкту ідентифікації, або повідомлення, що записів про суб'єкт ідентифікації не виявлено.
- Програма повертає ідентифікатор знайденого запису, надаючи користувачу можливість перегляду персональних даних ідентифікованого суб'єкта, або повідомлення, що суб'єкта ідентифікації не виявлено в базі даних.

Додатковими можливостями, реалізованими у програмному забезпеченні, можуть бути наступні:

- Перегляд попередніх результатів процесу ідентифікації.
- Реєстрація записів про новий суб'єкт у базі даних.

- Перегляд бази даних та окремо досьє кожного суб’єкта, зареєстрованого в базі даних.
- Здійснення експериментальних досліджень для покращення процесу ідентифікації з виведенням програмою на екран показників точності ідентифікації та графічної інформації про проведений експеримент.
- Налаштування параметрів методів, що лежать в основі розробленого комплексного методу, для покращення процесу ідентифікації.

Беручи до уваги виокремлені вимоги до програмного забезпечення ідентифікації особи за зображенням обличчя, виділимо функціональні особливості створюваної програмної системи, які проілюстровані на діаграмах прецедентів на Рисунках 3.1-3.3.

Як видно з діаграми, основним актором є користувач, який взаємодіє із програмною системою. Під час використання програми користувач може обрати один з варіантів використання: здійснити ідентифікацію суб’єкта, переглянути попередні результати ідентифікації, переглянути записи бази даних, здійснити експериментальне дослідження комплексного методу біометричної ідентифікації або змінити його параметри.

Перед ініціюванням процесу ідентифікації, користувач має обрати зображення, на якому необхідно ідентифікувати суб’єкт. Зображення може бути завантажене або з пристрою, на якому функціонує програмне забезпечення, або захоплене з відеопотоку камери, що підключена до пристрою. Далі користувач запускає ідентифікаційний процес, після чого система обробляє зображення та повертає користувачу ідентифікатор суб’єкта або відображає відповідне повідомлення, якщо записів про суб’єкт ідентифікації не міститься в базі даних.

Наступний варіант використання користувачем програмної системи – це перегляд попередніх результатів ідентифікації. Користувач може переглянути список всіх результатів, які збережені в історії, або обрати для перегляду конкретний результат ідентифікації, який отримано раніше.

При перегляді записів бази даних користувачу надається можливість переглянути загальну інформацію про всі записи, що містяться в базі даних,

переглянути певне досьє конкретного суб’єкта з можливістю його редагувати або зареєструвати дані про новий суб’єкт у базі даних, зберігаючи цей запис.

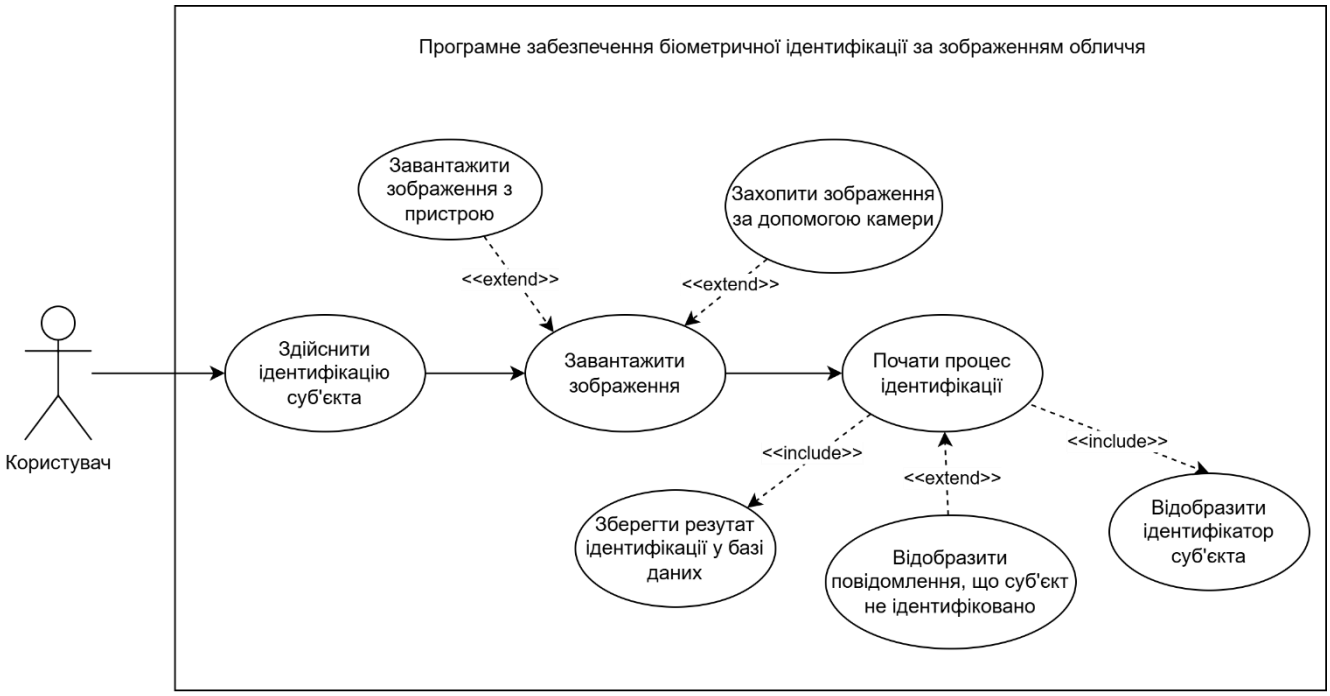


Рисунок 3.1 – Діаграма прецедентів використання програмного забезпечення для здійснення ідентифікації суб’єкта

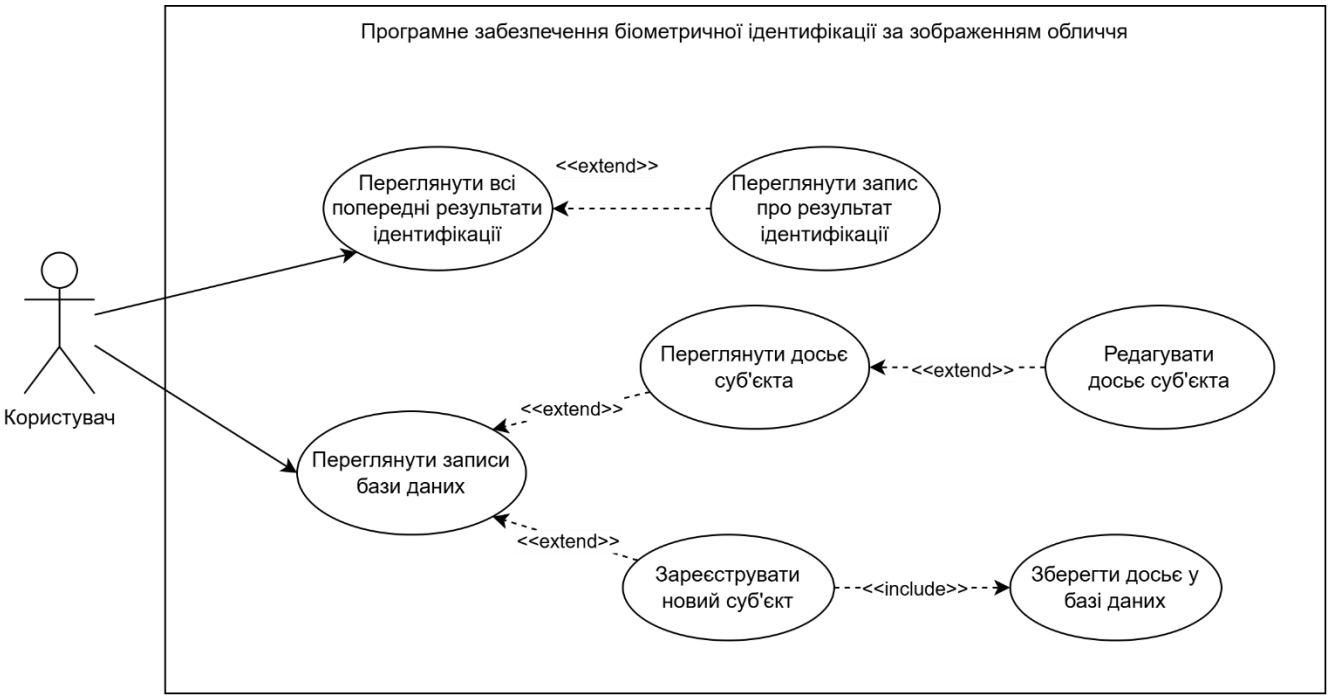


Рисунок 3.2 – Діаграма прецедентів використання програмного забезпечення для перегляду попередніх результатів ідентифікації та записів бази даних

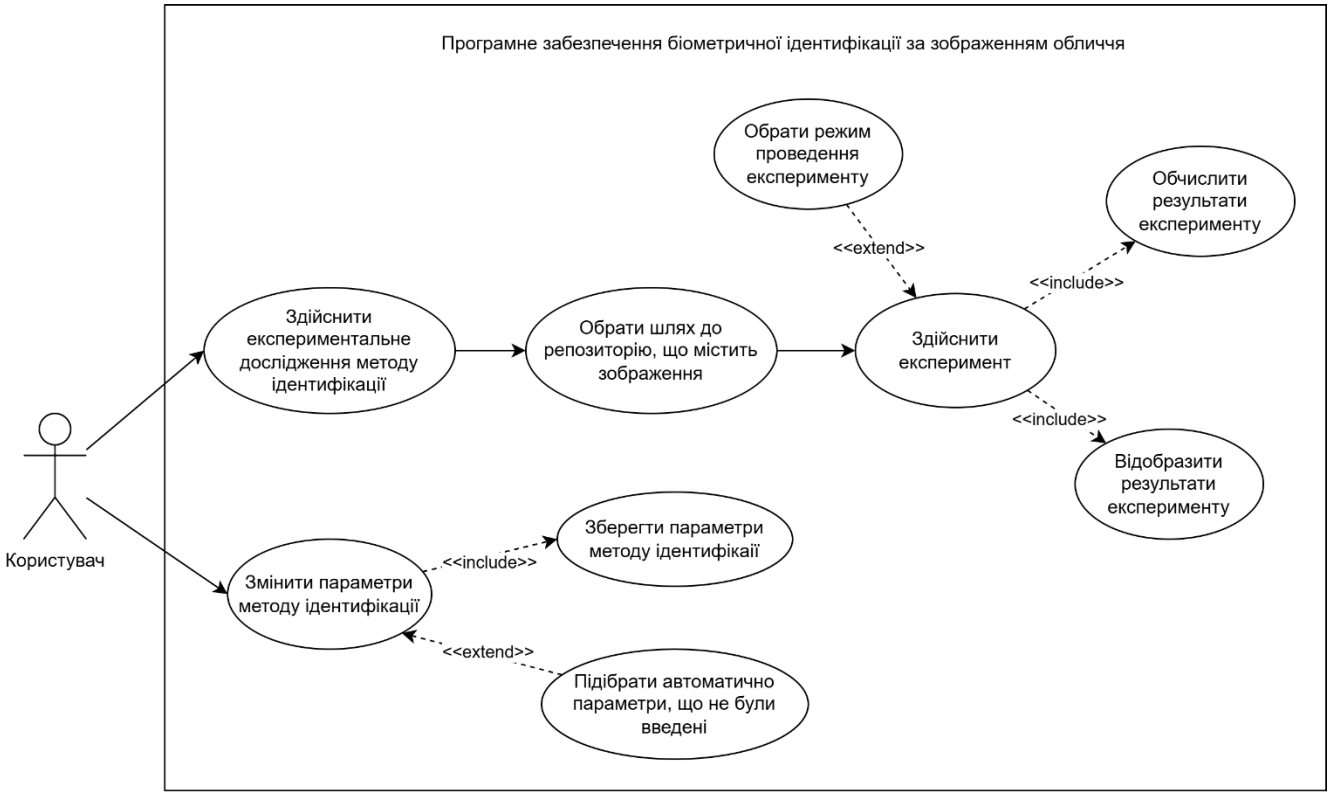


Рисунок 3.3 – Діаграма прецедентів використання програмного забезпечення для здійснення експериментального дослідження комплексного методу біометричної ідентифікації та зміни його параметрів

Здійснення експериментального дослідження комплексного методу біометричної ідентифікації вимагає від користувача надання шляху до репозиторію, що містить набір зображень, на яких необхідно ідентифікувати суб’єкти. Далі відбувається ініціація експерименту – кожне із зображень репозиторію обробляється за допомогою розробленого комплексного методу. За потреби користувач може обрати режим проведення експерименту для перевірки певних умов, за яких методу виконується більш або менш коректно, з метою покращення процесу ідентифікації. Результатом виконання експерименту є виведення програмою користувачу результатів ідентифікації по кожному із зображень, на яких проводилася ідентифікація.

Зміна параметрів методу передбачає введення користувачем значень параметрів для кожного з методів, що покладені в основу комплексного методу

біометричної ідентифікації. Ця функціональна особливість створена з метою перевірки ефективності методу та її покращення в майбутньому.

3.2 Сценарії функціонування програмної компоненти

Враховуючи дані аналізу варіантів використання, розглянемо сценарії функціонування програмної компоненти, тобто послідовність процесів, які виконуватимуться у створюваній програмі, та взаємодію між процесами та об’єктами програмного забезпечення.

Після початку роботи програми, користувачу надається можливість обрати дію, яку програма має виконати.

Для того, щоб ідентифікувати суб’єкт на зображенні, користувач завантажує зображення особи. Це зображення подається на вхід комплексного методу біометричної ідентифікації. Далі виконується процес локалізації області обличчя на зображенні. Зображення, що містить лише локалізовану область обличчя, передається на виконання наступному процесу – обробки зображення. На подальшому етапі виконання програми здійснюється формування вектору ознак зображення. Сформований вектор ознак використовується для класифікації зображення – відбувається порівняння отриманого вектору з векторами, що містяться в базі даних. Якщо вектор зображення вдалося класифікувати, програма надає користувачеві ідентифікатор суб’єкта, обличчя якого містилося на вхідному зображенні. В іншому випадку виводиться повідомлення про те, що суб’єкт не ідентифіковано, тобто дані про нього не містяться в базі даних.

При здійсненні експериментального дослідження програма запитує у користувача шлях до репозиторію, в якому містяться зображення, на яких потрібно виконати ідентифікацію суб’єктів, а також режим проведення експерименту для перевірки різних умов ідентифікації. Після цього запускається цикл перебору зображень, кожне з яких подається на вхід комплексного методу біометричної ідентифікації. Далі виконуються ті самі дії, що і при здійсненні ідентифікації на окремому зображенні. Після завершення циклу програма надає користувачеві

результати ідентифікатори суб’єктів, обличчя яких зафіксовані на кожному із оброблюваних зображень, або повідомлення, що суб’єкта не ідентифіковано.

Програмою передбачається налаштування комплексного методу біометричної ідентифікації, а саме введення значень параметрів методу. За умови, якщо користувачем введено значення не для всіх параметрів, програма автоматично обчислює та встановлює значення цих параметрів так, щоб метод залишався працездатним. Далі програма перевіряє введені користувачем або згенеровані автоматично дані. Якщо всі значення параметрів є валідними, вони зберігаються, або в іншому випадку програма здійснює запит до користувача на введення даних повторно.

Користувач також може здійснити перегляд попередніх результатів ідентифікації в узагальненому вигляді або обрати певний результат, який отримано внаслідок попередніх виконань програми.

Перегляд бази даних надає можливість користувачу переглянути узагальнену інформацію, що міститься в базі даних, або переглянути досьє окремого суб’єкта. При виконанні цієї дії також можливо здійснити реєстрацію нового суб’єкта для збереження інформації про нього у базі даних – користувач вводить дані про суб’єкт, після чого програма перевіряє валідність цих даних та зберігає їх за умови, що дані валідні, або в іншому випадку здійснює повторний запит до користувача на введення даних.

Діаграми діяльності, що детально демонструють послідовність виконання вище зазначених процесів і взаємодію між цими процесами та об’єктами програмної системи, зображена на Рисунках 3.4-3.8.

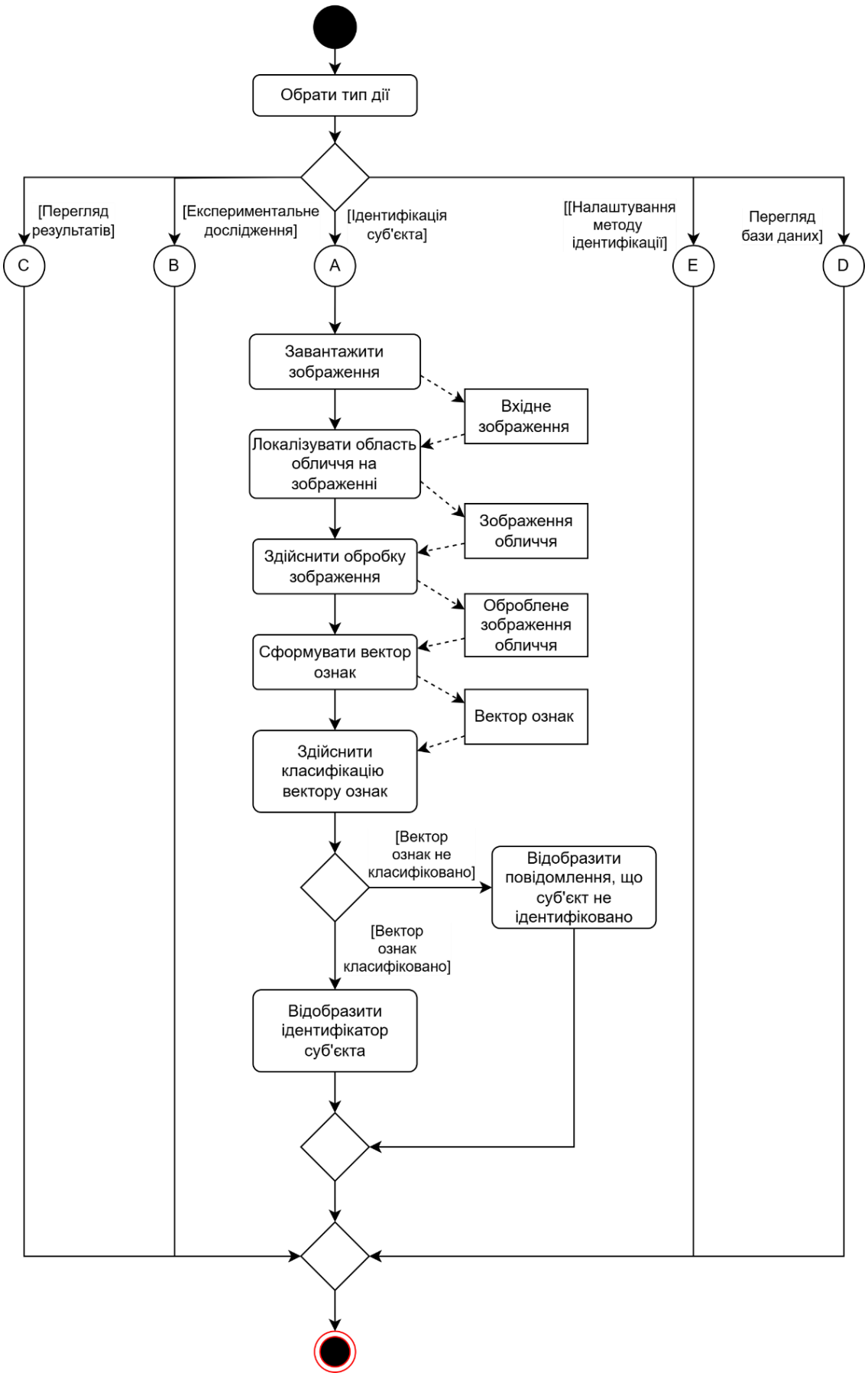


Рисунок 3.4 – Діаграма діяльності сценарію ідентифікації суб’єкта у програмній компоненті біометричної ідентифікації

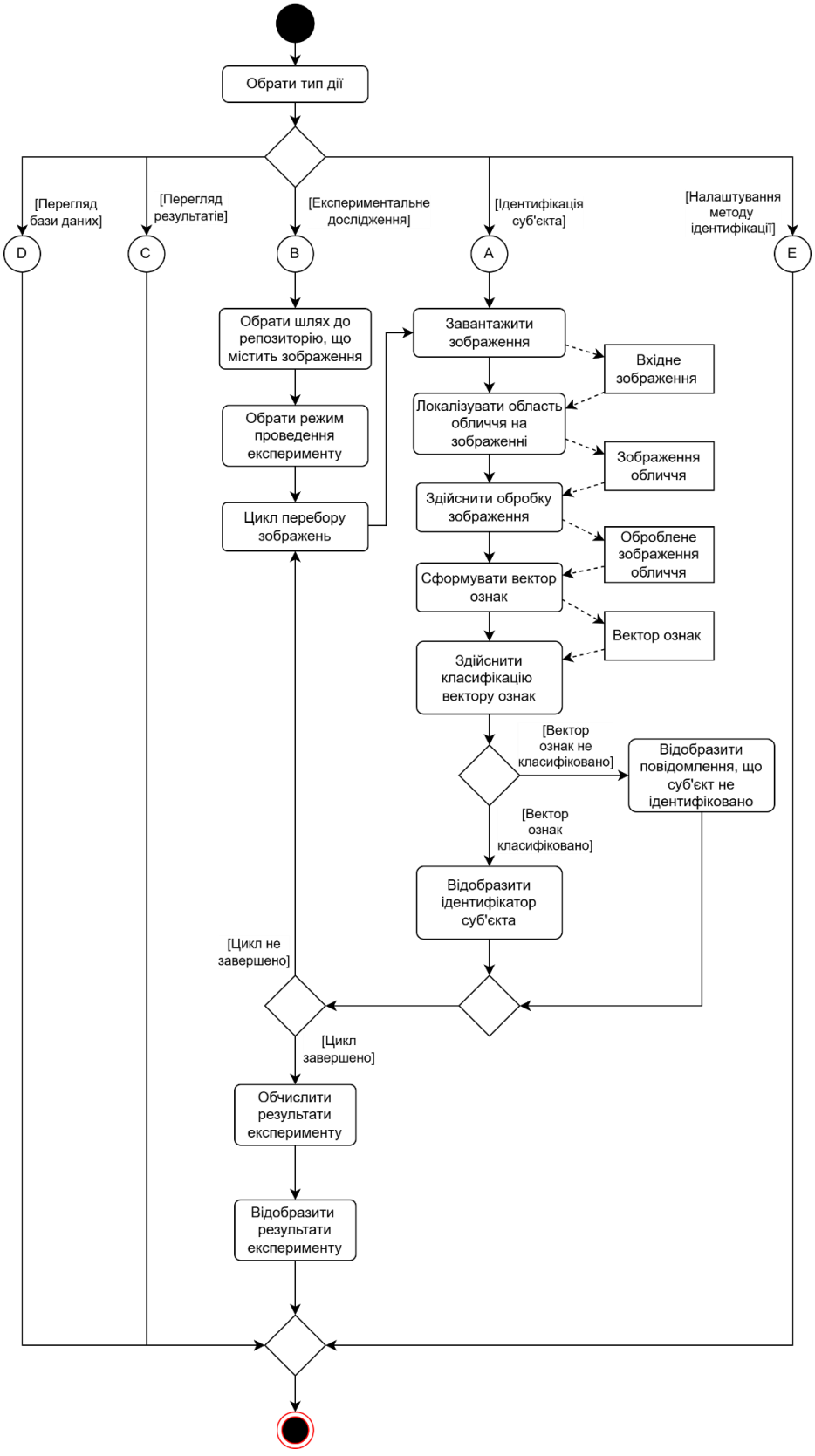


Рисунок 3.5 – Діаграма діяльності сценарію експериментального дослідження комплексного методу біометричної ідентифікації у програмній компоненті біометричної ідентифікації

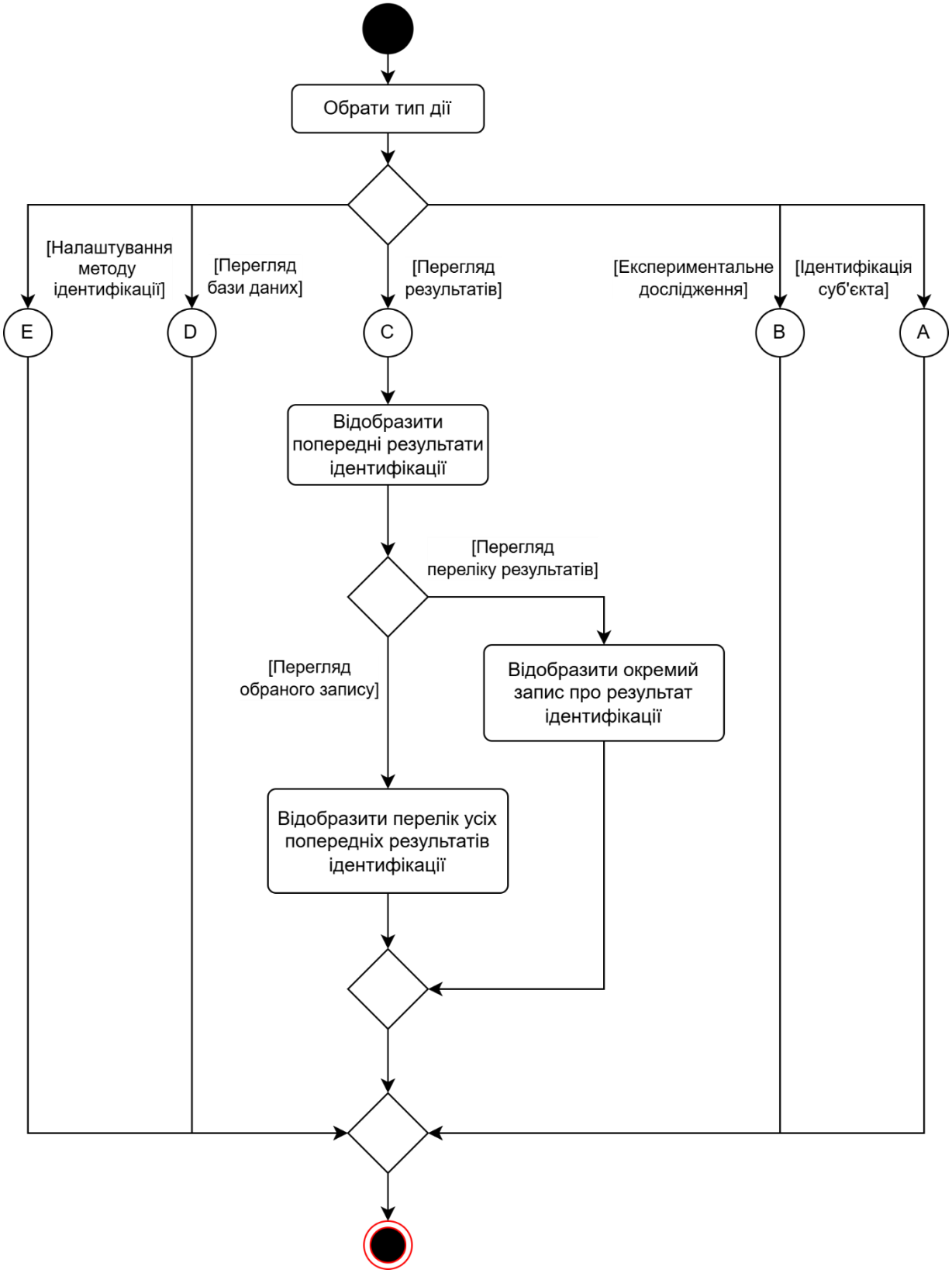


Рисунок 3.6 – Діаграма діяльності сценарію перегляду результатів ідентифікації у програмній компоненті біометричної ідентифікації

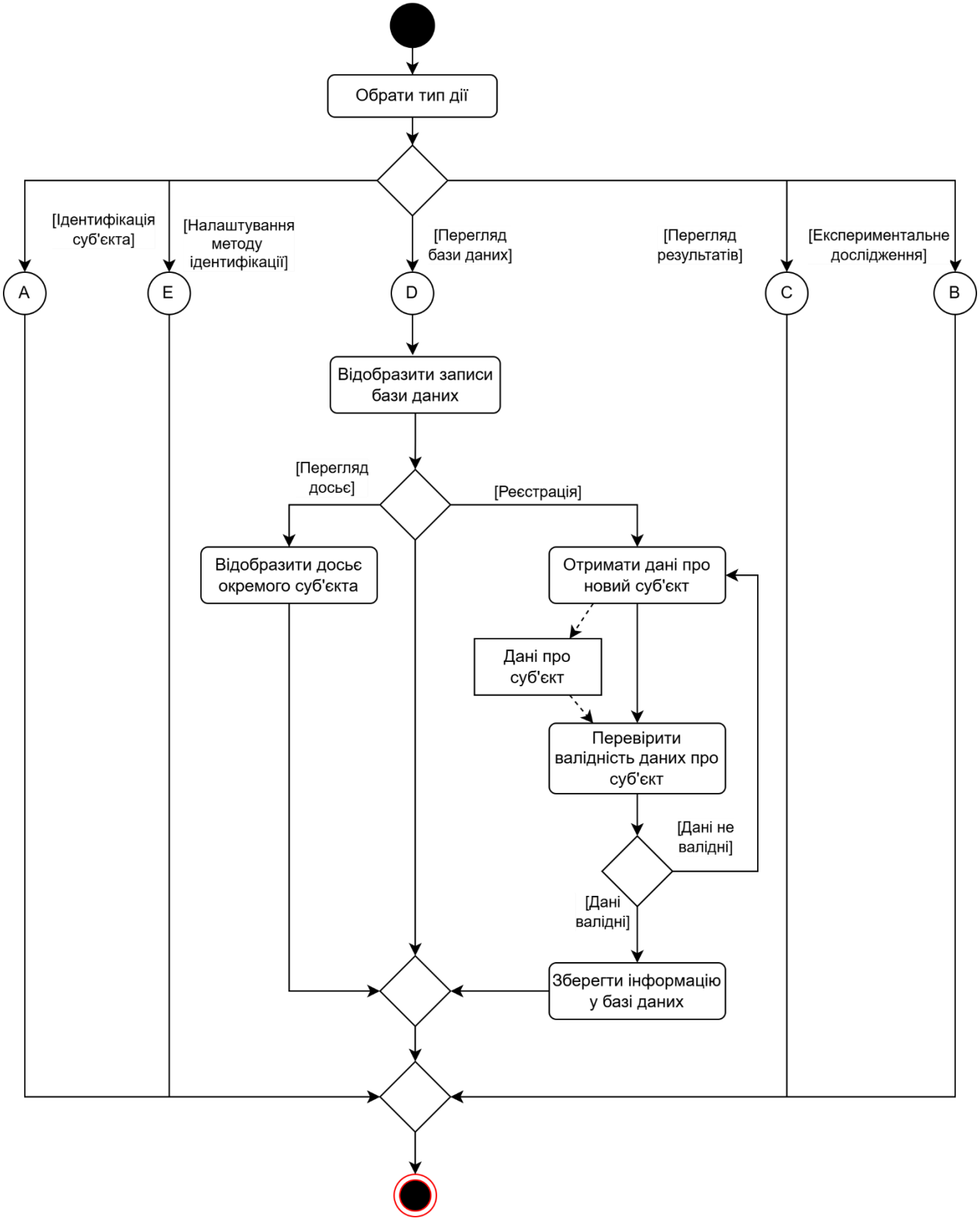


Рисунок 3.7 – Діаграма діяльності сценарію перегляду записів бази даних у програмній компоненті біометричної ідентифікації

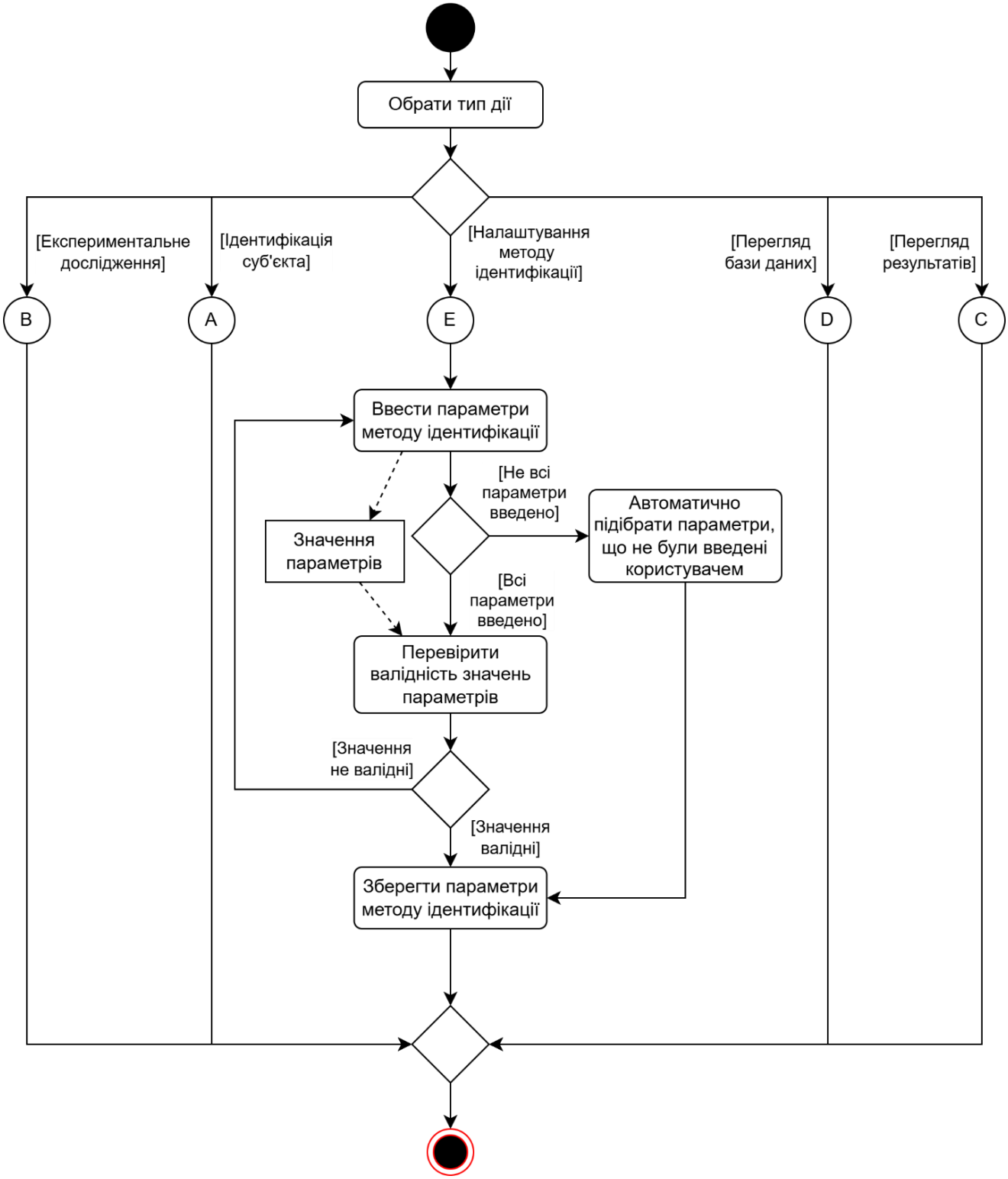


Рисунок 3.8 – Діаграма діяльності сценарію налаштування комплексного методу біометричної ідентифікації у програмній компоненті біометричної ідентифікації

3.3 Проєктування програмної компоненти комплексного методу біометричної ідентифікації

Оскільки основною метою програмного забезпечення є здійснення ідентифікації особи за зображенням обличчя, розглянемо більш детально основні складові програмної компоненти комплексного методу біометричної ідентифікації.

З огляду на функції та методи, що лежать в основі комплексного методу біометричної ідентифікації, концептуально комплексний метод біометричної ідентифікації можна поділити на такі компоненти:

- модуль отримання зображення;
- модуль локалізації обличчя на зображенні;
- модуль попередньої обробки зображення обличчя;
- модуль обробки зображення обличчя;
- модуль формування вектору ознак;
- модуль класифікації вектору ознак.

Модуль отримання зображення завантажує зображення з пристрою за шляхом, обраним користувачем, або з відеопотоку здійснює фіксацію зображення людини, на обличчя якої спрямовано камеру. Отримане зображення демонструється користувачеві, за необхідності перетворюється на зображення у відтінках сірого та передається на вхід модуля локалізації.

Модуль локалізації побудовано на основі методу Віола-Джонса на основі каскадів Гаара. Даний модуль виявляє на зображенні область, яка містить ознаки обличчя людини, та виконує перетворення зображення на таке, що містить лише обличчя, прибираючи зайві деталі або елементи фону. Якщо на зображенні не виявлено жодних ознак облич, модуль локалізації надає користувачеві відповідне повідомлення і подальше виконання комплексного методу біометричної ідентифікації припиняється. Блок-схема алгоритму виявлення обличчя на зображенні методом Віола-Джонса на основі каскадів Гаара представлена на Рисунку 3.9. Перетворене зображення, на якому міститься лише область обличчя, надходить на вхід модуля попередньої обробки.

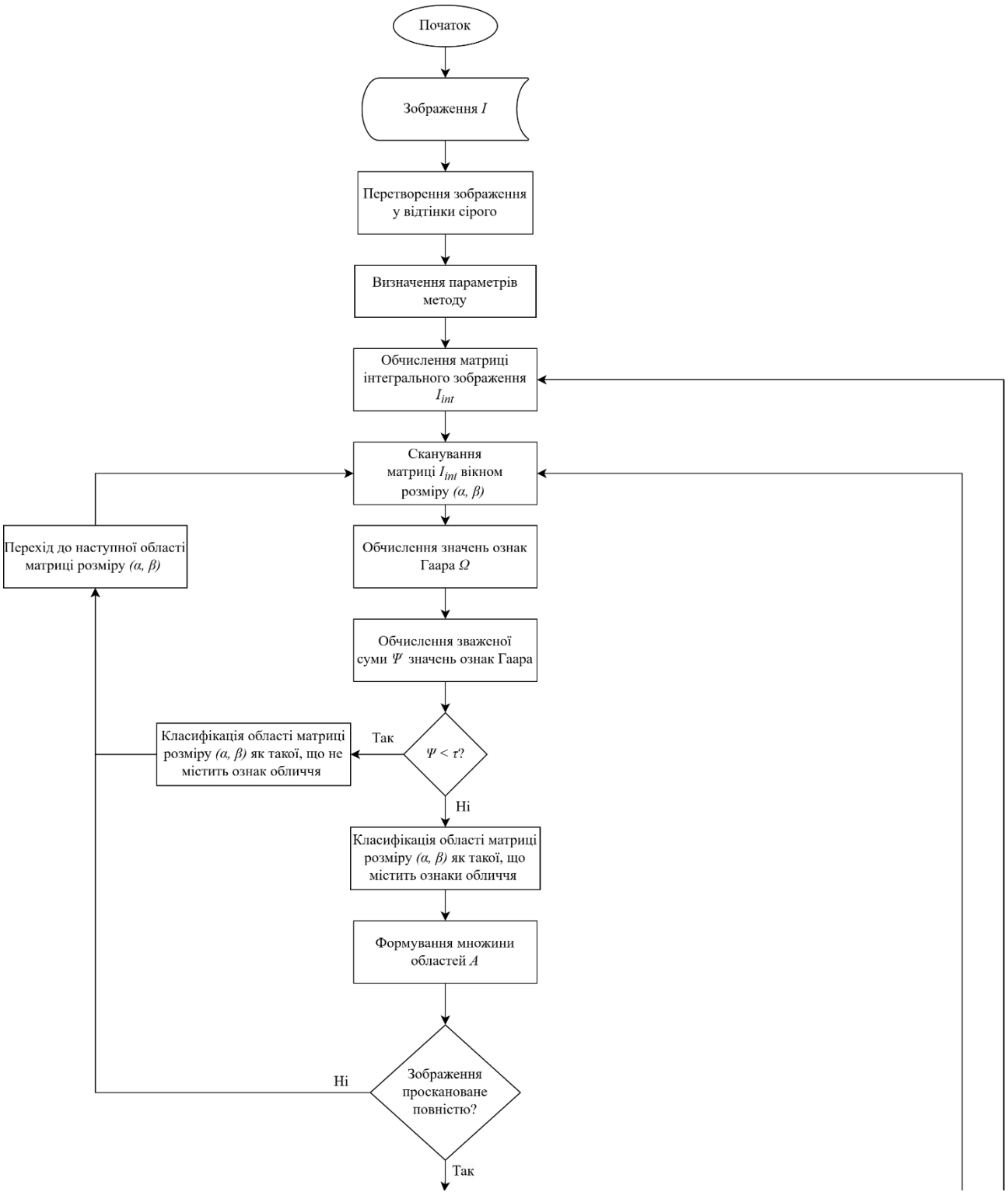


Рисунок 3.9 – Блок-схема алгоритму виявлення обличчя на зображенні методом Віола-Джонса на основі каскадів Гаара

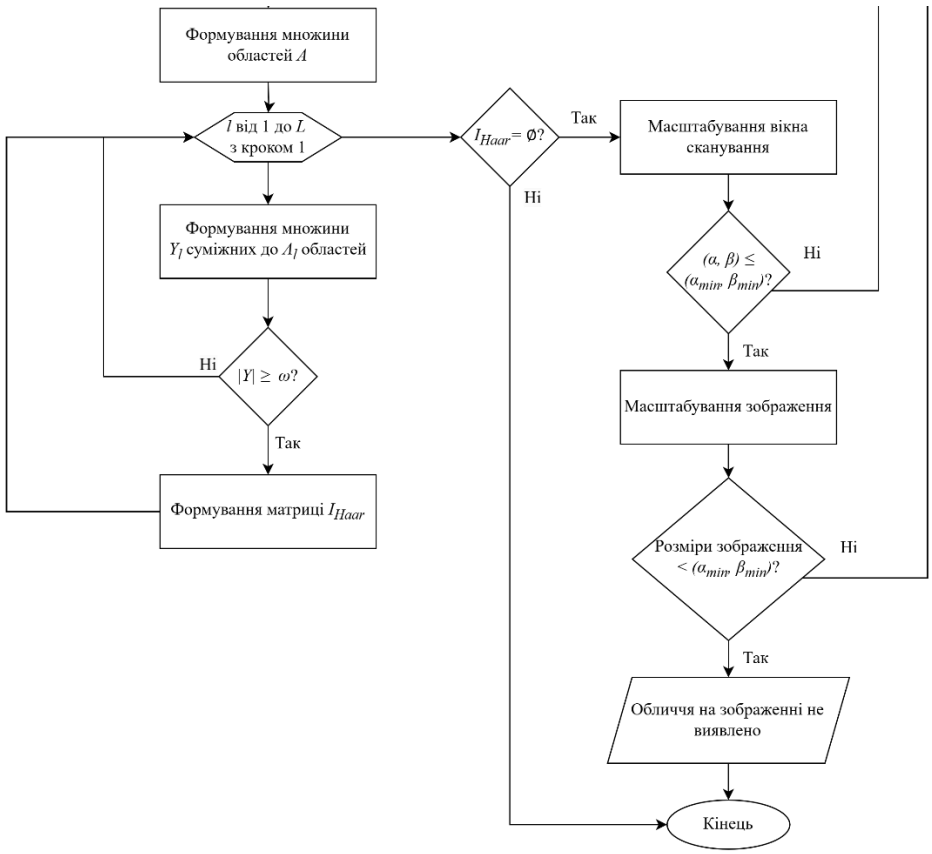


Рисунок 3.9 (продовження) – Блок-схема алгоритму виявлення обличчя на зображенні методом Віола-Джонса на основі каскадів Гаара

Модуль попередньої обробки застосовує до зображення обличчя метод анізотропної дифузії таким чином, щоб найбільш суттєві ознаки обличчя були більш видимими на зображенні. Блок-схема алгоритму попередньої обробки матриці зображення методом анізотропної дифузії представлена на Рисунку 3.10. Оброблене зображення передається в якості аргументу до модуля обробки зображення.

На початку роботи модуля обробки зображення генеруються фільтри Ґабора з різними параметрами вейвлет-функції. Далі кожен з цих фільтрів застосовується до вхідного зображення обличчя. Блок-схема алгоритму обробки матриці зображення методом вейвлет-перетворення Ґабора представлена на Рисунку 3.11.

Рисунок 3.10 – Блок-схема алгоритму обробки матриці зображення методом анізотропної дифузії

Рисунок 3.11 – Блок-схема алгоритму обробки матриці зображення методом вейвлет-перетворення Ґабора

Зображення, сформовані в результаті обробки зображення обличчя за допомогою вейвлет-перетворення, є вихідними об’єктами, до яких застосовуються функції модуля формування вектору ознак. Вектор ознак формується шляхом окремого застосування до вхідних зображень дескриптору локальних бінарних шаблонів в одновимірному просторі і дескриптору гістограм орієнтованих градієнтів. Блок-схеми методів вилучення векторів ознак представлені на Рисунках 3.12 і 3.13.

Далі вектори, сформовані в результаті роботи цих методів, нормалізуються з використанням мінімально-максимальної нормалізації та об’єднуються, утворюючи єдиний вектор ознак зображення.

Модуль класифікації отримує вектор ознак зображення обличчя та здійснює його порівняння з еталонними векторами ознак, які зберігаються в базі даних, що взаємодіє із програмним забезпеченням. Порівняння відбувається шляхом обчислення квадратичної відстані Евкліда між вхідним вектором і еталонними векторами.

Результатом роботи модуля є ідентифікатор суб’єкта, відстань до вектору ознак якого була найменшою. Якщо вектор не вдалося класифікувати, модуль класифікації надає користувачеві повідомлення про те, що суб’єкт ідентифікації не зареєстровано в базі даних.

Більш детально взаємозв’язок вищезазначених модулів представлено на діаграмі компонентів, що міститься на Рисунку 3.14.

Виходячи з призначення та функціональності модулів, які є складовими комплексного методу біометричної ідентифікації, виділимо основні методи, що використовуватимуться в кожному з визначених компонентів. Методи реалізації комплексного методу біометричної ідентифікації представлені у Таблиці 3.1, а взаємозв’язок класів, в яких реалізовані ці методи, зображено на Рисунку 3.15.

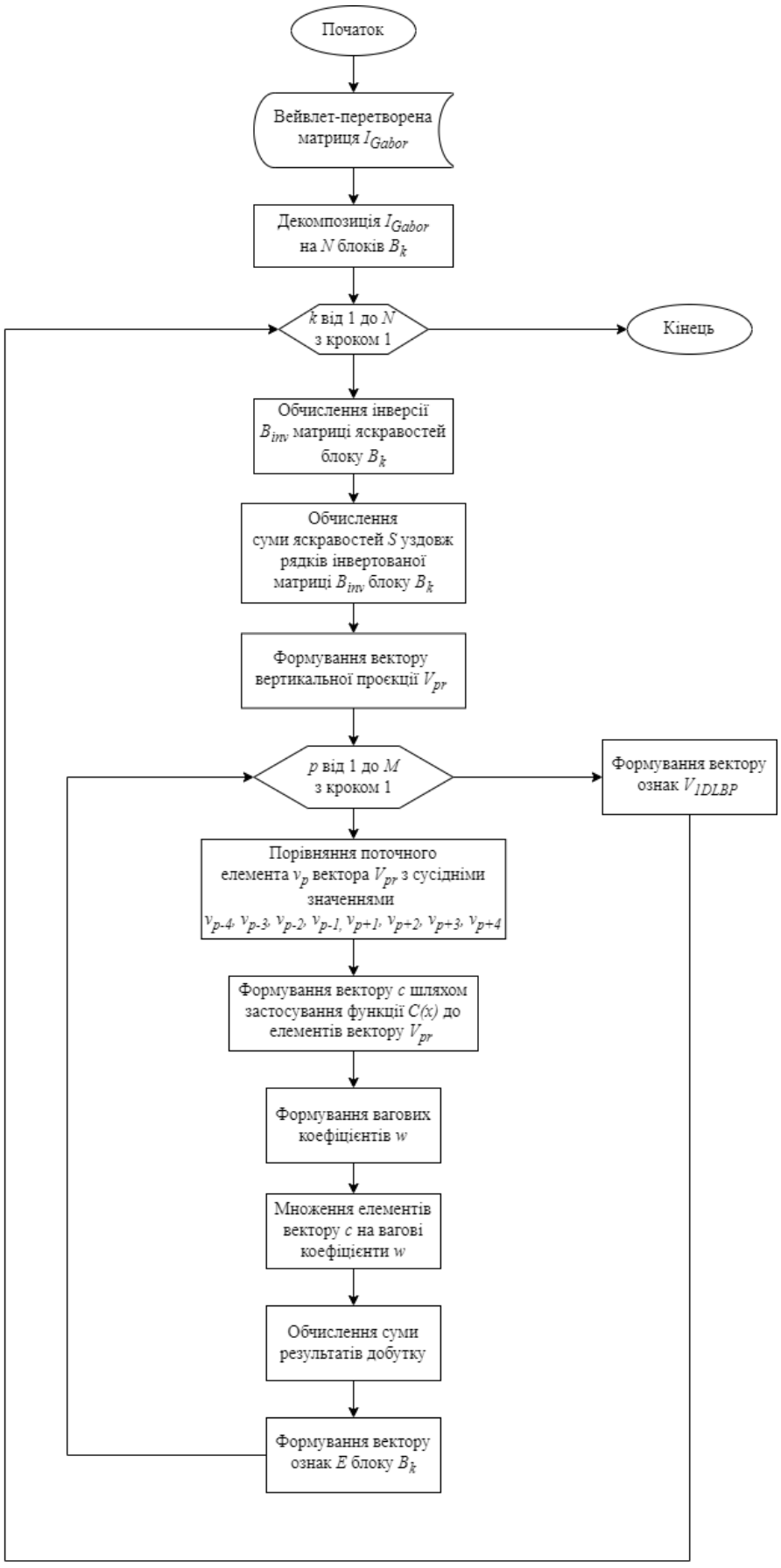


Рисунок 3.12 – Блок-схема алгоритму вилучення вектору ознак методом локальних бінарних шаблонів в одновимірному просторі (1DLBP)

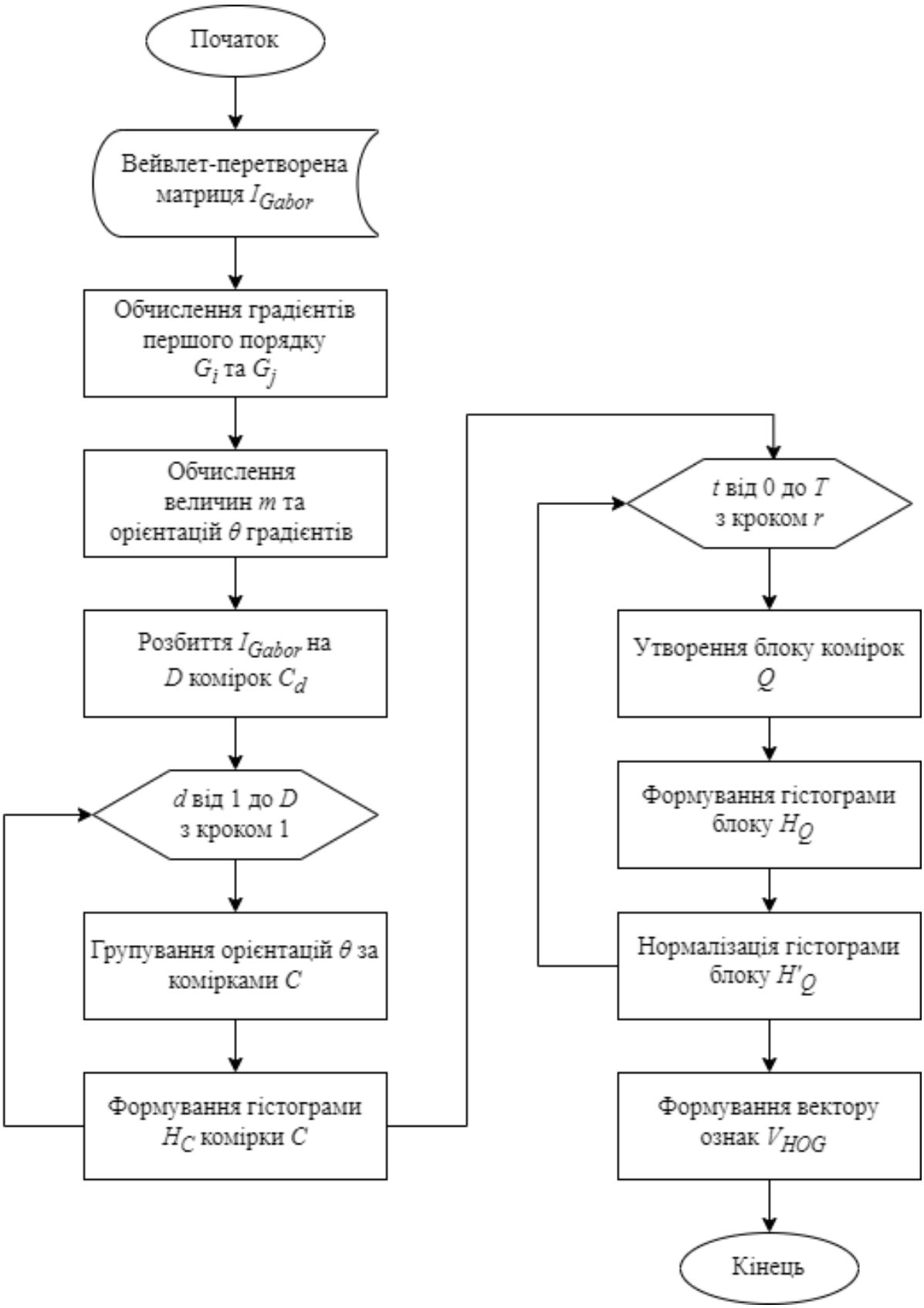


Рисунок 3.13 – Блок-схема алгоритму вилучення вектору ознак методом гістограм орієнтованих градієнтів (HOG)

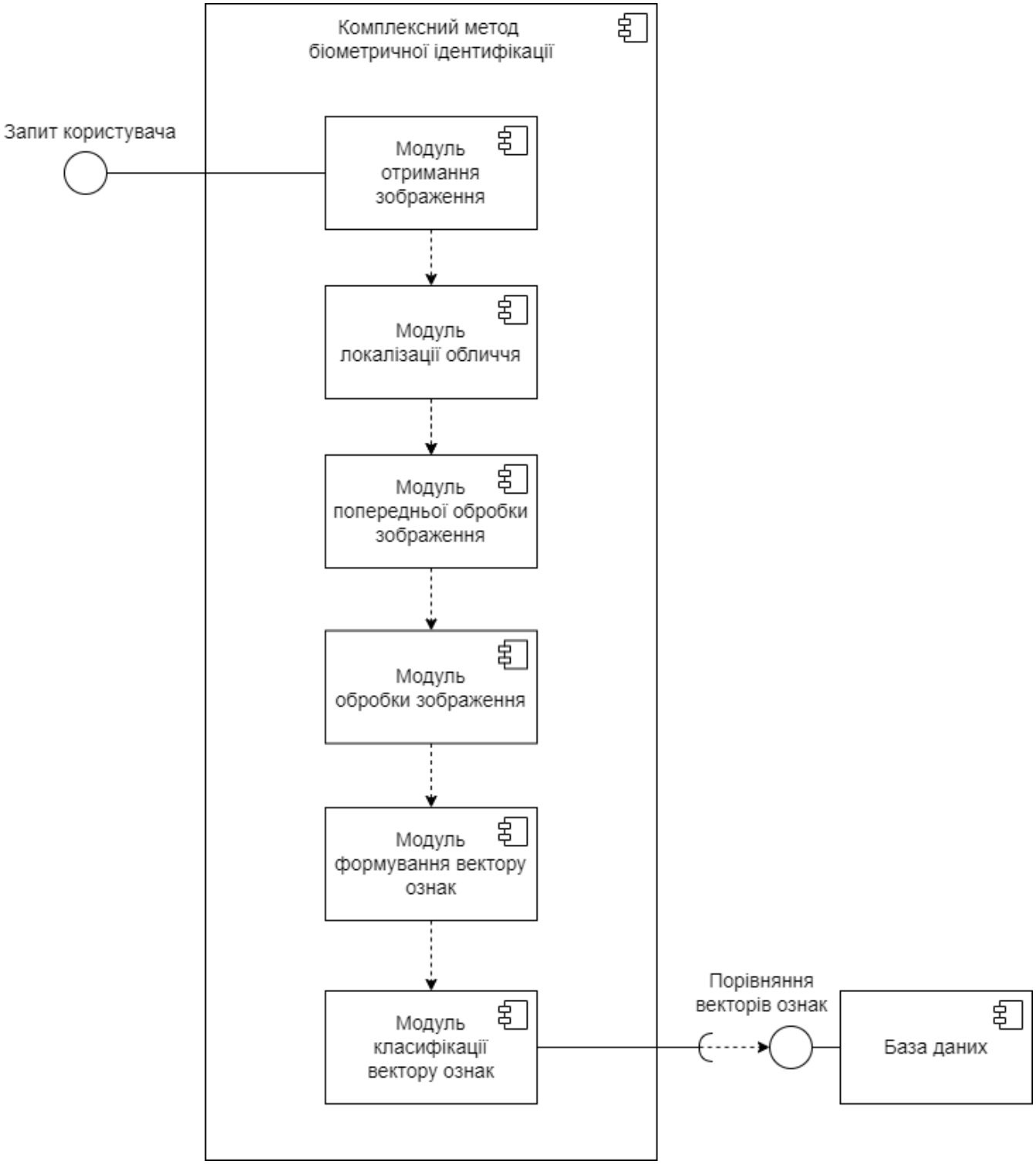


Рисунок 3.14 – Діаграма компонентів комплексного методу біометричної ідентифікації

Таким чином, комплексний метод біометричної ідентифікації на основі локально-текстурних дескрипторів є окремим й основним компонентом розроблюваного програмного забезпечення, з яким взаємодіють усі інші компоненти, що забезпечують додаткові функціональні можливості програми.

Таблиця 3.1 – Основні методи реалізації модулів комплексного методу біометричної ідентифікації

Модуль	Метод	Операція
Модуль отримання зображення	read_image()	Завантажує зображення, на якому необхідно ідентифікувати особу, з файлу, збереженого у пам’яті пристрою, шлях до якого вказано користувачем.
	capture_image()	Захоплює зображення, на якому необхідно ідентифікувати особу, з відеопотоку камери пристрою.
	show_image()	Відображає завантажене або захоплене зображення на екрані для перегляду користувачем.
	convert_to_grayscale()	Перетворює зображення у відтінки сірого, якщо подане на вхід модуля зображення є кольоровим. В іншому випадку перетворення не відбувається.

Продовження Таблиці 3.1

Модуль	Метод	Операція
Модуль локалізації обличчя на зображенні	detect_Haar_features()	Локалізує на зображенні область обличчя людини, використовуючи ознаки Гаара, та вилучає із зображення будь-які інші області, що не містять ознак обличчя. У випадку, якщо обличчя на зображенні локалізувати не вдалося, надає користувачу повідомлення про те, що облич на зображенні не знайдено, та припиняє виконання комплексного методу біометричної ідентифікації.
Модуль попередньої обробки зображення обличчя	apply_AD_filter()	Застосовує до зображення метод анізотропної дифузії, підсилюючи видимість рис обличчя.
Модуль обробки зображення обличчя	generate_Gabor_filters()	Генерує фільтри Ґабора з різною варіацією параметрів вейвлет-функції.
	apply_Gabor_filters()	Застосовує до зображення кожен зі згенерованих фільтрів Ґабора, формуючи послідовність вейвлет-перетворених зображень.
	form_global_image()	Формує глобальне зображення обличчя шляхом об’єднання усіх вейвлет-перетворених зображень.

Продовження Таблиці 3.1

Модуль	Метод	Операція
Модуль формування вектору ознак	extract_1DLBP_vector()	Вилучає із зображення вектор ознак шляхом застосування дескриптору локальних бінарних шаблонів в одновимірному просторі.
	extract_HOG_vector()	Вилучає із зображення вектор ознак шляхом застосування дескриптору гістограм орієнтованих градієнтів.
	normalize_vector()	Нормалізує вектори ознак шляхом застосування операції мінімально-максимальної нормалізації.
	form_feature_vector()	Формує глобальний вектор ознак шляхом об’єднання нормалізованих векторів ознак.
Модуль класифікації вектору ознак	get_db_vector ()	Отримує значення еталонних векторів ознак, збережених в базі даних.
	calculate_distance()	Обчислює квадратичну відстань Евкліда між сформованим глобальним вектором ознак і еталонними векторами, значення яких були отримані з бази даних.
	classify_feature_vector()	Класифікує вектор ознак шляхом визначення значення найменшої відстані та повертає значення ідентифікатора із бази даних. Якщо вектор ознак не вдалося класифікувати, надає користувачу повідомлення, що суб’єкт ідентифікації не зареєстровано в базі даних.

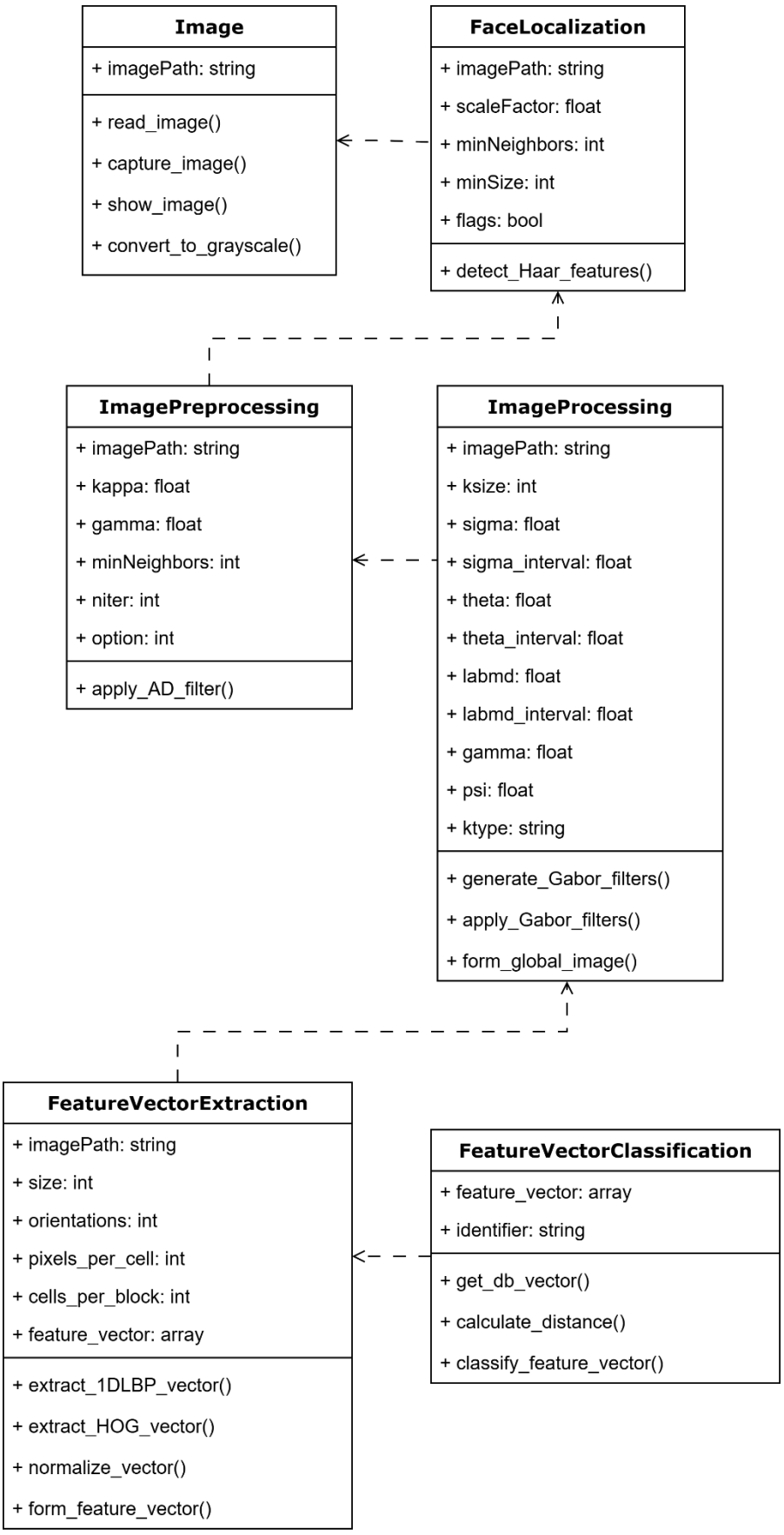


Рисунок 3.15 – Діаграма класів комплексного методу біометричної ідентифікації

3.4 Проєктування додаткових модулів програмної компоненти

Відповідно до результатів аналізу варіантів використання та моделювання процесів і даних, можна визначити компоненти програмного забезпечення, взаємозв'язок між якими представлено на Рисунку 3.16.

Рисунок 3.16 – Діаграма компонентів програмного забезпечення біометричної ідентифікації

Як вже зазначалося раніше, компонент, що реалізує комплексний метод біометричної ідентифікації, є основною складовою частиною програмного забезпечення. На використання функціональності цього компонента виконує запит компонент, в якому реалізована можливість проведення експериментального дослідження – застосування комплексного методу біометричної ідентифікації до набору зображень та використання результатів, що повертаються, для формування

результатів експериментів, а саме встановлення точності ідентифікації та формування візуальної інформації про результати роботи методу.

За необхідності здійснення налаштування параметрів комплексного методу біометричної ідентифікації, компонент, в якому він реалізований, виконує запит до компоненту, що реалізує в собі можливість введення параметрів комплексного методу біометричної ідентифікації користувачем або автоматичного розрахунку параметрів, значення для яких не встановлено.

Компонент бази даних отримує запити від компоненту, в якому реалізовано методі ідентифікації, на етапі здійснення класифікації вектору ознак, та повертає у відповідь результати класифікації – ідентифікатор суб'єкта; компоненти, що реалізують в собі функціональність для перегляду бази даних і перегляду результатів ідентифікації здійснюють запити до відповідних сутностей бази даних, що містять запитувану інформацію, та повертають результати запитів.

Основні методи реалізації компонентів програмного забезпечення біометричної ідентифікації наведено у Таблиці 3.2 та на Рисунку 3.17.

Таблиця 3.2 – Основні методи додаткових функціональних можливостей програмного забезпечення біометричної ідентифікації

Модуль	Метод	Операція
Експериментальне дослідження	select_db()	Дозволяє користувачу обрати шлях до репозиторію, що містить набір зображень, до яких необхідно застосувати метод ідентифікації, або шляхи до декількох таких репозиторіїв.
	set_mode()	Дозволяє користувачу обрати режим проведення експериментального дослідження на наборі зображень, який обрано користувачем.

Продовження Таблиці 3.2

	start_experiment()	Створює цикл перебору зображень в репозиторіях, які обрано користувачем, та застосовує комплексний метод біометричної ідентифікації до кожного зображення. Створює набір ідентифікаторів, які отримано в результаті роботи методу.
	calculate_results()	Порівнює набір ідентифікаторів, отриманих в результаті проведення експериментального дослідження на заданому наборі зображень, з очікуваними результатами. Обчислює показники точності ідентифікації методу для кожного обраного набору даних.
	display_results()	Формує та відображає користувачу числову та графічну інформацію про результати, отримані під час проведення експериментального дослідження.
Налаштування параметрів комплексного методу біометричної ідентифікації	get_params()	Надає користувачу можливість ввести дані щодо параметрів методів, покладених в основу комплексного методу біометричної ідентифікації.

Продовження Таблиці 3.2

Налаштування параметрів комплексного методу біометричної ідентифікації	save_params()	Зберігає надані користувачем параметри методів, покладених в основу комплексного методу біометричної ідентифікації.
	check_params()	Перевіряє коректність введених користувачем параметрів комплексного методу біометричної ідентифікації. Якщо введені дані не відповідають очікуваним, повідомляє користувача про помилку та надає можливість ввести дані повторно. У випадку, якщо певні дані не були введені, обчислює значення параметрів, область введення для яких залишилися порожньою, у відповідності за значенням до введених даних для досягнення найбільшої точності ідентифікації методом.
	set_Haar _params()	Встановлює значення параметрів методу локалізації обличчя на зображенні на основі ознак Гаара.
	set_AD_params()	Встановлює значення параметрів методу анізотропної дифузії для попередньої обробки зображення обличчя.

Продовження Таблиці 3.2

	set_Gabor_params()	Встановлює значення параметрів фільтрів Ґабора для обробки зображення обличчя.
	set_1DLBP_params()	Встановлює значення параметрів методу на основі дескриптора локальних бінарних шаблонів в одновимірному просторі для вилучення вектору ознак із зображення обличчя.
	set_HOG_params()	Встановлює значення параметрів методу на основі дескриптора гістограм орієнтованих градієнтів для вилучення вектору ознак із зображення обличчя.
Перегляд бази даних	search_subject()	Здійснює пошук записів в базі даних за запитом, який задано користувачем, та відображає отримані результати пошуку.
	register_subject()	Генерує користувачу форму для введення персональних даних про суб’єкт.

Продовження Таблиці 3.2

	upload_images()	Завантажує зображення суб’єкта реєстрації за шляхом, який надано користувачем.
	save_subject()	Зберігає дані про суб’єкт реєстрації в базі даних.
	check_data()	Перевіряє коректність введених користувачем даних про суб’єкт. Якщо введені дані не відповідають очікуваним, повідомляє користувача про помилку та надає можливість ввести дані повторно. У випадку, якщо певні дані не були введені, встановлює значення даних, область введення для яких залишилася порожньою, як невідоме значення (unknown).
	view_dossier()	Виводить дані про обраний користувачем суб’єкт, зареєстрований в базі даних.
Перегляд результатів ідентифікації	display_logs()	Здійснює запит до бази даних про збережені результати роботи комплексного методу біометричної ідентифікації та відображає їх.
	filter_logs()	Здійснює фільтрацію попередніх результатів роботи комплексного методу та відображає дані, що відповідають заданому параметру фільтрації.

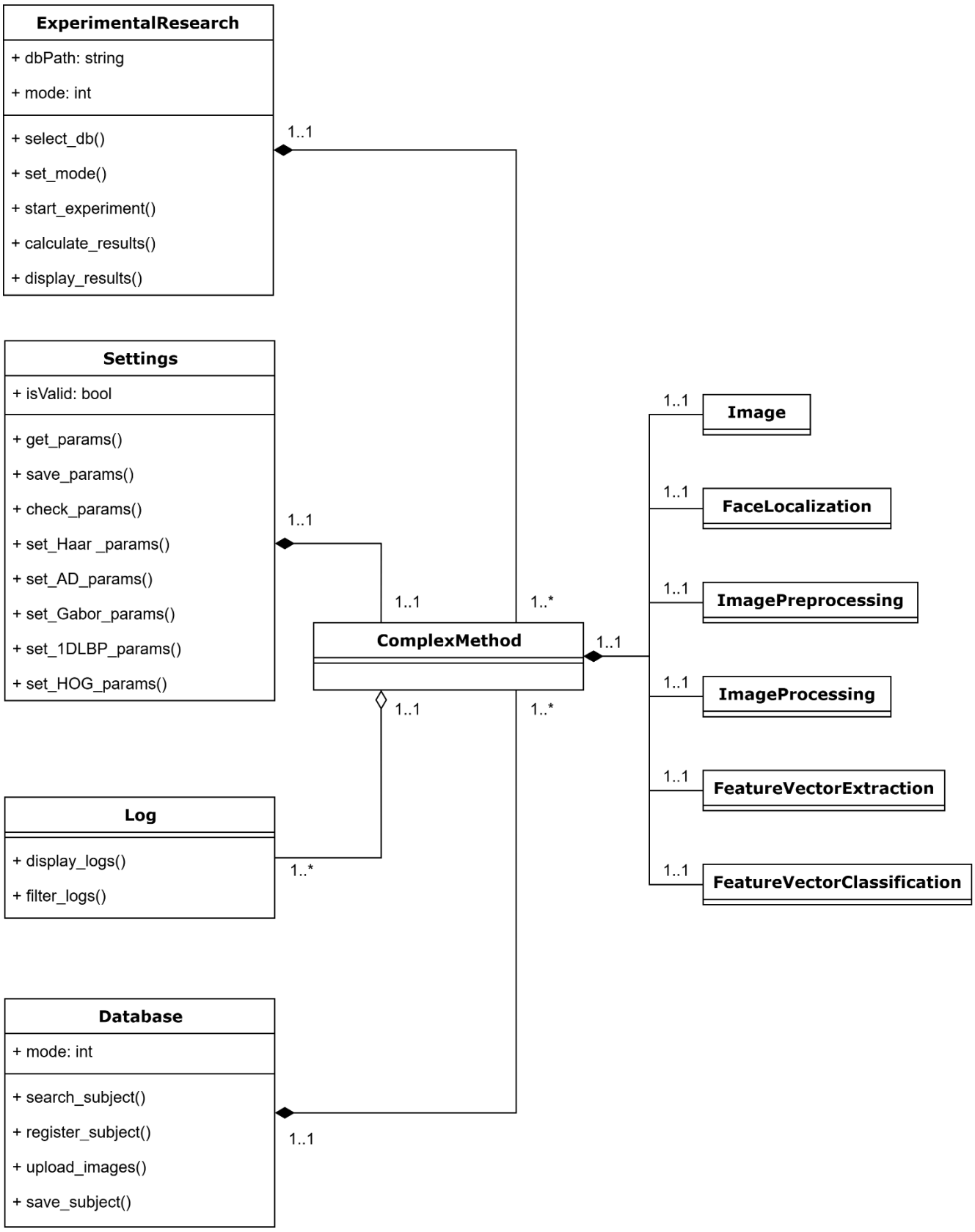


Рисунок 3.17 – Діаграма класів програмного забезпечення біометричної ідентифікації

Оскільки в програмному забезпеченні, що розробляється, база даних відіграє критичну роль у забезпеченні процесу ідентифікації, розглянемо більш детально особливості цього компоненту та питання інформаційного забезпечення програмної системи в цілому.

3.5 Вимоги до інформаційного забезпечення

Програмне забезпечення біометричної ідентифікації за зображенням обличчя спроєктовано таким чином, що для здійснення процесу ідентифікації необхідна наявність еталонних біометричних шаблонів, з якими відбуватиметься порівняння вектору ознак суб'єкта ідентифікації, сформованого в результаті роботи комплексного методу біометричної ідентифікації на етапі вилучення вектору ознак. Таким чином, програмне забезпечення має взаємодіяти з базою даних, що зберігатиме вектори ознак зареєстрованих суб'єктів.

Для забезпечення функціонування комплексного методу біометричної ідентифікації достатньо зберігати в базі даних ідентифікатори суб'єктів і вектори ознак зображень, що належать цим суб'єктам. При цьому одному суб'єкту можуть належати декілька векторів ознак, відповідно декілька записів у таблиці, якщо при реєстрації суб'єкта програмному забезпеченню користувачем надано декілька зображень. Приклад таблиці бази даних, необхідної для мінімального функціонування програмного забезпечення, наведено на Рисунку 3.18.

feature_vectors	
PK	id
FK	subject_id
	feature_vector

feature_vectors		
id	subject_id	feature vector
...	...	...
14092	e4df24175d4e474eabe2dcfc14745d96	[0.92281142 0.8970819 0.8920615 ... 0.46518134 0.52362141 0.60166699]
...	...	...
341302	d52be9f29866477195be34ba35f98184	[0.86220096 0.83795853 0.82583732 ... 0.15819893 0.20703315 0.53233095]
...	...	...
511781	82a3cf249fff48c6aa6d8243914780ab	[0.8119403 0.86932007 0.86069652 ... 0.15644595 0.16784498 0.31412166]
...	...	...

Рисунок 3.18 – Сутність бази даних для збереження векторів ознак та приклад її вмісту

Використання додаткових можливостей програмного забезпечення, що розробляється, також вимагає збереження певних даних. Зокрема, під час здійснення реєстрації суб'єктів користувачем програмного забезпечення може бути необхідним внесення про суб'єкт даних, що відносяться до категорії персональних даних та дозволяють більш точно визначити особу суб'єкта ідентифікації. Такими даними можуть бути ім'я суб'єкта, адреса його реєстрації, паспортні дані, ідентифікаційний номер платника податків та еталонне зображення, наприклад, фотозображення із паспорту. За необхідності, перелік ідентифікаційних даних може бути розширеним у залежності від потреб користувача програмного забезпечення. Також під час реєстрації нового суб'єкта користувач має обрати одне або декілька зображень цього суб'єкта, після чого формуються вектори ознак цих зображень, які згодом зберігаються у базі даних. Для кожного вектору ознак формується окремий запис в таблиці бази даних. Відповідно, суб'єкт з одним і тим самим ідентифікатором може мати декілька векторів ознак.

Також збереження даних вимагає функціональність програмного забезпечення, пов'язана з переглядом попередніх результатів ідентифікації, тобто фактично попередня історія виконання процесу ідентифікації. При цьому зберігається зображення, подане на вхід комплексного методу біометричної ідентифікації, а також результат роботи методу, тобто ідентифікатор суб'єкта, обличчя якого міститься на зображенні. Програмою може бути ідентифікований один і той самий суб'єкт при застосуванні комплексного методу біометричної ідентифікації до різних зображень при різних запусках програми, тому в таблиці попередніх результатів може декілька разів міститися один і той самий ідентифікатор суб'єкта з різними даними про результати ідентифікації.

Опис сутностей бази даних та їх атрибутів наведено у Таблиці 3.3.

Таблиця 3.3 – Опис сутностей бази даних та їх атрибутів

Назва сутності	Назва атрибута	Призначення	Тип даних
feature_vectors	fv_id	Первинний ключ	Лічильник, велике ціле
	subject_id	Зовнішній ключ, ідентифікатор суб’єкта	Рядок, що є хеш-кодом вектору ознак
	feature_vector	Шлях до файлу, що містить вектор ознак	Рядок довжиною до 100 символів
subjects	subject_id	Первинний ключ, ідентифікатор суб’єкта	Рядок, що є хеш-кодом вектору ознак
	name	Ім’я суб’єкта	Рядок довжиною до 60 символів
	address	Адреса	Рядок довжиною до 60 символів
	passport	Паспортні дані	Рядок довжиною до 20 символів
	TIN	Ідентифікаційний номер	Рядок довжиною до 10 символів
	image	Шлях до фотографічного зображення	Рядок довжиною до 60 символів

Продовження Таблиці 3.3

logs	log_id	Первинний ключ	Лічильник, мале ціле
	subject_id	Зовнішній ключ, ідентифікатор суб’єкта	Рядок, що є хеш-кодом вектору ознак
	image	Шлях до зображення обличчя, яке подавалося на вхід комплексного методу біометричної ідентифікації	Рядок довжиною до 60 символів
	result	Результат ідентифікації	Рядок довжиною до 10 символів

Під час проєктування програмної компоненти біометричної ідентифікації було враховано необхідність її інтеграції до складу вже існуючих інформаційних систем. У зв’язку з цим створення окремої автономної бази даних є недоцільним, оскільки розроблена компонента орієнтована на використання наявної інфраструктури зберігання даних. Архітектурні рішення, закладені в основу розробки, забезпечують сумісність з існуючими структурами баз даних, що дозволяє безпосередньо впроваджувати механізми збереження, доступу та обробки біометричної інформації. Такий підхід сприяє оптимізації ресурсів, збереженню цілісності даних і забезпеченню безперервної взаємодії між усіма функціональними модулями системи.

Розглянемо докладніше засоби реалізації компонентів програмного забезпечення ідентифікації особи та бази даних, що забезпечує їх функціонування.

3.6 Реалізація програмного забезпечення

Оскільки сфера застосування програмного забезпечення ідентифікації особи за зображенням обличчя охоплює різноманітні галузі, такі як безпека, банківська справа, роздрібна торгівля та багато інших, важливо розробити універсальну і доступну програму, що реалізує метод ідентифікації. У зв'язку з цим прийнято рішення здійснити розробку програмного забезпечення у вигляді вебзастосунку, що дозволить забезпечити його доступність та легкість використання на різних пристроях та платформах. Вебзастосунок надає можливість використовувати програмне забезпечення безпосередньо через веббраузер, що робить його доступним для широкого кола користувачів. Завдяки цьому не потрібно встановлювати додаткове програмне забезпечення на конкретному пристрої, що значно спрощує процес впровадження та підтримки програми. Вебзастосунок може бути використаний на різних типах пристроїв, зокрема на персональних комп'ютерах, ноутбуках, смартфонах, планшетах та інших мобільних пристроях. Це робить програмне забезпечення біометричної ідентифікації за зображенням обличчя більш гнучким та універсальним рішенням для користувачів, які працюють на різних платформах та в умовах, де доступність та мобільність є ключовими факторами.

Програмне забезпечення ідентифікації особи засноване на клієнт-серверній архітектурі. Клієнтська частина програмного забезпечення реалізована у вигляді вебінтерфейсу, який надає зручні засоби взаємодії з користувачем. Цей інтерфейс взаємодіє з сервером, передаючи запити користувача на сервер та отримуючи повідомлення про результати виконання цих запитів. Серверна частина програмного забезпечення ідентифікації особи відповідає за обробку запитів користувача та виконання методу біометричної ідентифікації на наданих зображеннях облич. Зокрема, серверна частина взаємодіє з базою даних при виконанні запитів на збереження наданих користувачем даних в базі, отримання даних за запитами, а також при виконанні комплексного методу біометричної ідентифікації на етапі класифікації вектору ознак.

Переваги такого підходу включають розділення функціональності між клієнтом та сервером, що спрощує розробку та підтримку програмного забезпечення, а також забезпечує надійність та безпеку обробки даних. Крім того, використання клієнт-серверної архітектури дозволяє легко масштабувати систему та забезпечувати швидку реакцію на зміни вимог до програмного забезпечення.

Приклад взаємодії архітектурних компонентів програмного забезпечення біометричної ідентифікації наведено на Рисунку 3.19. Користувач, взаємодіючи з інтерфейсом програми, що представляє собою клієнтську частину програмного забезпечення, завантажує або здійснює захоплення за допомогою камери зображення, на якому необхідно ідентифікувати суб'єкт, та запускає процес ідентифікації. Вхідне зображення передається на сервер, що містить реалізований метод ідентифікації. Далі послідовно виконуються методи, що лежать в основі реалізованого комплексного методу біометричної ідентифікації. На етапі класифікації вектору ознак, вилученого із поданого на вхід комплексного методу біометричної ідентифікації зображення, сервер робить запит до бази даних на отримання еталонних векторів ознак, з якими необхідно здійснити порівняння. По завершенню класифікації, сервер надсилає у відповідь клієнту зображення та ідентифікатор суб'єкта, якого ідентифіковано на вхідному зображенні.

Для реалізації компонентів клієнтської частини програмного забезпечення ідентифікації особи за зображенням обличчя використано поєднання технологій HTML (HyperText Markup Language), CSS (Cascading Style Sheets) та JavaScript.

Реалізацію серверної частини програмного забезпечення біометричної ідентифікації за зображенням обличчя виконано мовою програмування Python. Зокрема, для реалізації комплексного методу біометричної ідентифікації, що лежить в основі програмного забезпечення, були використані такі бібліотеки для обробки зображень та візуалізації даних, як OpenCV, NumPy та Matplotlib.

Для забезпечення зберігання та отримання доступу до даних, з якими взаємодіє програмне забезпечення ідентифікації особи, обрано систему управління базами даних MySQL.

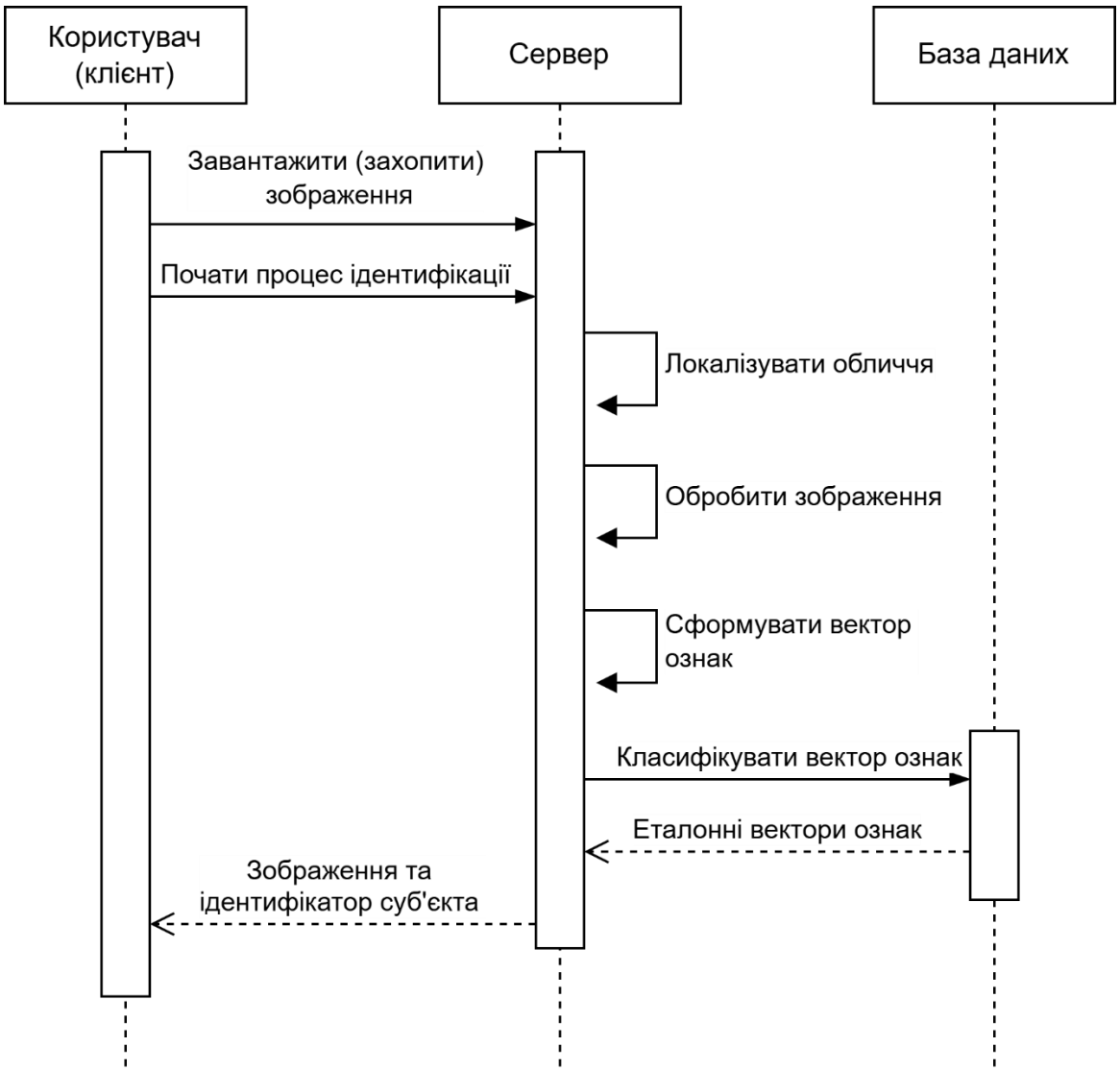


Рисунок 3.19 – Діаграма послідовності виконання комплексного методу біометричної ідентифікації

Використовуючи вищезгадані технології розроблено програмну компоненту рішення задачі біометричної ідентифікації за зображенням обличчя у вигляді вебзастосунку, який складається з таких основних фреймів:

- Home – головна сторінка застосунку.
- Identification – призначений для здійснення ідентифікації особи на зображенні або відео, що завантажене користувачем, використовуючи розроблений комплексний метод.
- Database – надає можливість переглядати вміст бази даних.

- Experiments – призначений для здійснення експериментальних досліджень комплексного методу біометричної ідентифікації на наборах зображень облич з виведенням графічної інформації про результати експериментів.
- Logs – надає можливість переглядати збережені попередні результати роботи комплексного методу біометричної ідентифікації.
- Settings – надає можливість змінювати налаштування параметрів комплексного методу біометричної ідентифікації.
- FAQ – містить інструкції для користувача за прогнозовано найбільш поширеними питаннями.

Розглянемо більш детально основні фрейми розробленого програмного забезпечення.

На Рисунку 3.20 представлено фрейм Home, що є головною сторінкою та відправною точкою роботи вебзастосунку, тобто першою сторінкою, яку бачить користувач після запуску програми на виконання. Даний фрейм містить привітальне повідомлення для користувача та кнопки переходу на всі інші фрейми застосунку.

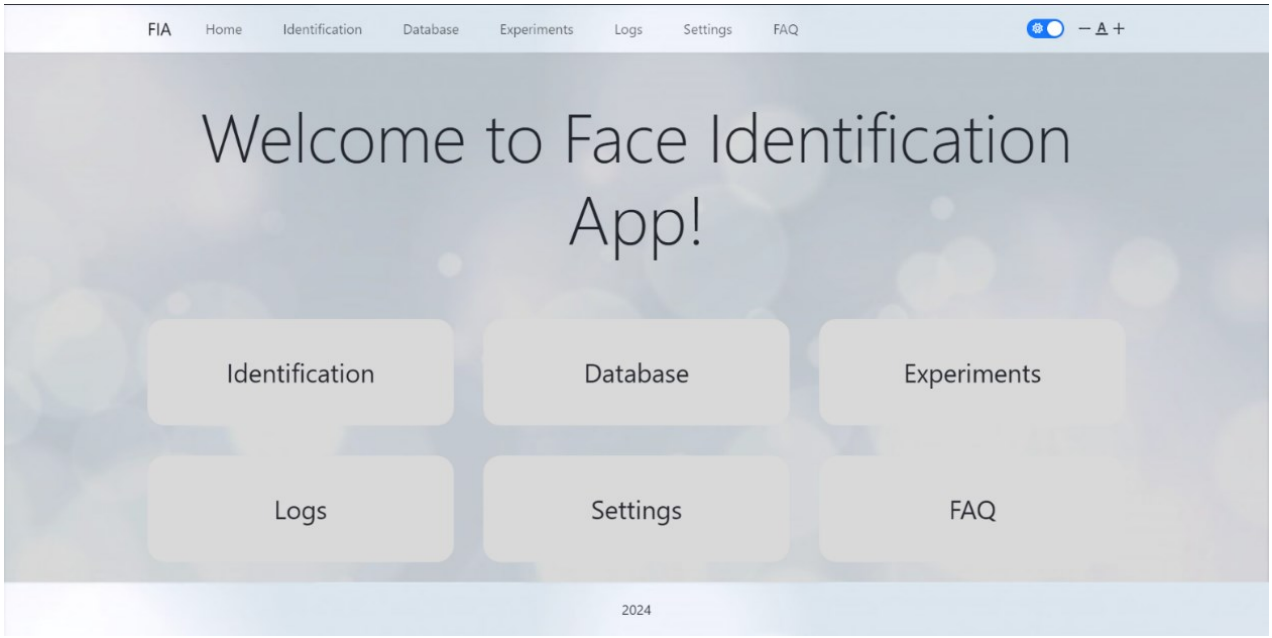


Рисунок 3.20 – Головна сторінка Home програмного забезпечення

Фрейм Identification, який зображено на Рисунку 3.21, надає користувачу можливості для використання функціональності, призначеної для виконання основної мети розробленого програмного забезпечення – ідентифікації особи на зображенні.

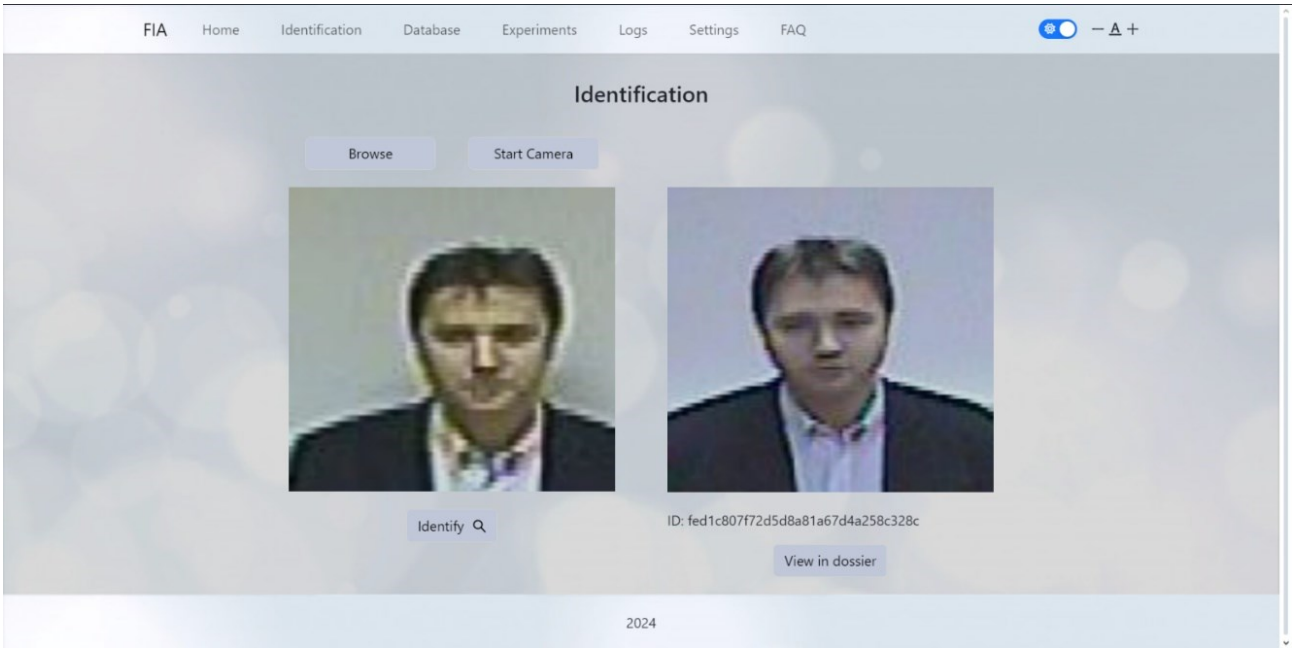


Рисунок 3.21 – Фрейм Identification програмного забезпечення біометричної ідентифікації

В лівій частині фрейму розташовані:

- кнопка Browse – відкриває діалогове вікно операційної системи, в якому користувач може обрати шлях до зображення або відео, на якому необхідно ідентифікувати особу;
- кнопка Start Camera – запускає камеру пристрою, на якому виконується програмне забезпечення, для ідентифікації особи з відеопотоку в реальному часі;
- область відображення зображення, обраного користувачем, або відео з камери, на яких необхідно ідентифікувати особу;
- кнопка Identify – запускає на виконання комплексний метод біометричної ідентифікації, що лежить в основі розробленого програмного забезпечення.

В правій частині фрейму містяться:

- область відображення еталонного зображення з бази даних особи, яку ідентифіковано на зображенні або відео, що були надані користувачем;
- поле ID, в якому відображається результат виконання комплексного методу біометричної ідентифікації – ідентифікатор знайденого на зображенні/відео суб’єкта;
- кнопка View in dossier – кнопка, що перенаправляє на сторінку перегляду досьє ідентифікованого суб’єкта.

Сторінка Database, представлена на Рисунку 3.22, дозволяє користувачеві переглядати вміст бази даних та здійснювати певні запити до неї з метою отримання або збереження інформації про суб’єкти ідентифікації. Даний фрейм складається з наступних елементів:

- рядок та кнопка пошуку – призначені для пошуку запису про конкретний суб’єкт, інформація про якого зберігається в базі даних;
- кнопка Register – призначена для реєстрації нових суб’єктів в базі даних, відкриває діалогове вікно, в якому користувач може внести дані про суб’єкт реєстрації та зберегти їх в базі даних;
- таблиця, що відображає вміст сутності бази даних, призначеної для збереження інформації про суб’єкти.

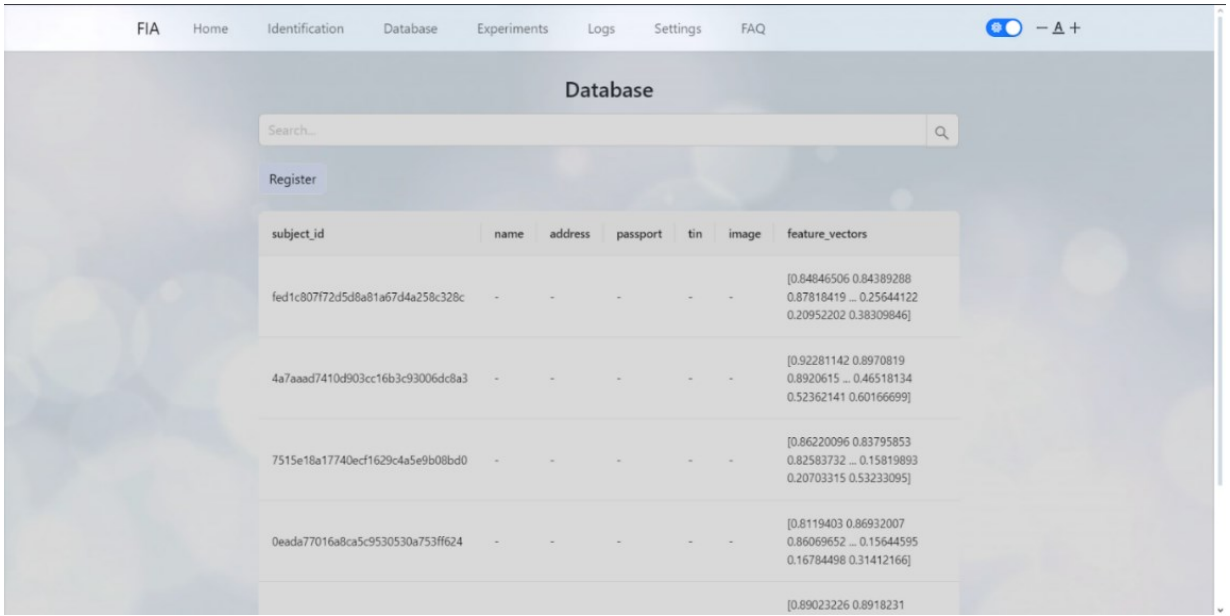


Рисунок 3.22 – Фрейм Database програмного забезпечення

Сторінка Experiments призначена для проведення експериментального дослідження комплексного методу біометричної ідентифікації, що лежить в основі розробленого програмного забезпечення, з метою перевірки його ефективності за різних умов здійснення ідентифікації, підбору відповідних параметрів методу і його подальшого удосконалення. Екранна форма сторінки зображена на Рисунку 3.23.

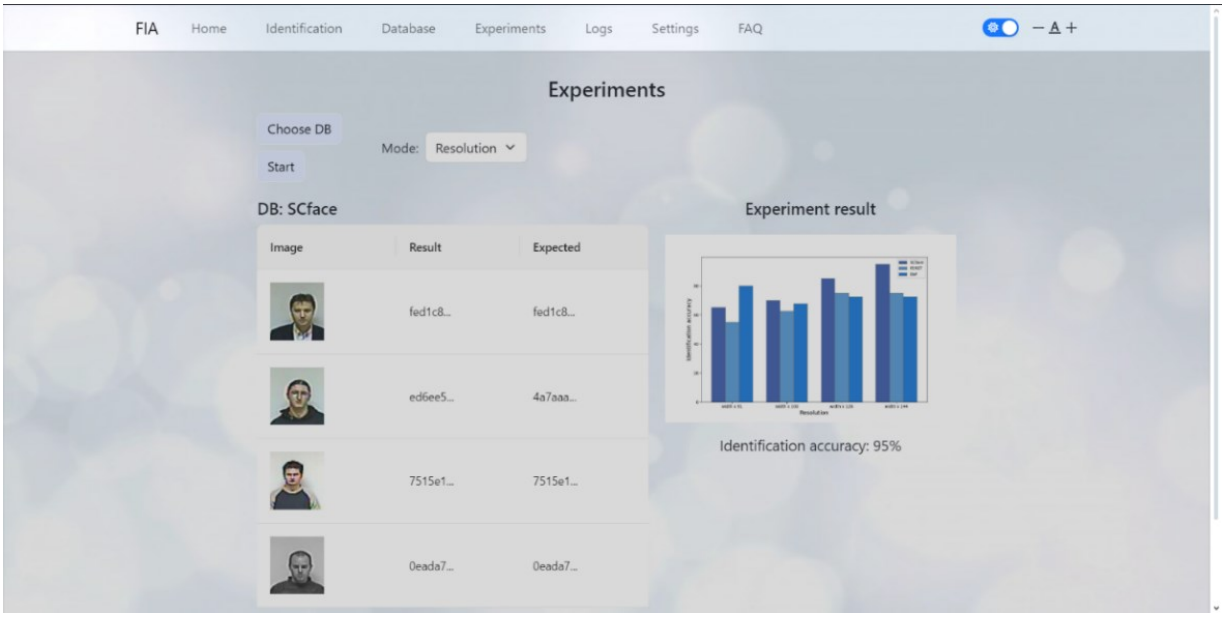


Рисунок 3.23 – Фрейм Experiments програмного забезпечення

Розглянемо більш детально елементи фрейму Experiments:

- кнопка Choose DB – відкриває діалогове вікно операційної системи, в якому користувач може обрати шлях до репозиторію, де зберігаються набори зображень, на яких необхідно виконати ідентифікацію;
- поле Mode та випадний список – надають користувачу можливість обрати режим, в якому будуть проводитися експерименти;
- кнопка Start – запускає на виконання метод ідентифікації, який застосовується до кожного зображення із обраного користувачем набору даних;
- поле DB, в якому відображається назва набору даних, до якого застосовується метод ідентифікації;
- таблиця результатів, в якій відображаються зображення, до яких застосовано комплексний метод біометричної ідентифікації, результат роботи

методу (отриманий в результаті експерименту ідентифікатор) та очікуваний результат (відомий ідентифікатор суб'єкта);

- область Experiment result, в якій відображається графічна інформація про результати проведеного експерименту та точність ідентифікації.

Налаштування параметрів комплексного методу біометричної ідентифікації користувач може здійснити на сторінці Settings, яка представлена на Рисунку 3.24. Фрейм містить поля для введення значень параметрів кожного з методів, покладених в основу комплексного методу біометричної ідентифікації. При натисканні на кнопку Save введенні значення перевіряються на валідність та передаються в компонент програмного забезпечення, в якому реалізовано метод ідентифікації. Користувач має можливість змінити лише деякі параметри методу, при цьому значення інших параметрів, для яких не здійснено введення, або будуть розраховані автоматично, або залишаться такими ж, як були до початку коригування.

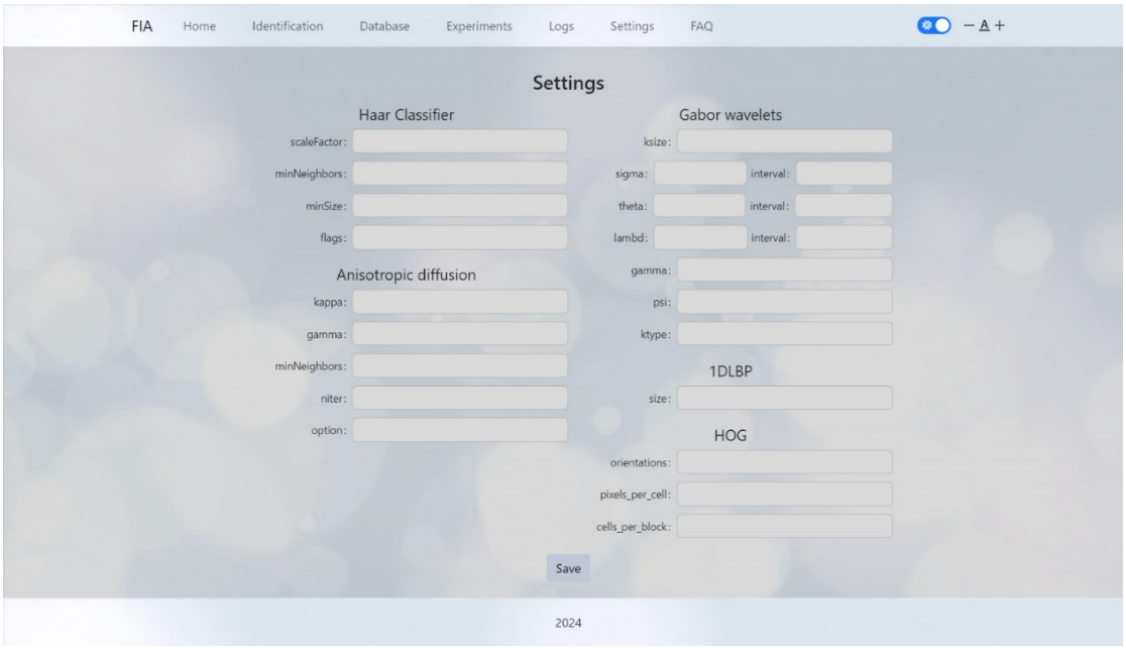


Рисунок 3.24 – Фрейм Settings програмного забезпечення

Таким чином, реалізоване програмне забезпечення надає можливості для використання комплексного методу біометричної ідентифікації, в основу якого покладено такі методи, як ознаки Гаара, анізотропна дифузія, вейвлет-перетворення

Ґабора, а також локально-текстурні дескриптори зображень локальні бінарні шаблони в одновимірному просторі та гістограми орієнтованих градієнтів.

Висновки до розділу 3

У третьому розділі описано процес створення програмної компоненти рішення задачі біометричної ідентифікації за зображенням обличчя та отримано наступні результати:

1. Визначено особливості програмного рішення, основні можливості, які мають бути в ньому реалізовані, а також здійснено аналіз варіантів використання.

2. Описано сценарії функціонування програмної компоненти, а саме визначено послідовність процесів, які виконуватимуться у створюваній програмі, та взаємодію між процесами та об’єктами програмного забезпечення.

3. Спроєктовано комплексний метод біометричної ідентифікації, а саме визначено його складові, описано основні методи цих складових і операції, які вони виконуватимуть.

4. Спроєктовано додаткові функціональні можливості програмного забезпечення відповідно до результатів аналізу варіантів використання та сценаріїв функціонування програмної компоненти. Визначено компоненти програмного забезпечення та описано основні методи реалізації цих компонентів.

5. Визначено вимоги до інформаційного забезпечення програмної компоненти, сформовано структуру бази даних, спроєктовано її основні сутності та атрибути з урахуванням вимог до інтеграції програмної компоненти в існуючі інформаційні системи.

6. Використовуючи вищенаведені результати, реалізовано програмну компоненту біометричної ідентифікації у вигляді вебзастосунку з клієнт-серверною архітектурою.

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА ФОРМУВАННЯ ВИМОГ

4.1 Методика проведення експериментального дослідження комплексного методу біометричної ідентифікації

1. Мета експериментального дослідження

– оцінка ефективності запропонованого комплексного методу біометричної ідентифікації, що базується на локально-текстурних дескрипторах, для вирішення задачі розпізнавання облич на зображеннях з варіативністю властивостей та за умов неповної видимості рис обличчя.

2. Набори даних

Для проведення експериментів використовувалися набори зображень з такими технічними характеристиками:

2.1. The Database of Faces [108]

- Кількість зображень: 400.
- Кількість суб'єктів: 40.
- Формат зображень: PGM.
- Роздільна здатність: 92×112 пікселів.
- Особливості фіксації: фронтальне положення, зміни освітлення, виразів обличчя (відкриті/закриті очі, усміхнені/неусміхнені), наявність оклюзивних елементів.

2.2. FERET [109]

- Кількість зображень: 14126.
- Кількість суб'єктів: 1199.
- Формат зображень: JPG.
- Роздільна здатність: 256×384 пікселів.
- Особливості фіксації: однакові фізичні налаштування для кожної сесії, різні вирази обличчя та зміни освітлення.

2.3. SCface [110]

- Кількість зображень: 4160.
- Кількість суб'єктів: 130.
- Формат зображень: JPG.
- Роздільна здатність: 75×100, 96×128, 108×144 пікселів.
- Особливості фіксації: камерами відеоспостереження, різні кути огляду, різні відстані, змінне освітлення.

2.4. AgeDB [111]

- Кількість зображень: 16488.
- Кількість суб'єктів: 568.
- Формат зображень: JPG.
- Роздільна здатність: змінна, середня роздільна здатність — 200×200 пікселів.
- Особливості фіксації: необмежені умови, різні вікові категорії, зміни у виразах обличчя, шум, оклюзії, зміни освітлення.

2.5. CFP (Celebrities in Frontal-Profile in the Wild) [112]

- Кількість зображень: 5000.
- Кількість суб'єктів: 500.
- Формат зображень: JPG.
- Роздільна здатність: 256×256 пікселів.
- Особливості фіксації: необмежені умови, фронтальні та профільні пози обличчя, різні варіації поз і освітлення.

2.6. LFW (Labeled Faces in the Wild) [113]

- Кількість зображень: 13233.
- Кількість суб'єктів: 5749.
- Формат зображень: JPG.
- Роздільна здатність: 250×250 пікселів.
- Особливості фіксації: природні умови, варіації пози, освітлення, виразів обличчя.

2.7. Tinyface [114]

- Кількість зображень: 169403.
- Кількість суб'єктів: 5139.
- Формат зображень: JPG.
- Роздільна здатність: 20×16 пікселів.
- Особливості фіксації: природні умови, низька роздільна здатність.

3. Етапи проведення експериментального дослідження

3.1. Формування тестової та еталонної вибірок зображень облич

Для проведення експериментального дослідження ефективності комплексного методу біометричної ідентифікації сформовано тестові та еталонні вибірки зображень. Вибірки зображень формувалися у залежності від кількості зображень, наявних у кожному наборі даних. Зважаючи на те, що набір The Database of Faces містить зображення облич лише 40 суб'єктів, що є найменшою кількістю серед усіх вибраних баз даних, для забезпечення об'єктивності результатів у вибірках з решти наборів також використовувалися зображення 40 суб’єктів. При цьому зображення, що входили до еталонної вибірки, не використовувалися в тестовій вибірці, і навпаки.

Під час проведення експериментів тестові та еталонні вибірки наборів зображень облич були розподілені на такі, що зафіксовані в контрольованих і неконтрольованих умовах. Контрольовані умови характеризуються стабільними параметрами фіксації зображень, такими як рівномірне освітлення, фіксовані вирази обличчя та сталі пози суб’єктів. Неконтрольовані умови включають значну варіативність освітлення, фону, виразів обличчя, а також інші фактори, які змінювалися під час фіксації зображень, зокрема, рухи суб’єкта та зміни ракурсу. Такий розподіл вибірок зображень дозволяє оцінити ефективність методу в умовах, що більше наближені до реальних сценаріїв, де характеристики зображень можуть бути варіативними.

3.1.1. Вибірки зображень, зафіксованих у контрольованих умовах

The Database of Faces:

- Еталонна вибірка: 80 зображень, 2 зображення на суб’єкт.
- Тестова вибірка: 40 зображень, 1 зображення на суб’єкт.
- Характеристики зображень: варіації виразів обличчя (відкриті/закриті очі, усміхнені/неусміхнені) та умов освітлення.

FERET:

- Еталонна вибірка: 59 зображень, 1-2 зображення на суб’єкт (залежно від доступної кількості зображень для кожного суб’єкта в наборі).
- Тестова вибірка: 40 зображень, 1 зображення на суб’єкт.
- Характеристики зображень: варіації освітлення, поз обличчя та часу між моментами фіксації.

SCface:

- Еталонна вибірка: 120 зображень, 3 зображення на суб’єкт.
- Тестова вибірка: 40 зображень, 1 зображення на суб’єкт.
- Характеристики зображень: зафіксовані камерами відеоспостереження з варіаціями відстані, кута огляду та рівня освітленості.

3.1.2. Вибірки зображень, зафіксованих у неконтрольованих умовах

AgeDB:

- Еталонна вибірка: 134 зображення, 3-4 зображення на суб’єкт.
- Тестова вибірка: 40 зображень, 1 зображення на суб’єкт.
- Характеристики зображень: охоплюють різні вікові періоди, дозволяючи оцінити вплив вікових змін зовнішності на ідентифікацію.

CFP:

- Еталонна вибірка: 162 зображення, 3-4 зображення на суб’єкт.
- Тестова вибірка: 40 зображень, 1 зображення на суб’єкт.
- Характеристики зображень: містять фронтальні та профільні позиції обличчя для аналізу впливу зміни ракурсу обличчя.

LFW:

- Еталонна вибірка: 85 зображень, 2-3 зображення на суб’єкт (залежно від доступної кількості зображень для кожного суб’єкта в наборі).
- Тестова вибірка: 40 зображень, 1 зображення на суб’єкт.
- Характеристики зображень: варіації освітлення, фону, виразів обличчя та кута зйомки.

Tinyface:

- Еталонна вибірка: 49 зображень, 1-2 зображення на суб’єкт (залежно від доступної кількості зображень для кожного суб’єкта в наборі).
- Тестова вибірка: 40 зображень, 1 зображення на суб’єкт.
- Характеристики зображень: низька роздільна здатність.

3.2. Експерименти щодо визначення ефективної комбінації методів

Визначення ефективної комбінації методів, що лежать в основі комплексного методу, з використанням вибірок з наборів даних:

- The Database of Faces – описано в пп. 2.1.3 розділу 2.
- FERET і SCface.

3.3. Застосування комплексного методу до вибірок зображень з наборів даних The Database of Faces, FERET і SCface, зафіксованих у контрольованих умовах

3.3.1. Експерименти щодо визначення вимог до вхідних даних комплексного методу біометричної ідентифікації з перетворенням таких властивостей зображень:

- формату зображення;
- роздільної здатності зображення;
- роздільної здатності області обличчя на зображенні.

3.3.2. Експерименти в умовах неповної видимості рис обличчя на зображенні.

3.4. Застосування комплексного методу до вибірок зображень з наборів даних AgeDB, CFP, LFW і Tinyface, зафіксованих у неконтрольованих умовах

3.4.1. Експерименти з перетворенням властивостей зображень, аналогічно етапу 3.3.1.

3.4.2. Експерименти в умовах неповної видимості рис обличчя на зображенні, аналогічно етапу 3.3.2.

4. Оцінка ефективності комплексного методу біометричної ідентифікації

Для оцінки ефективності комплексного методу використовуються метрики точності ідентифікації та помилкової ідентифікації. Показник точності (*Accuracy*) визначається як відношення кількості коректно ідентифікованих суб'єктів до загальної кількості суб'єктів у тестовій вибірці та обчислюється за формулою:

$$Accuracy = \frac{N_{correct}}{N_{total}} \cdot 100\%, \quad (4.1)$$

де $N_{correct}$ – кількість коректно ідентифікованих суб'єктів, N_{total} – загальна кількість суб'єктів у тестовій вибірці.

Показник помилкової ідентифікації (*Error*) визначається як доповнення до точності:

$$Error = 100\% - Accuracy. \quad (4.2)$$

5. Очікувані результати

- Порівняння ефективності комплексного методу при застосуванні до зображень, зафіксованих у контрольованих і неконтрольованих умовах.
- Визначення впливу властивостей зображень на ефективність комплексного методу.
- Визначення ефективності комплексного методу в умовах неповної видимості рис обличчя на зображеннях.
- Формулювання вимог до вхідних зображень.

6. Порівняльний аналіз результатів

Порівняльний аналіз результатів роботи запропонованого комплексного методу з результатами роботи:

- методів на основі локально-текстурних дескрипторів;
- алгоритмів на основі методів штучного інтелекту.

4.2 Експериментальні дослідження щодо визначення ефективної комбінації методів

У розділі 2 досліджено ефективність методів, на основі яких розроблено комплексний метод біометричної ідентифікації, при застосуванні їх до вибірок зображень з набору даних The Database of Faces. Зокрема, встановлено, що найбільше значення точності методу вдалося отримати при застосуванні комбінації методів вилучення векторів ознак 1DLBP і HOG. Проте, доцільним є проведення дослідження щодо встановлення найбільш ефективної комбінації методів, що лежать в основі комплексного методу біометричної ідентифікації, при застосуванні їх до наборів зображень, що мають характеристики, відмінні від характеристик набору даних, який використано в початковому експерименті.

З цією метою обрано два набори зображень облич, відмінних від набору даних The Database of Faces за форматом, роздільною здатністю, кількістю зображень для окремого суб'єкта та якістю в контексті умов, за яких здійснено фіксацію зображень, а саме FERET і SCface.

Експериментальні результати для набору даних FERET представлені в Таблиці 4.1.

Таблиця 4.1 – Результати експериментального дослідження визначення ефективної комбінації методів при застосуванні до зображень з набору даних FERET

	HOG		1DLBP		HOG + 1DLBP	
	Точність	Помилка	Точність	Помилка	Точність	Помилка
Всього суб'єктів	40		40		40	
Кількість суб'єктів	29	11	26	14	29	11
Показник точності ідентифікації	72,5%	27,5%	65%	35%	72,5%	27,5%

З Рисунку Б.1 випливає, що на зображеннях більшої роздільної здатності використання методу 1DLBP не є доцільним, оскільки показник точності ідентифікації однаковий і становить 72,5% під час проведення експерименту лише

з методом вилучення вектору ознак HOG, а також при застосуванні комбінації методів HOG та 1DLBP. Показник помилкової ідентифікації, отриманий під час експериментів з набором зображень FERET, коливається від 27,5 до 35,5%.

Результати експериментів, проведених на зображеннях з набору даних SCface, представлені в Таблиці 4.2.

Таблиця 4.2 – Результати експериментального дослідження визначення ефективної комбінації методів при застосуванні до зображень з набору даних SCface

	HOG		1DLBP		HOG + 1DLBP	
	Точність	Помилка	Точність	Помилка	Точність	Помилка
Всього суб'єктів	40		40		40	
Кількість суб'єктів	37	3	31	9	38	2
Показник ідентифікації	92,5%	7,5%	77,5%	22,5%	95%	5%

З аналізу показників точності, представлених на порівняльній діаграмі на Рисунку Б.2, випливає, що використання лише методу 1DLBP для процесу вилучення ознак забезпечує всього 77,5% коректно ідентифікованих зображень обличчя. Використання методу HOG покращує результати роботи комплексного методу приблизно на 15% і забезпечує точність ідентифікації у 92,5%. Але комбінація векторів ознак HOG і 1DLBP збільшує ефективність комплексного методу біометричної ідентифікації до 95%. Результати цієї серії експериментів підтверджують, що використання комбінації двох методів вилучення векторів ознак є доцільним на зображеннях низької якості та роздільної здатності, а коефіцієнт помилкової ідентифікації в цьому випадку є найнижчим серед усіх експериментів – 5%.

На порівняльній діаграмі на Рисунку 4.1 представлені результати ідентифікації з використанням обраних методів на різних наборах даних. Зважаючи на те, що зображення обличчя з бази даних SCface, які використовувалися для проведення експерименту, є низькоякісними зображеннями, зафіксованими

камерами відеоспостереження, що наближено до реальних умов розпізнавання, сукупність усіх досліджуваних методів забезпечує високу точність ідентифікації на зображеннях обличчя низької якості. У контексті цього дослідження зображення низької якості визначаються як зображення з низькою роздільною здатністю, розмиті, нечіткі, піксельні, з шумами, а зображення високої якості, навпаки, визначаються як більш чіткі, з низьким рівнем стиснення та зниженим рівнем шуму.

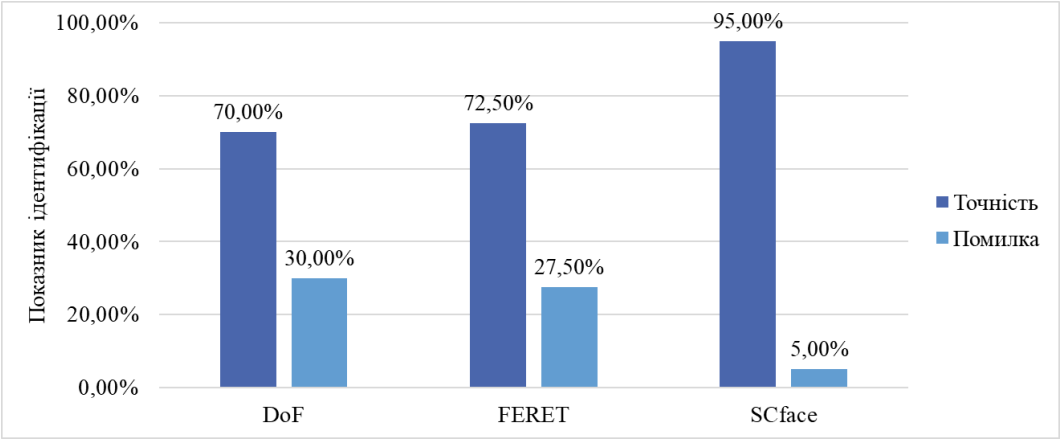


Рисунок 4.1 – Порівняльна діаграма результатів експериментів із застосуванням комплексного методу біометричної ідентифікації до наборів зображень

З результатів аналізу всіх експериментальних результатів випливає, що застосування методів анізотропної дифузії, вейвлет-перетворення Ґабора у комбінації з одночасно двома локально-текстурними дескрипторами гістограми орієнтованих градієнтів і локальні бінарні шаблони в одновимірному просторі демонструє найвищі результати ідентифікації серед всіх досліджуваних наборів даних.

4.3 Експериментальні дослідження на зображеннях обличчя, зафіксованих в контрольованих умовах

Оскільки найвищий показник точності ідентифікації 95% отримано при застосуванні комплексного методу до зображень з набору даних SCface, а показники точності ідентифікації на інших наборах даних коливаються від 70 до 72,5%, значна варіація отриманих результатів, що становить 22,5-25%, свідчить про

необхідність дослідити чинники, що впливають на ефективність комплексного методу при застосуванні до зображень з інших наборів даних та чи можливо підвищити ефективність роботи методу за рахунок зміни цих чинників.

Крім того, зазвичай методи розпізнавання та ідентифікації облич працюють бездоганно в умовах високої якості зображень еталонної (зображення, що зберігаються в базі даних) і тестової (зображення, до яких застосовується метод ідентифікації) вибірок зображень, а також, коли ці два набори незначно відрізняються за характеристиками. Однак існує багато випадків, коли зображення еталонної і тестової вибірок зображень значно варіюються за характеристиками, тому продуктивність методів розпізнавання обличчя та ідентифікації може погіршуватися [115].

З метою вирішення проблеми варіації показників точності комплексного методу біометричної ідентифікації при застосуванні до зображень з різними характеристиками проведено експериментальне дослідження для визначення залежності показника точності ідентифікації від таких властивостей зображення, як формат, роздільна здатність та область обличчя, що покриває зображення.

Методи розпізнавання облич зазвичай розробляються для зображень із повністю видимими рисами. Проте пандемія COVID-19 поставила під сумнів їх ефективність у системах прийняття рішень, оскільки носіння масок, що закривають нижню частину обличчя, ускладнювало ідентифікацію [116]. Дослідження показали, що більшість методів нестабільні при розпізнаванні облич із масками. Детальніше цю проблему розглянуто в розділі 1.5.

Відповідно, окрім раніше згаданих пунктів, ще однією метою даної роботи є проведення експериментального дослідження розробленого комплексного методу біометричної ідентифікації із застосуванням його до зображень облич в умовах неповної видимості рис.

Для проведення експериментального дослідження використовувалися набори зображень облич The Database of Faces, FERET і SCface. Вимоги до відбору зображень облич були сформовані на основі попередніх досліджень комплексного методу біометричної ідентифікації: вибірки повинні містити фронтальні

зображення з різними виразами обличчя, оклюзіями, різноманітністю поз голови та освітлення.

Спершу розглянемо експерименти з перетворенням формату зображень. У задачах розпізнавання облич використовуються формати BMP, PNG, JPEG, TIFF. Формати TIFF, BMP і PNG забезпечують стиснення без втрат, тоді як JPEG використовує стиснення з втратами, що може впливати на якість зображення. PNG має мінімальні втрати при стисненні, подібні до JPEG. Ступінь стиснення без втрат становить 1:2–1:4, тоді як стиснення з втратами може досягати 1:40. TIFF має найменший рівень стиснення, а JPEG – найбільший [117-120]. Важливо визначити, який формат найбільш підходить для розпізнавання облич та ідентифікації суб'єкта. Необхідно дослідити, який із форматів файлів зображень більше підходить для завдання розпізнавання обличчя з подальшою ідентифікацією суб'єкта.

Першу серію експериментів проведено з перетворенням оригінальних зображень із наборів даних, обраних для проведення дослідження, у формати зображень BMP, PNG (стиснуті формати) і JPG (нестиснутий формат). Результати цих експериментів представлені в Таблиці Б.1.

Як видно з порівняльної діаграми на Рисунку 4.2, конвертація формату не вплинула на результати експериментів для бази даних SCface – показник точності ідентифікації незмінно дорівнює 95%. Аналізуючи експериментальні результати для зображень із набору The Database of Faces, доцільно зазначити, що перетворення оригінального формату зображення, яким є PGM, у JPG покращило отриманий результат із 70 до 75%, тобто ефективність покращилась на 5%. Навпаки, результат для бази даних FERET знизився на 2,5% при конвертації зображення у формат JPG, проте стабільно дорівнює 72,5% при конвертації зображення у формати BMP і PNG.

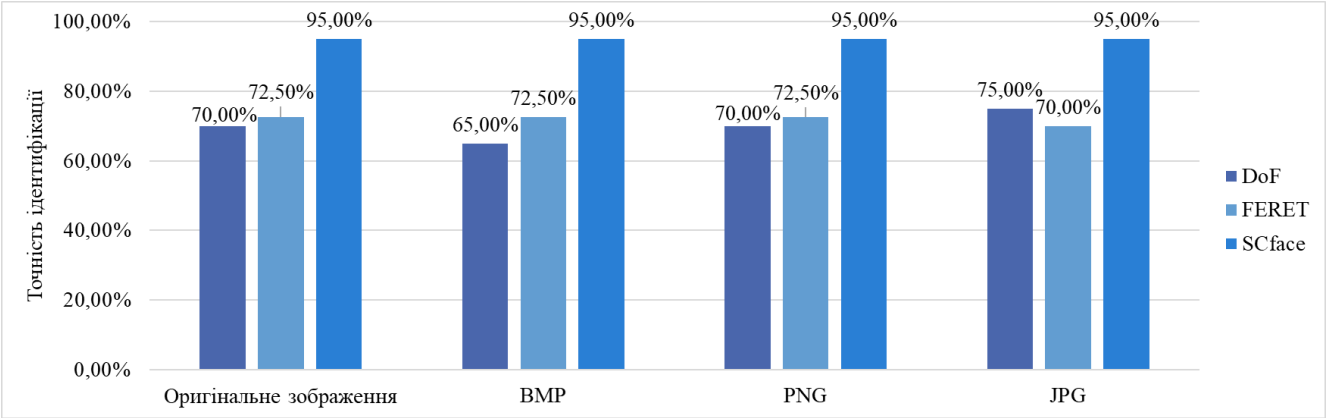


Рисунок 4.2 – Порівняльна діаграма результатів, отриманих під час експериментів, проведених із перетворенням форматів зображень з наборів даних The Database of Faces, FERET, SCface

Оскільки експериментально встановлено, що формати файлів, які зберігають зображення, впливають на показники точності комплексного методу біометричної ідентифікації, в подальших експериментах вирішено виконувати перетворення форматів з метою встановлення можливості уніфікації параметрів зображень.

Далі здійснено експерименти з перетворенням роздільної здатності зображень. Оптимальна роздільна здатність для розпізнавання облич досі обговорюється серед дослідників. Загальноприйнятого критерію для визначення низької роздільної здатності немає. Дослідження показують, що для високої точності потрібно щонайменше 32×32 пікселі, хоча для ідентифікації може бути достатньо 16×16 [121].

Однією з цілей даного експериментального дослідження є аналіз можливості уніфікації зображень за роздільною здатністю таким чином, щоб отримати найвищий показник точності ідентифікації запропонованого комплексного методу.

З метою визначення того, чи залежить точність ідентифікації від різноманітності роздільної здатності зображення, вирішено провести експерименти з кількома значеннями роздільної здатності.

Оскільки всі набори даних, що використовуються в даній роботі, містять зображення з різною роздільною здатністю, а для перетворення цих зображень в уніфіковану роздільну здатність потрібно або збільшити, або зменшити їх значення

висоти та ширини, вибрати лише один метод перетворення неможливо. Тому вирішено провести експеримент, який порівнює ці два методи і роздільні здатності, початкові значення яких потрібно збільшити або зменшити до значення *ширина*×100. Для збереження зображень на основі попередньо отриманих результатів обрано формат JPG, оскільки показники точності методу були найбільш стабільними при застосуванні до зображень, перетворених в цей формат. Результати експерименту наведені в Таблиці Б.2.

Аналіз результатів дає підстави стверджувати, що при застосуванні до різних наборів даних ефективність одного із методів може як перевищувати точність ідентифікації іншого методу, так і поступатися своїми показниками. Враховуючи цей результат, для проведення експерименту з роздільною здатністю зображення вирішено використовувати обидва ці методи, враховуючи необхідність збільшення або зменшення роздільної здатності зображення.

Раніше отримані експериментальні результати показали, що найвищий показник точності ідентифікації отримано на зображеннях з бази даних SCface з роздільною здатністю 75×100, 96×128 і 108×144 пікселів. Ці значення роздільної здатності були обрані для проведення експериментів на інших наборах даних, а також для бази даних SCface з перетворенням усіх зображень в уніфіковану роздільну здатність.

Під час підготовки експериментів важливо конвертувати зображення в однакові значення роздільної здатності. Проте, оскільки всі набори даних, що використовуються в даному дослідженні, містять вихідні зображення з різною роздільною здатністю, співвідношення сторін зображень також могло бути змінено. Зміна співвідношення сторін може спричини зміну характеристик зображень, зокрема викривлення рис облич, які є критично важливими для подальшої успішної ідентифікації. Отже, роздільна здатність зображень була перетворена таким чином, щоб співвідношення сторін залишалося незмінним, тобто висота зображень є фіксованим значенням, а ширина – змінним, пропорційним до коефіцієнта співвідношення сторін.

Для перетворення роздільної здатності зображення на ранніх етапах дослідження використовувалася функція thumbnail(). У ході експериментів виявилося, що зображення з баз даних облич не можливо конвертувати в розмір 75×100 лише за допомогою цієї функції, натомість зображення були конвертовані в роздільну здатність 75×91 пікселів. Оскільки отримані результати на цій роздільній здатності здавалися багатообіцяючими, вирішено також використовувати цю роздільну здатність для проведення експериментів.

У результаті були проведені експерименти з такими значеннями роздільної здатності для наборів зображень: The Database of Faces – 75×91,75×100, 96×128 і 108×144; FERET– 61×91, 67×100, 85×128 і 96×144; SCface – 68×91, 75×100, 96×128 і 108×144. Крім того, формат зображень змінено відповідно до першої серії експериментів. Результати експериментального дослідження представлені в Таблиці Б.3.

На Рисунках 4.3-4.5 представлені узагальнені для кожного набору даних показники точності, отримані в результаті застосування комплексного методу біометричної ідентифікації до зображень з перетвореною роздільною здатністю, аналізуючи які можна зробити наступні висновки.

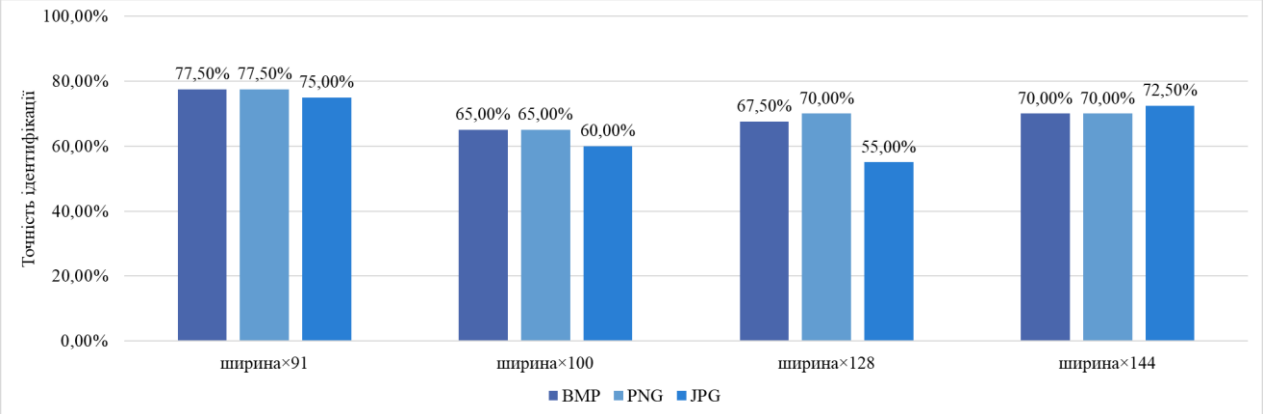


Рисунок 4.3 – Експериментальні результати застосування комплексного методу біометричної ідентифікації до зображень з набору даних The Database of Faces з перетворенням роздільної здатності

Застосування методів перетворення роздільної здатності до зображень з набору даних The Database of Faces дозволило підвищити точність ідентифікації з 70% на оригінальних зображеннях до 77,5% на зображеннях з роздільною здатністю 75×91 пікселів, конвертованих у формати BMP і PNG. У порівнянні з результатами перетворення формату, отримані результати зросли на 2,5%. Результати з використанням значень роздільної здатності 82×100, 105×128 і 118×144 в порівнянні з раніше отриманими результатами знизилися до 55-72,5%.

Показники точності ідентифікації, отримані на зображеннях з набору даних FERET, суттєво знизилися після перетворення роздільної здатності зображення на значення 61×91 і 67×100 пікселів – з 72,5% до 52,5-62,5%. З іншого боку, результати стабільно дорівнюють отриманому раніше результату 72,5% на зображеннях з перетворенням формату на BMP і PNG і роздільної здатності на 85×128 і 96×144 пікселів. А результат для зображень формату JPG з роздільною здатністю 96×144 є найвищим серед усіх отриманих з використанням набору даних FERET і становить 75%.

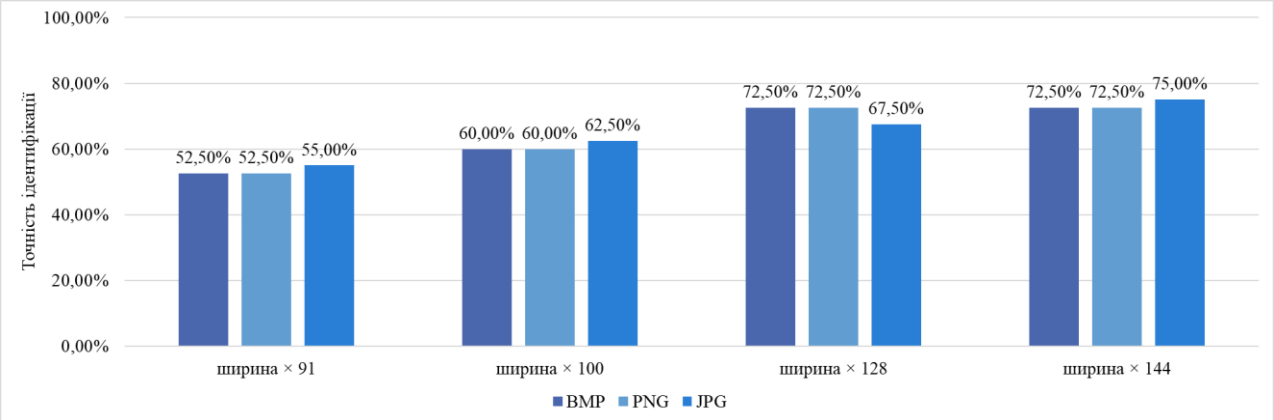


Рисунок 4.4 – Експериментальні результати застосування комплексного методу біометричної ідентифікації до зображень з набору даних FERET з перетворенням роздільної здатності

Результати для зображень бази даних SCface зменшилися після перетворення на роздільну здатність 68×91, 75×100 і 96×128 пікселів. Показник точності ідентифікації коливається в діапазоні від 62,5% до 87,5%. Навпаки, перетворення

роздільної здатності зображення до 108×144 пікселів дозволило отримати результат 92,5% на зображеннях формату BMP і PNG і найвищий результат 95% на зображеннях формату JPG.

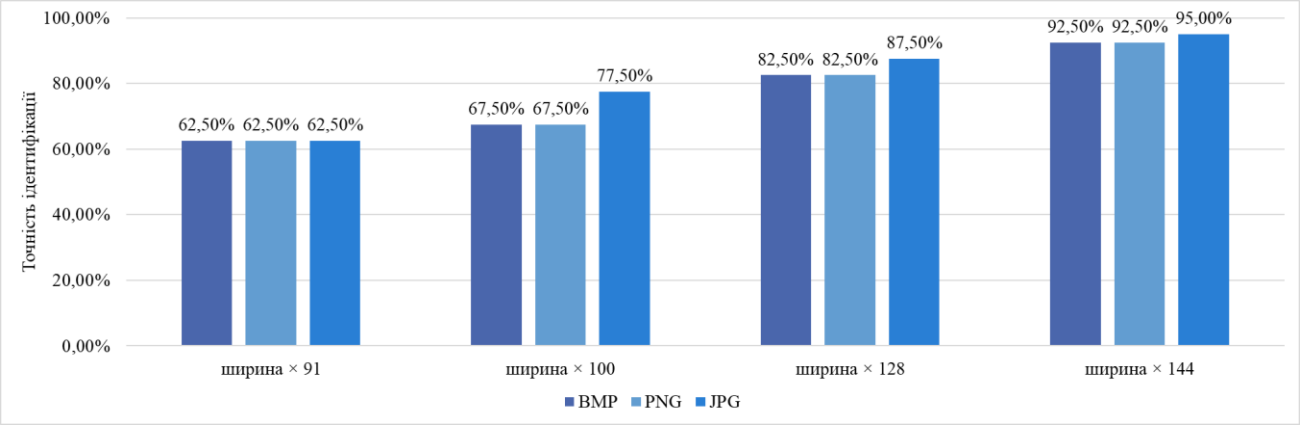


Рисунок 4.5 – Експериментальні результати застосування комплексного методу біометричної ідентифікації до зображень з набору даних SCface з перетворенням роздільної здатності

На наступному кроці дослідження здійснено експерименти з перетворенням роздільної здатності області обличчя на зображеннях. Мала область обличчя та відсутність деталей ускладнюють його розпізнавання. Камери спостереження часто дають зображення низької роздільної здатності, або ж обличчя фіксується здалеку, втрачаючи локальні ознаки, необхідні для ідентифікації.

Локальні особливості формують глобальний опис зображення, але більшість детекторів навчені на якісних зображеннях. Тому їх ефективність знижується при обробці зображень низької якості, що ускладнює виявлення обличчя.

Отже, на наступному етапі експериментального дослідження необхідно визначити, чи залежить показник точності ідентифікації від розміру ділянки зображення, що містить обличчя. Для цього вирішено створити еталонну та тестову вибірки зображень, які містять лише область обличчя без будь-яких інших деталей. Еталонна і тестові вибірки зображень, що містять тільки область обличчя, при проведенні експериментів також перетворено за форматом і роздільною здатністю. Зокрема, проаналізовано експеримент, який показав найвищий результат за

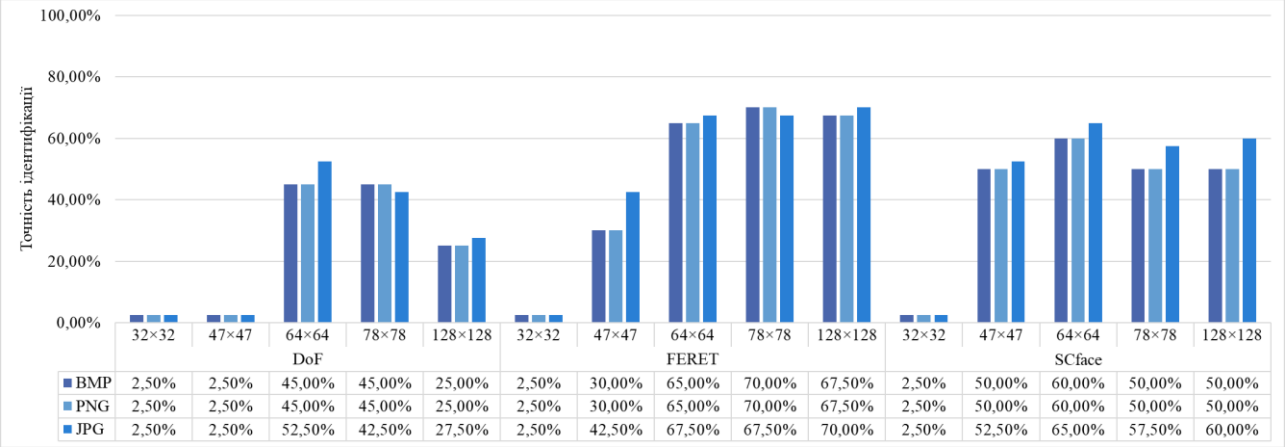
показником точності ідентифікації під час попередніх досліджень, а саме експеримент із зображеннями формату JPG, які містить набір даних SCface. У результаті аналізу встановлено, що зображення з областю обличчя 47×47 і 78×78 пікселів були коректно ідентифіковані в більшості експериментів. Розмір області обличчя на зображеннях з набору даних SCface відрізняється через те, що вихідне еталонне та тестове зображення також мають різні розміри. Відповідно вирішено використати зазначені розміри з метою проведення дослідження в цій серії експериментів. Крім того, з метою визначення варіативності коефіцієнта ідентифікації за межами вибраних розмірів вирішено виконати експерименти на зображеннях, які містять область обличчя, з пороговими мінімальним і максимальним значеннями роздільних здатностей (32×32 та 128×128), а також зі значенням між вибраними значеннями та пороговими значеннями (64×64).

Таким чином, експерименти з областю зображення обличчя проводилися з наступними значеннями роздільної здатності зображень, що містять лише область обличчя: 32×32, 47×47, 64×64, 78×78 та 128×128 пікселів.

Отже, як видно з Рисунку 4.6, показник точності ідентифікації не залежить від того, чи містять еталонні та тестові вибірки зображень будь-які інші деталі, крім самої області обличчя. Це означає, що методи виявлення обличчя та перетворення роздільної здатності зображення, які закладено в запропонований метод ідентифікації, здатні коректно вирішити поставлену задачу, незалежно від роздільної здатності та якості вхідних зображень. Таблиця Б.4 містить результати описаних експериментів.

Розглянемо виконання експериментального дослідження розробленого комплексного методу в умовах неповної видимості рис обличчя на зображеннях. З точки зору анатомії обличчя, такі оклюзії, як медична маска або балаклава, зазвичай покривають середню та нижню частини обличчя, залишаючи відкритою верхню частину обличчя. Крім того, як з’ясовано під час огляду літератури, атаки змагального характеру часто засновуються на наявності масок і патчів, що спотворюють риси обличчя людини. Зазвичай такі спотворюючі елементи застосовуються до нижньої частини обличчя, оскільки часто атаки такого характеру

виконуються у фізичному просторі. Оскільки досліджуваний комплексний метод біометричної ідентифікації вирішує задачу виявлення обличчя на зображенні з подальшою його обробкою, для моделювання стану неповної видимості рис обличчя вирішено перетворити зображення на етапі попередньої обробки зображення методом таким чином, щоб зображення містили тільки верхню частину обличчя. Були проведені експерименти з методами перетворення формату зображення, роздільної здатності та області зображення, що містить обличчя.



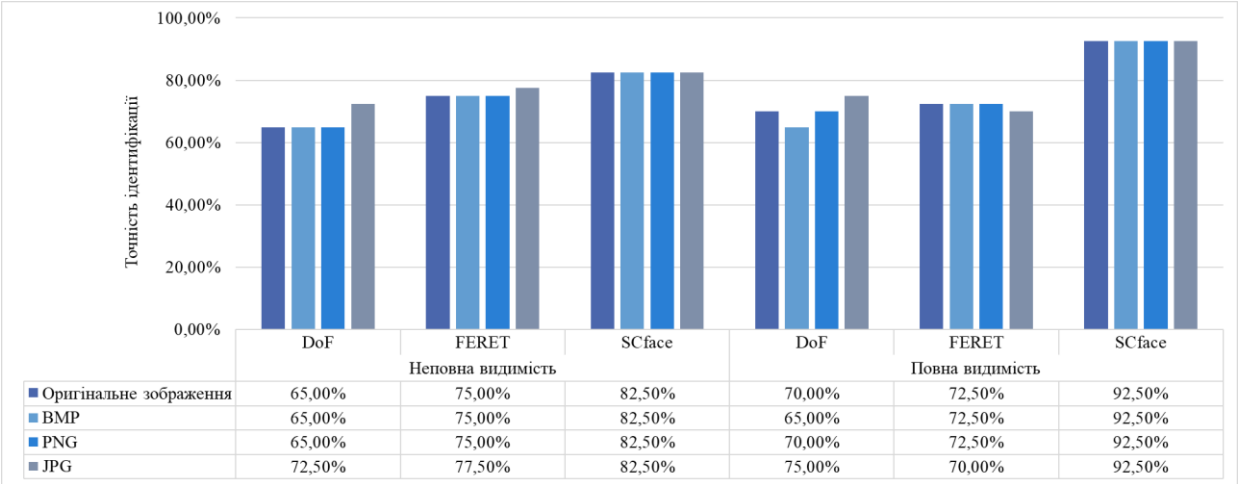
	32×32	47×47	64×64	78×78	128×128	32×32	47×47	64×64	78×78	128×128	32×32	47×47	64×64	78×78	128×128
	DoF					FERET					SCface				
BMP	2,50%	2,50%	45,00%	45,00%	25,00%	2,50%	30,00%	65,00%	70,00%	67,50%	2,50%	50,00%	60,00%	50,00%	50,00%
PNG	2,50%	2,50%	45,00%	45,00%	25,00%	2,50%	30,00%	65,00%	70,00%	67,50%	2,50%	50,00%	60,00%	50,00%	50,00%
JPG	2,50%	2,50%	52,50%	42,50%	27,50%	2,50%	42,50%	67,50%	67,50%	70,00%	2,50%	52,50%	65,00%	57,50%	60,00%

Рисунок 4.6 – Експериментальні результати застосування комплексного методу біометричної ідентифікації до зображень з наборів даних з перетворенням роздільної здатності області обличчя

Результати експериментів, проведених на зображеннях в умовах неповної видимості рис облич з перетворенням формату зображень, представлені в Таблиці Б.5.

Порівнюючи результати, представлені на порівняльній діаграмі на Рисунку 4.7, показник точності ідентифікації методу, застосованого на зображеннях з набору даних SCface, знизився на 10% на зображеннях з неповною видимістю рис облич по відношенню до експериментів на вихідних зображеннях, де обличчя видимі повністю. Для зображень з набору даних The Database of Faces показник точності ідентифікації знизився на 2,5-5%. А в експериментах із зображеннями з набору даних FERET точність ідентифікації підвищилася на 2,5% на початкових

зображеннях і після їх конвертації у формати BMP і PNG, а також на 5% після конвертації зображень у формат JPG.



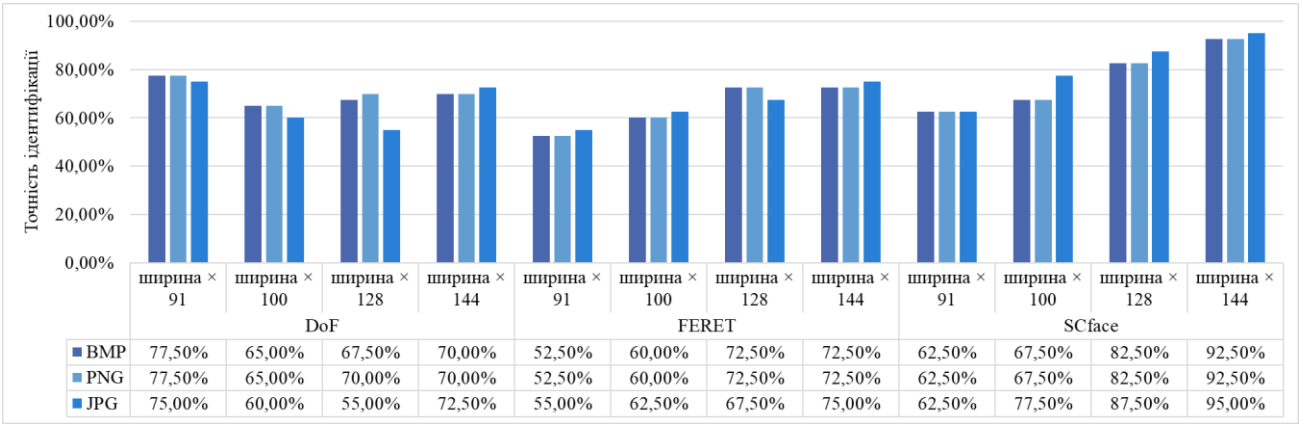
	Неповна видимість			Повна видимість		
	DoF	FERET	SCface	DoF	FERET	SCface
Оригінальне зображення	65,00%	75,00%	82,50%	70,00%	72,50%	92,50%
BMP	65,00%	75,00%	82,50%	65,00%	72,50%	92,50%
PNG	65,00%	75,00%	82,50%	70,00%	72,50%	92,50%
JPG	72,50%	77,50%	82,50%	75,00%	70,00%	92,50%

Рисунок 4.7 – Порівняльна діаграма результатів експериментів, проведених на зображеннях з наборів даних The Database of Faces, FERET і SCface в умовах повної та неповної видимості рис облич з перетворенням формату

Результати експериментів, проведених на зображеннях неповністю видимих облич з перетворенням формату та роздільної здатності, представлені в Таблиці Б.6.

Експериментальні результати на зображеннях із перетворенням формату та роздільної здатності можна порівняти з результатами експериментів на початкових зображеннях та зображеннях з перетвореннями формату. З порівняльної діаграми на Рисунку 4.8 видно, що результати для наборів даних The Database of Faces і FERET знизилися після перетворення роздільної здатності зображення в усіх серіях експериментів. Трансформація зображень з набору даних SCface до роздільної здатності 108x144 пікселів підвищила результат точності ідентифікації до 85% на зображеннях, конвертованих у BMP та PNG.

Результати експериментів, проведених на зображеннях із перетворенням формату зображення та роздільної здатності області зображення, що містить лише риси обличчя, наведені в Таблиці Б.7.



	DoF				FERET				SCface			
	ширина × 91	ширина × 100	ширина × 128	ширина × 144	ширина × 91	ширина × 100	ширина × 128	ширина × 144	ширина × 91	ширина × 100	ширина × 128	ширина × 144
BMP	77,50%	65,00%	67,50%	70,00%	52,50%	60,00%	72,50%	72,50%	62,50%	67,50%	82,50%	92,50%
PNG	77,50%	65,00%	70,00%	70,00%	52,50%	60,00%	72,50%	72,50%	62,50%	67,50%	82,50%	92,50%
JPG	75,00%	60,00%	55,00%	72,50%	55,00%	62,50%	67,50%	75,00%	62,50%	77,50%	87,50%	95,00%

Рисунок 4.8 – Порівняльна діаграма результатів експериментів, проведених на зображеннях з наборів даних The Database of Faces, FERET і SCface в умовах неповної видимості рис облич з перетвореннями формату та роздільної здатності

4.4 Експериментальні дослідження на зображеннях обличчя, зафіксованих в неконтрольованих умовах

З метою подальшого дослідження та покращення ефективності запропонованого комплексного методу біометричної ідентифікації за зображенням обличчя, здійснено експерименти на наборах даних, які містять зображення, отримані за різних умов фіксації щодо інтенсивності освітлення, наявності косметики, гриму чи оклюзивних елементів, вікової мінливості суб'єктів, різноманітності пози голови та міміки тощо. Для експериментального дослідження обрано кілька наборів даних, зафіксованих в неконтрольованих умовах, наближених до природного середовища, в якому можна спостерігати людські обличчя, а саме AgeDB [111], CFP (Celebrities in Frontal-Profile data set) [112], LFW (Labeled Faces in the Wild) [113] і Tinyface [114].

Для проведення експериментального дослідження використовувалися ті ж налаштування, що і для набору експериментів на зображеннях, зафіксованих в контрольованих умовах. Спершу розглянемо експерименти з перетворенням властивостей зображень.

Результати експериментів з перетворенням формату зображень з наборів даних, зафіксованих в неконтрольованих умовах, наведено в Таблиці Б.8.

Як видно з результатів експерименту, показники точності ідентифікації є постійними при застосуванні комплексного методу до зображень з усіх наборів даних, незалежно від формату зображення. Відповідно в наступних експериментах перетворення формату не застосовується.

Другий набір експериментів проводився з перетворенням роздільної здатності вихідних зображень, що зберігаються в наборах даних. Роздільна здатність перетворювалася лише на фіксоване значення висоти, а ширина визначалася автоматично так, щоб зберегти співвідношення сторін вихідного зображення. Згідно з результатами аналізу попередніх експериментальних досліджень, описаних у пункті 4.3.2, встановлено, що найвищі показники точності ідентифікації під час застосування досліджуваного комплексного методу отримано на зображеннях з роздільною здатністю *ширина*×91, *ширина*×100, *ширина*×128 та *ширина*×144 пікселів, де *ширина* – значення ширини, що визначалося автоматично для зображень так, щоб зберегти початкове співвідношення сторін зображення. Ці ж значення були використані і для поточної серії експериментів.

Результати експериментів з перетворенням роздільної здатності зображень з наборів даних, зафіксованих в неконтрольованих умовах, наведено в Таблиці 4.3.

На третьому етапі дослідження були проведені експерименти із зображеннями облич з наборів даних, перетвореними таким чином, щоб зображення містили лише риси обличчя людини без будь-яких інших деталей, наприклад, фону. Для проведення дослідження були обрані параметри розміру зображення, які дозволили отримати високі результати роботи комплексного методу біометричної ідентифікації в попередньому дослідженні, описаному в пункті 4.3.2, а саме 47×47 та 78×78 пікселів, а також порогові значення розміру області обличчя (32×32 і 128×128) і середнє значення між вибраними значеннями та пороговими значеннями (64×64).

Результати експериментів з перетворенням роздільної здатності області зображень, що містить лише риси обличчя людини, з наборів даних, зафіксованих в неконтрольованих умовах, наведено в Таблиці Б.9.

Таблиця 4.3 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних AgeDB, CFP, LFW і Tinyface з перетворенням роздільної здатності

	ширина×91		*ширина*×100		*ширина*×128		*ширина*×144	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	AgeDB							
Всього зображень / суб'єктів	174 / 40		174 / 40		174 / 40		174 / 40	
Кількість суб'єктів	18	22	16	24	20	20	16	24
Показник ідентифікації	45%	55%	40%	60%	50%	50%	40%	60%
	CFP							
Всього зображень / суб'єктів	202 / 40		202 / 40		202 / 40		202 / 40	
Кількість суб'єктів	26	14	28	12	24	16	26	14
Показник ідентифікації	65%	35%	70%	30%	60%	40%	65%	35%
	LFW							
Всього зображень / суб'єктів	125 / 40		125 / 40		125 / 40		125 / 40	
Кількість суб'єктів	16	24	14	26	14	26	18	22
Показник ідентифікації	40%	60%	35%	65%	35%	65%	45%	55%
	Tinyface							
Всього зображень / суб'єктів	89 / 40		89 / 40		89 / 40		89 / 40	
Кількість суб'єктів	18	22	18	22	14	26	14	26
Показник ідентифікації	45%	55%	45%	55%	35%	65%	35%	65%

З аналізу результатів експериментів випливають такі висновки. Після застосування комплексного методу до зображень із набору даних AgeDB отримано загальні результати ідентифікації в діапазоні від 25% до 50%. Найвищий показник точності ідентифікації становить 50% і отримано його після перетворення роздільної здатності вихідних зображень на 128 пікселів по висоті зі збереженням співвідношення сторін. Такі середні показники точності ідентифікації могли спричинити наступні фактори. По-перше, мінливість віку осіб, чиї обличчя були зафіксовані на зображеннях. По-друге, набір даних містить переважно зображення відомих людей, тому багато з них містять театральну косметику, яка в деяких випадках спотворює риси обличчя людини. Останнім можливим фактором є те, що зображення були зафіксовані в необмежених умовах, тобто вони не є рівномірними щодо повороту голови, наявності шуму, мінливості виразу обличчя, наявності оклюзії.

Для зображень з набору даних CFP показники коректної ідентифікації комплексним методом коливаються від 15% до 70%. Після перетворення роздільної здатності вихідних зображень на 100 пікселів у висоту та ширину зі збереженням співвідношення сторін, отримано найвищий рівень точності ідентифікації, що складає 70%. Варто зазначити, що на отримані результати може вплинути різноманіття поз осіб, зафіксованих на зображеннях, оскільки набір даних CFP містить як фронтальні зображення, так і ті, що містять повороти голови на 90 градусів, відповідно, деякі риси обличчя можуть бути невидимими при спостереженні камерою. Крім того, як і у випадку з набором даних AgeDB, зображення в цьому наборі – це переважно фотографії публічних діячів, які були зафіксовані в необмежених умовах з точки зору навколишнього освітлення та інтенсивності спалаху камери. Ці фактори зробили деякі ділянки зображення надмірно освітленими, що могло спричинити спотворення зображення рис обличчя особи, яку потрібно ідентифікувати.

Точність ідентифікації, отримана в результаті проведення експериментів на зображеннях з набору даних LFW, становить від 5% до 60%. На оригінальних зображеннях з набору даних точність ідентифікації становить 55% і залишається

постійною після перетворення формату зображення. Після перетворення роздільної здатності показники коректної ідентифікації знизилися на 10-20%. Такі результати можна пояснити тим, що в наборі даних LFW міститься певна кількість зображень, на яких зафіксовано кілька облич різних людей. Унаслідок цього метод виявлення облич, реалізований у комплексному методі біометричної ідентифікації, може вилучити із зображення обличчя не тієї особи, яка є суб'єктом ідентифікації, що призводить до зниження точності. Однак найвищий показник точності ідентифікації отриманий після перетворення зображення на таке, що містить лише область обличчя та має роздільну здатність 128 пікселів у висоту та ширину. Крім того, це єдиний набір даних, при застосуванні до зображень з якого комплексний метод біометричної ідентифікації є найбільш ефективним саме у серії експериментів щодо перетворення зображень на такі, що містять лише область обличчя.

Результати експериментів на зображеннях з набору даних Tinyface – показники точності ідентифікації від 10% до 45%, що є найнижчим результатом серед усіх наборів експериментів у роботі в цілому. Такі результати комплексного методу біометричної ідентифікації можна пояснити специфікою параметрів зображень, що містяться в цьому наборі даних, і умовами, за яких вони були зафіксовані. Роздільна здатність зображень, що містяться в наборі даних Tinyface, критично низька для розпізнавання більшістю стандартних методів. Щоб застосувати запропонований комплексний метод біометричної ідентифікації до цих зображень, необхідно попередньо обробити зображення, збільшивши їх для можливості виявлення області обличчя. Такі перетворення можуть вплинути на коректність зображення рис обличчя, розмиваючи їх і унеможливлюючи подальше виділення вектора ознак у формі, придатній для подальшої класифікації. Оскільки вихідні зображення були зняті в необмежених умовах природного середовища, це могло істотно вплинути на ефективність комплексного методу біометричної ідентифікації.

Далі розглянемо експерименти на зображеннях обличчя з неповною видимістю рис. На першому етапі дослідження проведено експерименти на

зображеннях з вихідними властивостями із наборів даних, до яких застосовано лише перетворення, у результаті якого на зображеннях видно лише верхню частину обличчя, що імітувало наявність на обличчі елементу оклюзії, такого як, наприклад, медична маска або балаклава. Показники точності ідентифікації комплексного методу, отримані під час проведення експерименту, представлені в Таблиці 4.4.

Таблиця 4.4 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних AgeDB, CFP, LFW і Tinyface в умовах неповної видимості рис облич з вихідними властивостями

	AgeDB		CFP		LFW		Tinyface	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
Всього зображень / суб'єктів	174 / 40		202 / 40		125 / 40		80 / 40	
Кількість суб'єктів	10	30	20	20	10	30	4	36
Показник ідентифікації	25%	75%	50%	50%	25%	75%	10%	90%

Порівняємо отримані показники точності ідентифікації з результатами експериментів щодо застосування комплексного методу до цих же зображень, але з повною видимістю рис обличчя, описаних у пункті 4.3.1. Як видно з порівняльної діаграми на Рисунку 4.10, ефективність запропонованого комплексного методу біометричної ідентифікації знизилася на 10-30% у результаті застосування до зображень з неповною видимістю облич з наборів зображень AgeDB, CFP і LFW. Для набору зображень Tinyface результативність комплексного методу біометричної ідентифікації не змінилася, проте залишилася на рівні 10%, що є найменшим результатом серед усіх проведених експериментів у даному наборі.

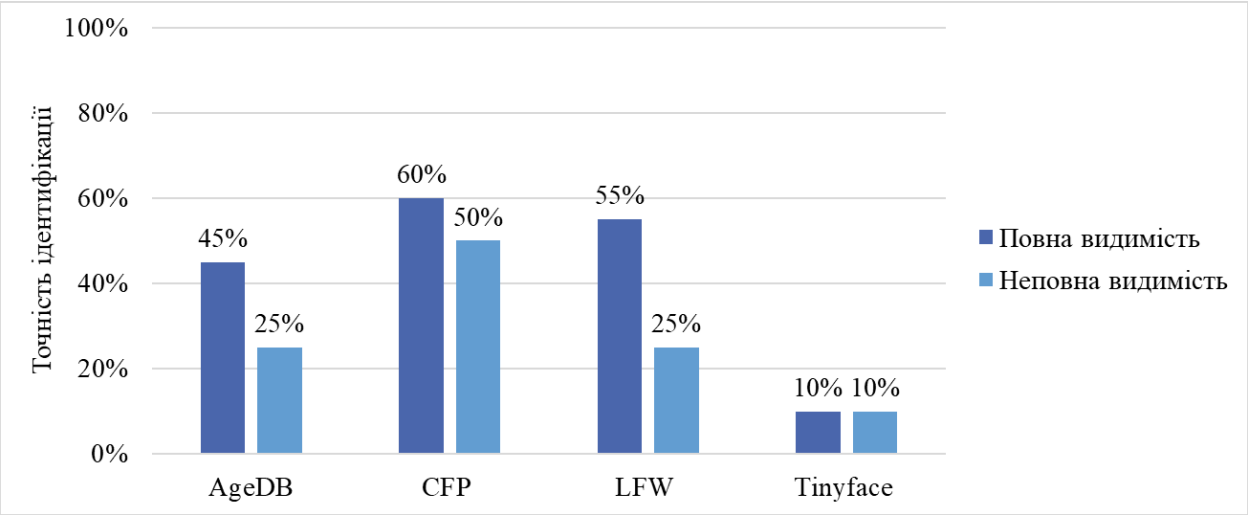


Рисунок 4.10 – Порівняльна діаграма результатів експериментів, проведених на зображеннях з наборів даних AgeDB, CFP, LFW і Tinyface в умовах повної та неповної видимості рис облич з вихідними властивостями

З метою підвищення ефективності запропонованого комплексного методу біометричної ідентифікації при застосуванні до зображень облич в умовах неповної видимості рис, а також дослідження впливу на показники точності ідентифікації властивостей зображень, до яких застосовується метод, наступні серії експериментів проведено з використанням зображень, що були перетворені за форматом стиснення, значенням роздільної здатності та областю зображення, що містить обличчя.

Дослідження щодо обсягу інформації, що міститься в зображеннях, проводилися шляхом перетворення зображень з обраних наборів зображень облич з неповною видимістю рис у формати BMP, PNG та JPG. Результати цих експериментів наведені у Таблиці Б.10.

Порівняння результатів експерименту з показниками точності ідентифікації після застосування запропонованого комплексного методу до зображень з неповною видимістю облич та оригінальними властивостями дозволяє дійти висновку, що, як видно з Рисунку 4.11, ефективність методу підвищилася у двох випадках: для зображень із наборів LFW – на 5% і CFP – на 10%, в обох випадках після перетворення зображень на формат JPG. При цьому для зображень з набору

CFP показник точності ідентифікації досяг значення 60%, що дорівнює показникові точності ідентифікації для цього набору даних на зображеннях повністю видимих облич з оригінальними властивостями.

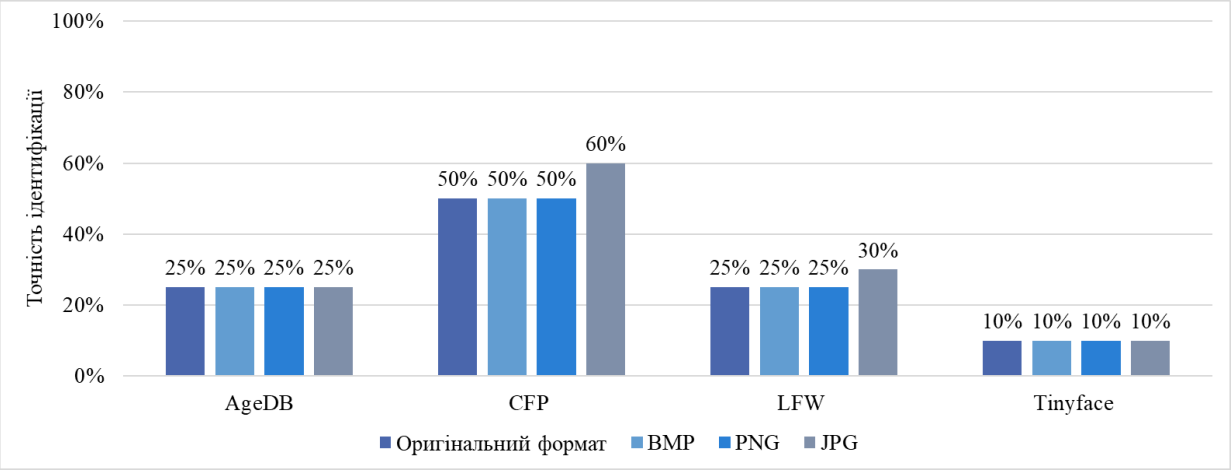


Рисунок 4.11 – Порівняльна діаграма результатів експериментів, проведених на зображеннях з наборів даних AgeDB, CFP, LFW і Tinyface в умовах неповної видимості рис облич з вихідними властивостями і з перетворенням формату

Такі результату експерименту свідчать про те, що в окремих випадках формат стиснення зображень, до яких застосовується запропонований метод ідентифікації, впливає на його ефективність.

Для проведення експериментів з перетворенням роздільної здатності зображень були обрані значення, які використовувалися в попередніх дослідження, а саме *ширина*×91, *ширина*×100, *ширина*×128 і *ширина*×144, де *ширина* – це значення ширини зображення, яке розраховується автоматично таким чином, щоб зберігалося співвідношення сторін оригінального зображення для збереження рис обличчя в первозданному вигляді. Результати експерименту наведені в Таблиці Б.11.

Виходячи з наведених результатів і порівняльної діаграми, представленої на Рисунку 4.12, можна зробити висновки, що показники точності ідентифікації запропонованого комплексного методу зросли в усіх експериментах на наступні

значення для наборів зображень: AgeDB – на 5-20%, CFP – на 15-25%, LFW – на 10-15%, Tinyface – на 15-30%.

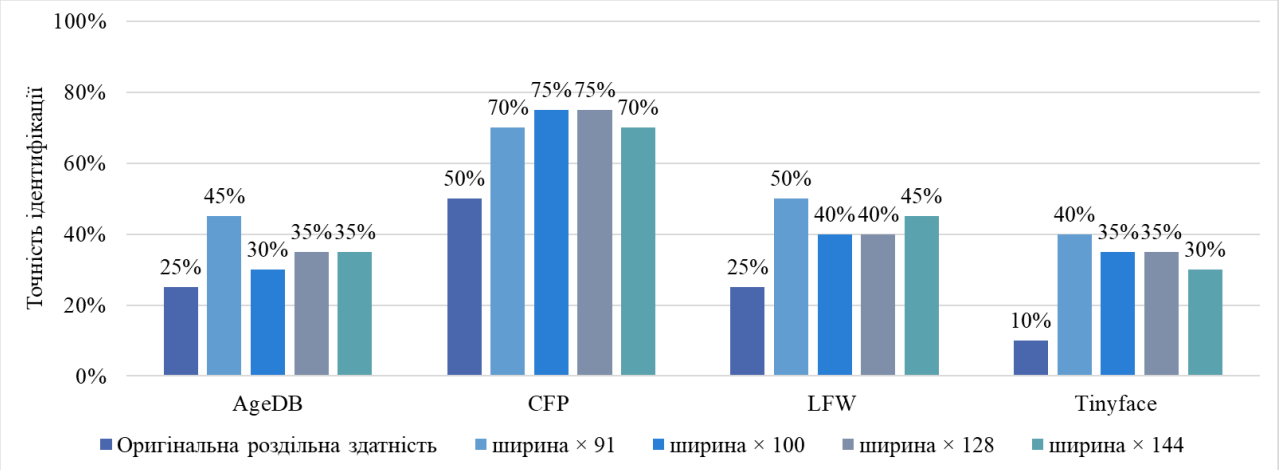


Рисунок 4.12 – Порівняльна діаграма результатів експериментів, проведених на зображеннях з наборів даних AgeDB, CFP, LFW і Tinyface облич в умовах неповної видимості рис облич з вихідними властивостями та перетворенням роздільної здатності (представлені найвищі показники)

Найвищі результати отримано після наступних перетворень: AgeDB (45%) – формат JPG та роздільна здатність *ширина*×91; CFP (75%) – формат JPG та роздільна здатність *ширина*×100, а також формат BMP/PNG та роздільна здатність *ширина*×128; LFW (50%) – формат BMP/PNG та роздільна здатність *ширина*×91; Tinyface (40%) – формат BMP/PNG та роздільна здатність *ширина*×91.

У результаті аналізу результатів попередніх досліджень встановлено, що зображення з областю обличчя *ширина*×47 і *ширина*×78 пікселів коректно ідентифіковані в більшості експериментів. Відповідно вирішено використати зазначені розміри з метою проведення дослідження в цій серії експериментів. Крім того, з метою визначення варіативності коефіцієнта ідентифікації за межами вибраних розмірів вирішено виконати експерименти на зображеннях, які містять область обличчя, з пороговими мінімальним і максимальним значеннями роздільних здатностей (*ширина*×32 та *ширина*×128), а також зі значенням між

вибраними значеннями та пороговими значеннями (*ширина*×64). Результати експерименту наведені в Таблиці Б.12.

Аналіз отриманих показників, наведених на Рисунку 4.13, свідчить про те, що за певних перетворень показники точності ідентифікації значно знижувалися, а за інших – зростали. Порівнюючи з результатами експерименту на зображеннях з оригінальними параметрами, результати даного експерименту зросли для наступних наборів зображень: AgeDB – на 5-25%, CFP – на 10-15%, LFW – на 5-25%, Tinyface – на 20-25%.

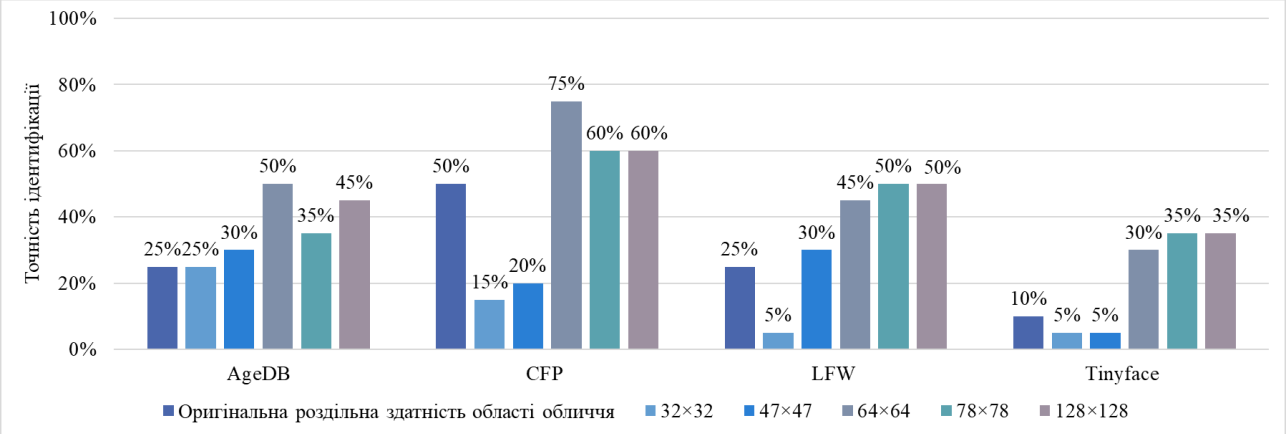


Рисунок 4.13 – Порівняльна діаграма результатів експериментів, проведених на зображеннях з наборів даних AgeDB, CFP, LFW і Tinyface облич в умовах неповної видимості рис облич з вихідними властивостями і з перетворенням області обличчя (представлені найвищі показники)

Найвищі результати отримано після наступних перетворень: AgeDB (50%) – формат JPG та значення області обличчя *ширина*×64; CFP (75%) – формат JPG та значення області обличчя *ширина*×64; LFW (50%) – формат BMP/JPG та значення області обличчя *ширина*×78, а також формат BMP та значення області обличчя *ширина* × 128; Tinyface (35%) – формат BMP/PNG та значення області обличчя *ширина*×78 і ширина×128. Варто зазначити, що застосування комплексного методу біометричної ідентифікації до зображень з набору AgeDB саме в цьому експерименті дозволило отримати найвище значення показника точності серед усіх серій експериментів.

Спершу порівняємо показники точності ідентифікації комплексного методу, отримані при застосуванні його до наборів зображень з перетвореними властивостями з неповною видимістю рис облич, з результатами експериментального дослідження із застосуванням запропонованого комплексного методу біометричної ідентифікації до тих же наборів зображень з перетвореними властивостями, на яких риси облич видимі повністю. Порівнювані показники представлені на Рисунку 4.14.

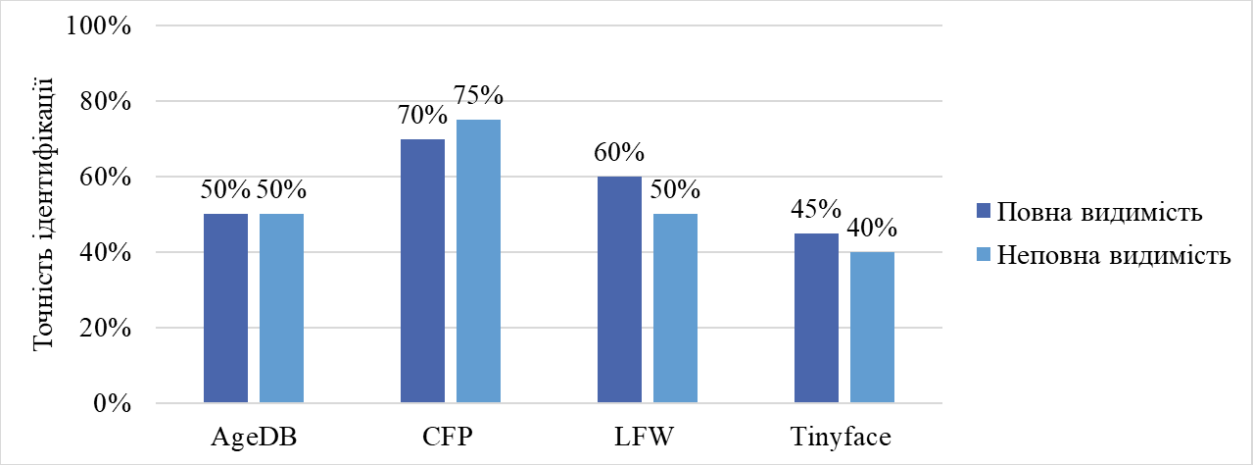
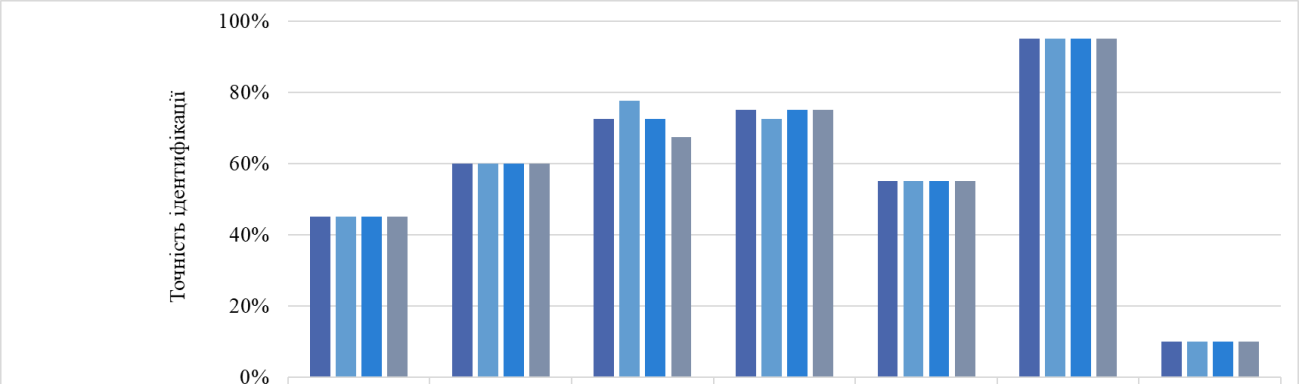


Рисунок 4.14 – Порівняльна діаграма показників точності ідентифікації комплексного методу на зображеннях з наборів даних AgeDB, CFP, LFW і Tinyface з повністю та неповністю видимими рисами обличчя

Отже, при застосуванні комплексного методу біометричної ідентифікації до зображень з набору даних AgeDB показник точності становить 50% незалежно від того, чи повністю видимі на зображеннях риси обличчя. У випадках застосування комплексного методу біометричної ідентифікації до зображень з наборів LFW і Tinyface показник точності знизився на 10% і 5% відповідно після перетворення зображень таким чином, щоб риси обличчя були видимі неповністю. Для набору зображень CFP показник точності ідентифікації збільшився на 5% після застосування комплексного методу біометричної ідентифікації до зображень з неповною видимістю рис обличчя.

4.5 Аналіз результатів та формування вимог до вхідних даних

Порівняльна діаграма результатів експериментів, проведених на оригінальних зображеннях та з перетворенням формату, представлена на Рисунку 4.15. Як видно з діаграми, найвищі показники точності ідентифікації отримані на зображеннях з наборів даних The Database of Faces (77,5% після конвертації зображень у формат JPG), FERET (75% на оригінальних зображеннях формату TIFF і після конвертації формату в PNG і BMP) і SCface (95% - на всіх досліджених форматах зображень). Результати експериментів на зображеннях з інших наборів коливаються від 10% до 60% точності ідентифікації.

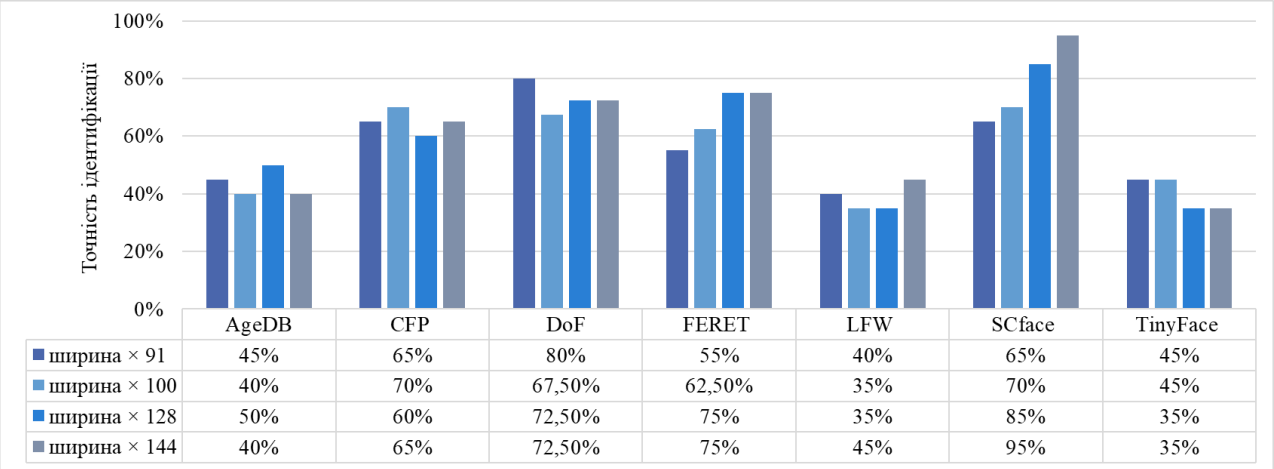


	AgeDB	CFP	DoF	FERET	LFW	SCface	TinyFace
Оригінальне зображення	45%	60%	72,50%	75%	55%	95%	10%
JPG	45%	60%	78%	72,50%	55%	95%	10%
PNG	45%	60%	72,50%	75%	55%	95%	10%
BMP	45%	60%	67,50%	75%	55%	95%	10%

Рисунок 4.15 – Порівняльна діаграма результатів експериментів на зображеннях із перетворенням формату

Аналіз результатів, отриманих при застосуванні комплексного методу біометричної ідентифікації до зображень з наборів даних The Database of Faces і FERET свідчить про те, що формат зображень, які подаються на вхід комплексного методу біометричної ідентифікації, у деяких випадках впливає на ефективність методу. Для всіх інших наборів даних результати є постійними, незалежно від зміни формату зображення. Варто зазначити, що всі ці набори даних містять зображення у форматі JPG, тому цей формат є найбільш придатним для зображень, до яких у майбутньому буде застосований запропонований метод ідентифікації.

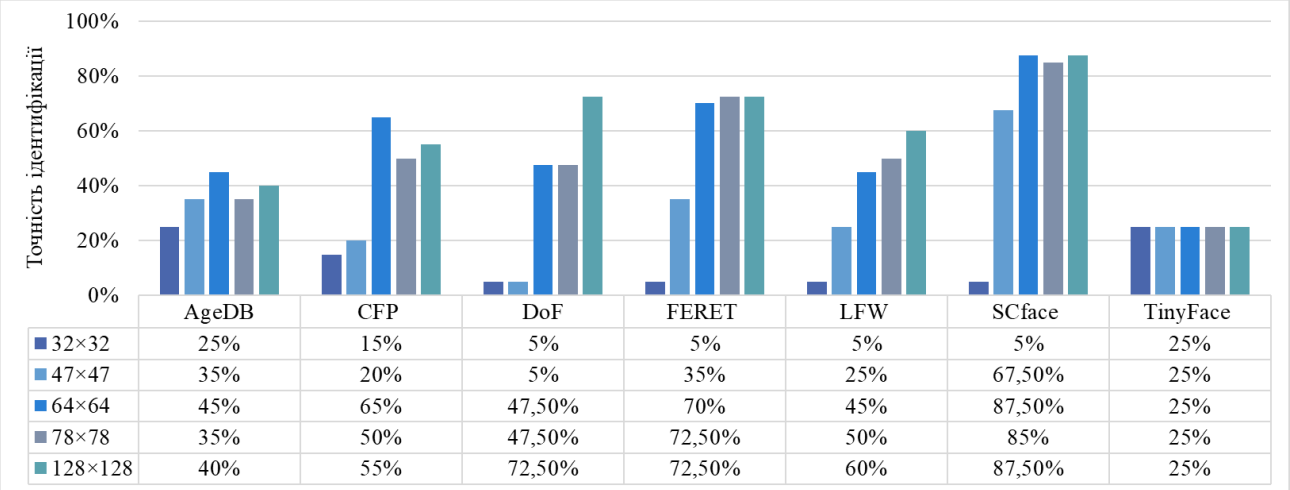
На Рисунку 4.16 представлено порівняльну діаграму результатів експериментів, проведених для дослідження роздільної здатності зображень, при застосуванні до яких запропонований комплексний метод біометричної ідентифікації є найбільш ефективним. Найвищий показник точності ідентифікації серед усіх серій експериментів, тобто 95%, отримано на зображеннях з набору даних SCface, роздільна здатність яких була перетворена на 108×144 пікселів. Однак досить високі показники були отримані і при використанні зображень з різних наборів даних після перетворення параметрів роздільної здатності на 75×91 і 96×128 пікселів.



	AgeDB	CFP	DoF	FERET	LFW	SCface	TinyFace
ширина × 91	45%	65%	80%	55%	40%	65%	45%
ширина × 100	40%	70%	67,50%	62,50%	35%	70%	45%
ширина × 128	50%	60%	72,50%	75%	35%	85%	35%
ширина × 144	40%	65%	72,50%	75%	45%	95%	35%

Рисунок 4.16 – Порівняльна діаграма результатів експериментів на зображеннях із перетворенням роздільної здатності

Діаграма результатів експериментів на зображеннях, які містять лише область обличчя без будь-яких інших деталей, наведена на Рисунку 4.17. Згідно з отриманими результатами точність ідентифікації суттєво знижується при застосуванні такого типу трансформації до зображень. Це може означати, що методи виявлення обличчя та зміни роздільної здатності області обличчя, закладені в основу запропонованого комплексного методу біометричної ідентифікації, успішно обробляють вхідні зображення, незалежно від того, чи містять вхідні дані будь-які деталі, крім рис обличчя людини.



	AgeDB	CFP	DoF	FERET	LFW	SCface	TinyFace
32×32	25%	15%	5%	5%	5%	5%	25%
47×47	35%	20%	5%	35%	25%	67,50%	25%
64×64	45%	65%	47,50%	70%	45%	87,50%	25%
78×78	35%	50%	47,50%	72,50%	50%	85%	25%
128×128	40%	55%	72,50%	72,50%	60%	87,50%	25%

Рисунок 4.17 – Порівняльна діаграма результатів експериментів на зображеннях, які містять лише область обличчя

Далі порівняємо показники точності ідентифікації методу при застосуванні його до зображень з повною та неповною видимістю рис обличчя. При цьому варто зазначити, що набори зображень AgeDB, CFP, LFW та Tinyface, до яких застосовувався запропонований метод ідентифікації, містять зображення, зафіксовані в необмежених умовах, що характеризуються наступними ознаками: надмірна інтенсивність освітлення, що впливає на можливість вилучення вектора ознак зображення; наявність косметики або гриму, які спотворюють риси обличчя людини; наявність оклюзивних елементів та положення голови в межах кута повороту, за яких риси обличчя частково або повністю закриті для спостереження камерою; мінливість міміки суб'єктів зйомки; порогова низька роздільна здатність зображень; велика варіабельність віку на різних зображеннях одного суб'єкта. У свою чергу набори зображень The Database of Faces, FERET і SCface характеризуються контрольованими або напівконтрольованими умовами фіксації зображень: однорідний фон, фронтальні або незмінні положення голови суб'єкта відносно камери, однакові умови освітлення та фізичні налаштування. Порівняльну діаграму наведено на Рисунку 4.18.

З результатів аналізу показників точності ідентифікації випливає, що запропонований комплексний метод біометричної ідентифікації є більш дієвим при застосуванні його до зображень, зафіксованих у контрольованих або

напівконтрольованих умовах. При цьому, показники знизилися при застосуванні методу до зображень з неповністю видимими рисами обличчя на 2.5-7.5% для зображень, зафіксованих в контрольованих умовах, у порівнянні з 5-10% для зображень, зафіксованих в неконтрольованих умовах.

Проте і у випадку контрольованих умов фіксації зображень, і неконтрольованих умов, існують виключення, за яких ефективність комплексного методу біометричної ідентифікації є вищою на 5% при застосуванні до зображень з наборів даних CFP і FERET з неповністю видимими рисами обличчя у порівнянні з експериментами на зображеннях з повністю видимим обличчям.

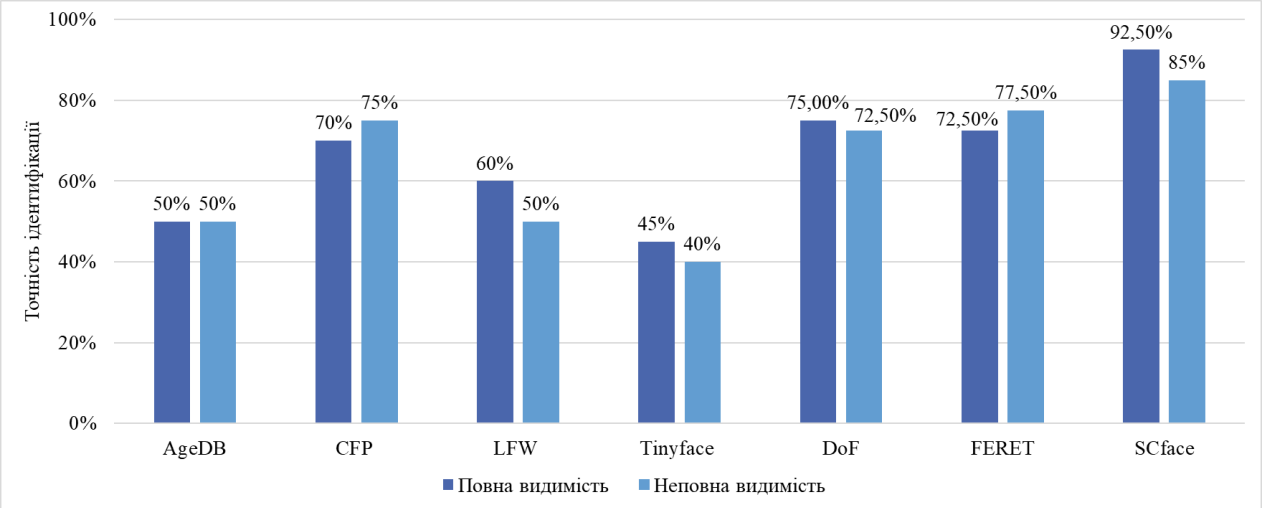


Рисунок 4.18 – Порівняльна діаграма показників точності ідентифікації комплексного методу на зображеннях, зафіксованих в контрольованих і неконтрольованих умовах з повністю та неповністю видимими рисами обличчя

Найвищий показник точності ідентифікації комплексного методу при застосуванні до зображень з неповністю видимими рисами обличчя становить 85% на зображеннях з набору SCface.

Одним із механізмів підвищення точності розпізнавання та ідентифікації є чітке формулювання вимог до зображень, що подаються на вхід методу ідентифікації. З огляду на результати експериментів, описаних в даній роботі,

сформулюємо вимоги до вхідних зображень запропонованого комплексного методу біометричної ідентифікації:

- Формат зображення – JPG.
- Роздільна здатність зображення в діапазоні від *ширина*×91 пікселів до *ширина*×144 пікселів, де *ширина* – це ширина зображення, яка розраховується автоматично зі збереженням співвідношення сторін зображення та, відповідно, рис обличчя, що міститься на ньому.
- Допускається поворот голови суб'єкта ідентифікації до 45 градусів, оскільки на зображенні мають бути видимі всі риси обличчя людини. Такий параметр відповідає зображенням у наборі SCface, при застосуванні до яких комплексний метод забезпечив найвищу точність.
- Зображення мають бути зроблені за стандартних умов освітлення з належним використанням інтенсивності спалаху для уникнення надмірного затемнення або освітлення певних ділянок зображення.
- Відстань між суб'єктом і камерою може становити від 1 м до 4,20 м. Саме в цьому діапазоні зафіксовані зображення з набору SCface, при застосуванні до яких отримано найвищий показник точності
- Прийнятним є середній часовий інтервал у 2 роки між фіксацією зображень, що утворюють вибірку для однієї особи. Дана вимога відповідає характеристикам більшості наборів зображень, до яких застосовано комплексний метод.
- Обличчя, зафіксовані на зображеннях, не повинні мати театрального гриму, оклюзивних елементів, які спотворюють риси обличчя або роблять їх повністю або частково непомітними з точки спостереження камерою.
- Зображення має містити обличчя лише однієї людини.
- Допускається незначна варіативність виразу обличчя, наприклад, відкриті/заплющені/примружені очі, усмішка/без усмішки.

4.6 Порівняльний аналіз результатів дослідження

З метою визначення, чи є запропонований комплексний метод біометричної ідентифікації технічно надійним, варто порівняти отримані показники точності з іншими існуючими методами на основі локально-текстурних дескрипторів. Виходячи з результатів аналізу сучасних робіт за темою дослідження, експерименти, подібні до представлених у даній роботі, не проводилися на методах, заснованих на локально-текстурних дескрипторах, і на тих розглянутих раніше алгоритмах, які базуються на методах штучного інтелекту. Тому отримані результати точності ідентифікації подібних методів можна порівнювати лише за наборами зображень облич, на яких отримано показники точності, і такому параметру зображень, що містяться в цих наборах, як роздільна здатність.

У статті [122] представлено огляд 18 локально-текстурних дескрипторів зображень, які були застосовані до кількох наборів зображень облич окремо та в поєднанні з іншими методами. У Таблиці Б.13 представлено порівняльні результати цих дескрипторів і дескрипторів, які лежать в основі запропонованого комплексного методу біометричної ідентифікації. Ефективність методів істотно відрізняється в залежності від набору зображень облич, до якого вони були застосовані. Комбінація 1DBP і HOG перевершує GDP на 16,2–40,22%, LDTP на 7,05–42,92%, LFD на 3,65–30,42%, LGP на 9,1–35,36% і LTrP на 19,9–41%.

Точність запропонованого методу перевищує нижню межу ефективності методів ORL: LBP на 22,06%, MBP на 23,67%, MBC на 1,97%, LAP на 21,86%, LDN на 24,31%, LPQ на 4,78%, LGIP на 17,42%, LMP на 15,83%, LTP на 17,78%, GLTP на 23,58%, MTP на 12,81%, PHOG на 1,89% і WLD на 15,36%.

Також отримані результати експериментального дослідження можна порівняти з результатами досліджень аналогічних методів, які містять дескриптори LBP та HOG, оскільки застосування комбінації дескрипторів 1DLBP та HOG для зображень обличчя, оброблених за допомогою вейвлет-перетворення Ґабора, раніше не досліджувалося в задачах розпізнавання обличчя та ідентифікації. Результати порівняння ефективності дескрипторів на основі LBP і HOG наведені в Таблиці 4.5. Ефективність комбінації методів, запропонованих у даній роботі,

перевищує ефективність методів на основі оригінальних дескрипторів LBP і HOG на 1-12,5% і близька до ефективності інших комбінацій дескрипторів на основі LBP і HOG.

Таблиця 4.5 – Порівняльна таблиця показників точності ідентифікації комбінації локально-текстурних дескрипторів на основі LBP і HOG

Дескриптор	Набір даних	Роздільна здатність	Кількість суб'єктів / зображень	Точність
HOG + LBP [85]	LFW	58×50	N/A	75-94%
	AR		N/A	88-93%
	Yale		N/A	86-97%
HOG + LBP [89]	Yale	N/A	N/A	86.47-92%
OC-LBP + HOG [86]	ORL	64×64	N/A	91-96%
	Yale	64×64	N/A	85.4-100%
	FERET	64×64	N/A	82.3-100%
HOG + LBP + KNN [87]	N/A	N/A	10 / 100	82.5%
CS-NWALBP + HOG [88]	CMUPIE	112×112	40 / 240	72.8-94.2%
	Yale B	192×168	N/A	97-99%
	FERET	80×80	40 / 240	79.1-96.6%
1DLBP + HOG	DoF (ORL)	92×112	40 / 120	72.5%
	FERET	256×384	40 / 99	75%
	SCface	108×144	40 / 160	95%

Також показники точності ідентифікації запропонованого комплексного методу можна порівняти з результатами найбільш поширених методів на основі нейронних мереж, зазначеними в огляді літератури, зокрема в роботі [27]. Результати експериментів наведено в Таблиці Б.14. Для порівняння використано найвищі показники точності ідентифікації серед усіх серій експериментів.

З метою порівняння запропонованого комплексного методу біометричної ідентифікації з методами на основі нейромережевого підходу, на наступному етапі дослідження були проведені експерименти на зображеннях з різними положеннями голови суб'єкта ідентифікації. Набір даних складався із зображень облич в діапазоні від лівого до правого профілю з рівними кроками у 22,5 градусів. Таким чином, для

одного суб’єкта набір містив кілька зображень з кутом огляду від -67,5 до +67,5 градусів. Експериментальні результати, наведені в Таблиці Б.15, порівнюються з результатами методу на основі нейронної мережі CNN, наведеними в роботі [90].

На Рисунку 4.19 представлена порівняльна діаграма результатів експериментів на зображеннях з варіативністю положення голови суб’єкта ідентифікації. У цій серії експериментів запропонований комплексний метод біометричної ідентифікації на основі локально-текстурних дескрипторів перевищує результати методу на основі нейронної мережі на 13,75% на зображеннях, де обличчя суб’єкта розташоване прямо (суб’єкт дивиться в камеру) і на 16,25% % на зображеннях, де обличчя об’єкта не видно повністю (об’єкт дивиться вниз).

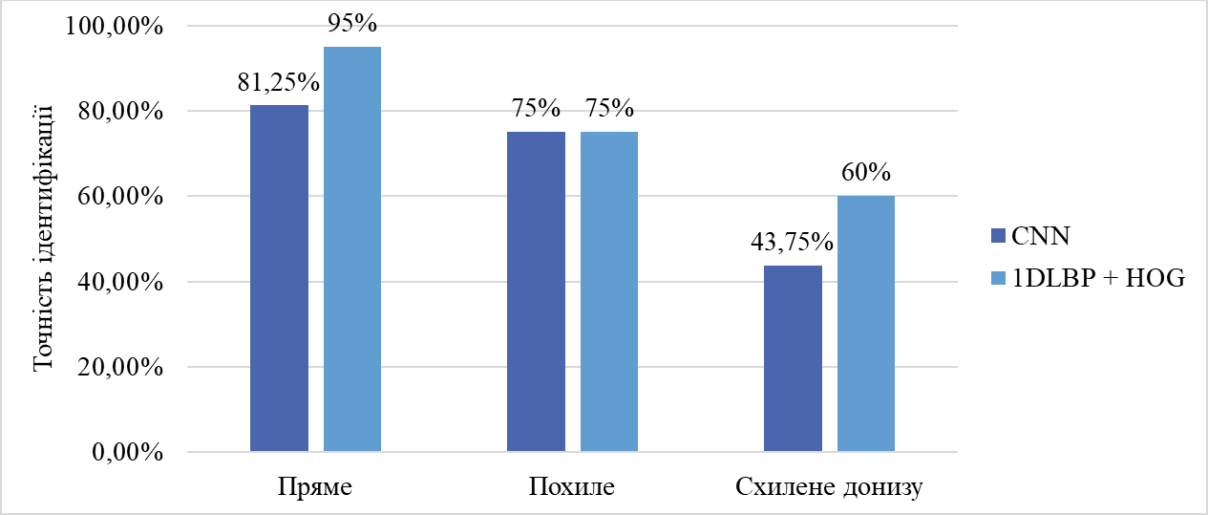


Рисунок 4.19 – Порівняльна діаграма показників точності ідентифікації методів на основі нейронної мережі та локально-текстурних дескрипторів при застосуванні до зображень обличчя за різних положень голови

Наступний набір експериментів для дослідження запропонованого комплексного методу біометричної ідентифікації проводився на зображеннях облич, нижня частина яких прихована від спостерігача, таким чином моделюючи можливість ідентифікації людини в медичній масці або балаклаві. Показники точності ідентифікації запропонованого методу порівнюються з результатами

методів на основі нейронних мереж ResNet і FaceNet, які були отримані в ході попереднього дослідження [11]. Результати експериментів представлені в Таблиці Б.16.

Порівняльну діаграму результатів експериментів із зображеннями з різною видимістю обличчя суб'єкта наведено на Рисунку 4.20. Хоча на зображеннях, де обличчя досліджуваного видно повністю, методи на основі нейронних мереж демонструють вищі результати, під час застосування до зображень з частковою видимістю обличчя ефективність таких методів значно знижується: для методу на основі нейронної мережі ResNet – на 42,5%, для методу на основі нейронної мережі FaceNet – на 26,25%. У свою чергу, показник точності ідентифікації запропонованого комплексного методу на основі локально-текстурних дескрипторів є найвищим серед усіх отриманих і становить 82,5% у порівнянні з 55% та 72%, отриманими після застосування нейромережевих методів.

Таким чином, в умовах часткової видимості рис обличчя запропонований комплексний метод біометричної ідентифікації ефективніший на 10,5-27,5% порівняно з підходами на основі FaceNet та ResNet відповідно. Відсоток зниження ефективності порівняно з результатом, отриманим на зображеннях повністю видимих облич, становить 12,5%, що є найменшим показником серед усіх експериментів.

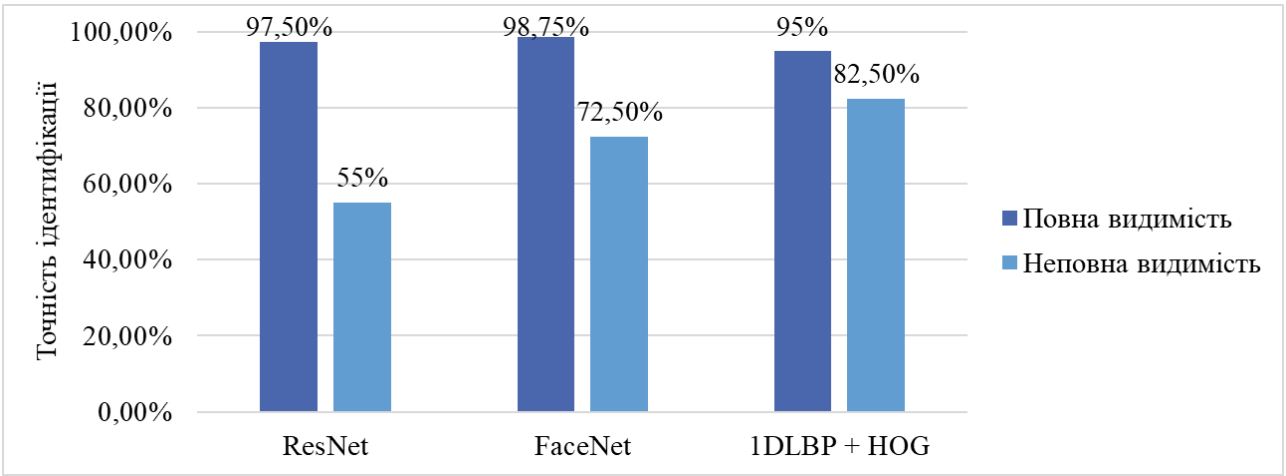


Рисунок 4.20 – Порівняльна діаграма результатів експерименту з різною видимістю обличчя суб'єкта на зображеннях

Варто наголосити на тому, що більшість підходів до розпізнавання облич на сьогоднішній день здебільшого базуються на методах штучного інтелекту, таких як нейронні мережі та методи машинного навчання. Зазвичай, щоб розпочати застосування до зображень з неповністю видимими рисами облич, такі методи потребують попереднього навчання на великих вибірках даних для того, щоб продемонструвати високі результати, що, у свою чергу, займає велику кількість ресурсів, зокрема часу та обчислювальної потужності, для коректного налаштування методів ідентифікації. Натомість, методи на основі локально-текстурних методів не потребують додаткових ресурсів або даних для навчання та налаштування, при цьому точність ідентифікації таких методів є наближеною до точності найбільш поширених і використовуваних методів при використанні в умовах неповної видимості облич.

Висновки до розділу 4

Четвертий розділ присвячено експериментальному дослідженню розробленого комплексного методу біометричної ідентифікації за зображенням обличчя на основі локально-текстурних дескрипторів. Під час проведення дослідження отримано наступні результати:

1. Експериментально підтверджено, що найвищих показників точності ідентифікації запропонований комплексний метод досягає при застосуванні одночасно двох локально-текстурних дескрипторів (локальні бінарні шаблони в одновимірному просторі та гістограми орієнтованих градієнтів), що використовуються для вилучення векторів ознак із зображень облич. При цьому найвищу точність ідентифікації 95% у даному наборі експериментів отримано при застосуванні запропонованого комплексного методу до набору даних SCface, що містить зображення облич низької якості. На зображеннях з наборів даних The Database of Faces і FERET показники точність склали 70% і 72,5% відповідно.

2. Враховуючи велику варіативність показників точності ідентифікації на зображеннях з різних наборів даних, досліджено такі чинники впливу на

ефективність запропонованого комплексного методу, як стиснення зображень в залежності від формату файлу, в якому вони збережені; різноманітність роздільної здатності зображень; область обличчя, яка покриває зображення. Крім того, досліджено ефективність запропонованого комплексного методу біометричної ідентифікації при застосуванні до зображень в умовах неповної видимості рис облич.

3. Експериментально встановлено, що в окремих випадках ефективність запропонованого комплексного методу біометричної ідентифікації залежить від формату стиснення зображень облич, до яких він застосовується, а застосування відповідного перетворення дозволяє отримати зростання показника точності на 5-10%.

4. Експериментально підтверджено, що перетворення роздільної здатності зображень облич, до яких застосовується запропонований комплексний метод, дозволяє отримати підвищення показника точності ідентифікації на 5-30%.

5. Експериментально доведено, що перетворення роздільної здатності області обличчя, що міститься на зображеннях, дозволяє підвищити показник точності ідентифікації на 5-25%.

6. Експериментально встановлено, що в окремих випадках ефективність запропонованого комплексного методу біометричної ідентифікації є вищою на 5% при застосуванні його до зображень, що містять обличчя з неповністю видимими рисами.

7. Шляхом аналізу отриманих результатів встановлено, що найбільш ефективним є застосування запропонованого комплексного методу біометричної ідентифікації до зображень, зафіксованих у напівконтрольованих або контрольованих умовах навколишнього середовища. З метою підвищення точності ідентифікації комплексного методу сформульовано вимоги до зображень, що подаються на вхід методу.

8. Найвищий показник точності ідентифікації комплексного методу, що становить 95%, отримано при застосуванні його до зображень з набору даних SCface, що містить низькоякісні зображення, зафіксовані камерами

відеоспостереження. Таким чином, запропонований комплексний метод біометричної ідентифікації забезпечує високу точність ідентифікації на зображеннях обличчя низької якості.

9. У результаті порівняльного аналізу визначено, що запропонована комбінація локально-текстурних дескрипторів локальні бінарні шаблони в одновимірному просторі (1DLBP) та гістограми орієнтованих градієнтів (HOG), що лежать в основі комплексного методу біометричної ідентифікації, перевершує показники точності методів на основі методів LBP і HOG на 1-12.5% та аналогічних дескрипторів на 3.65-42.92%.

10. Встановлено, що точність ідентифікації комплексного методу на основі локально-текстурних дескрипторів є наближеною до показників алгоритмів на основі методів штучного інтелекту, які є більш поширеними методами для розпізнавання облич на поточний момент, та перевищує точність деяких методів на 0.5-35.5%. Оскільки локально-текстурні дескриптори характеризуються деякими перевагами щодо кількості ресурсів і даних, необхідних для їх використання, виявлено необхідність у подальшому дослідженні використання таких методів у завданнях розпізнавання облич.

ВИСНОВКИ

Дисертаційне дослідження присвячено вирішенню актуального наукового завдання підвищення ефективності програмного забезпечення біометричної ідентифікації за зображенням обличчя на основі локально-текстурних дескрипторів при варіативності якості зображень та умов їх фіксації.

Основні результати роботи полягають у наступному:

1. Здійснено огляд та аналіз програмних рішень у сфері біометричної ідентифікації, виявлено виклики, що постають при розв’язанні задачі біометричної ідентифікації за зображенням обличчя, та обґрунтовано доцільність застосування локально-текстурних дескрипторів для підвищення точності процесу біометричної ідентифікації.

2. Вперше обґрунтовано доцільність одночасного застосування методів вилучення ознак із зображень на основі локально-текстурних дескрипторів 1DLBP (локальні бінарні шаблони в одновимірному просторі) та HOG (гістограми орієнтованих градієнтів), що забезпечило підвищення точності біометричної ідентифікації в програмному забезпеченні порівняно з використанням кожного дескриптора окремо.

3. Розроблено математичне підґрунтя розв’язання задачі біометричної ідентифікації, що включає вибір методів виявлення обличчя на зображенні, попередньої обробки, обробки зображення, вилучення вектору ознак і його класифікації. Вперше запропоновано комплексний метод біометричної ідентифікації за зображенням обличчя, який заснований на методах Віола-Джонса на основі каскадів Гаара, анізотропної дифузії, вейвлет-перетворення Ґабора, комбінації локально-текстурних дескрипторів 1DLBP (локальні бінарні шаблони в одновимірному просторі) та HOG (гістограми орієнтованих градієнтів) та метрики квадратної евклідової відстані.

4. Удосконалено розроблений комплексний метод біометричної ідентифікації шляхом визначення оптимальних параметрів методу вейвлет-перетворення Ґабора,

що підвищило ефективність комплексного методу біометричної ідентифікації за зображенням обличчя.

5. Виконано проєктування та реалізацію програмної компоненти на основі розробленого комплексного методу біометричної ідентифікації за зображенням обличчя, визначено її функціональні можливості, сценарії функціонування, архітектуру та інформаційне забезпечення відповідно до принципів програмної інженерії.

6. Здійснено експериментальне дослідження розробленого комплексного методу біометричної ідентифікації за зображенням обличчя, оцінено його ефективність на зображеннях з варіативністю якості та умов фіксації, порівняно результати з існуючими рішеннями та сформулювано вимоги до вхідних даних.

7. Встановлено, що в окремих випадках ефективність запропонованого комплексного методу біометричної ідентифікації зростає на 5-10% при використанні перетворення формату стиснення зображень облич, до яких застосовується метод.

8. Підтверджено, що показник точності запропонованого комплексного методу біометричної ідентифікації підвищується на 5-30% при використанні перетворення роздільної здатності зображень облич, до яких застосовується метод.

9. Встановлено, що точність ідентифікації запропонованого комплексного методу зростає на 5-25% при використанні перетворення роздільної здатності області обличчя, що міститься на зображеннях, до яких застосовується метод.

10. Виявлено, що точність ідентифікації запропонованого комплексного методу є вищою на 5% в окремих випадках застосування методу до зображень, що містять обличчя з неповністю видимими рисами.

11. Шляхом аналізу результатів встановлено, що найбільш ефективним є застосування запропонованого комплексного методу біометричної ідентифікації до зображень, зафіксованих у напівконтрольованих або контрольованих умовах навколишнього середовища. Сформульовано вимоги до зображень, до яких застосування запропонованого комплексного методу біометричної ідентифікації є найбільш ефективним.

12. Найвищий показник точності ідентифікації розробленого комплексного методу становить 95% при застосуванні його до набору зображень низької якості, зафіксованих камерами відеоспостереження. Такий результат дозволяє зробити висновок, що запропонований комплексний метод забезпечує високу точність ідентифікації на зображеннях обличчя низької якості.

13. Встановлено, що точність ідентифікації запропонованого комплексного методу на основі локально-текстурних дескрипторів перевершує показники точності аналогічних методів на 1-42,92%, а також є наближеною до показників алгоритмів на основі методів штучного інтелекту, які є більш поширеними методами для розпізнавання облич на поточний момент, перевищуючи точність деяких методів на 0.5-35.5%. Враховуючи, що локально-текстурні дескриптори характеризуються деякими перевагами щодо кількості ресурсів і даних, необхідних для їх використання, виявлено необхідність у подальшому дослідженні застосування таких методів до завдань розпізнавання облич.

Виходячи з вищенаведених висновків, мету дисертаційного дослідження досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Facial Recognition – Worldwide. Statista – The Statistics Portal for Market Data, Market Research and Market Studies. [Online]. Available: https://www.statista.com/outlook/tmo/artificial-intelligence/computer-vision/facial-recognition/worldwide

2. Say hello to the new face of efficiency, security and safety. Introducing Biometric Facial Comparison Technology. U.S. Customs and Border Protection. [Online]. Available: https://www.cbp.gov/travel/biometrics

3. P. Bischoff, “Facial recognition technology (FRT): Which countries use it? [100 analyzed],” Comparitech, January 24, 2022. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/

4. Facial Recognition. INTERPOL, The International Criminal Police Organization. [Online]. Available: https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition

5. T. Ryan-Mosley, “The movement to limit face recognition tech might finally get a win,” MIT Technology Review, July 20, 2023. [Online]. Available: https://www.technologyreview.com/2023/07/20/1076539/face-recognition-massachusetts-test-police/

6. Q. Zhu, Y. Fang, Y. Cai, C. Chen and L. Fan, “Rethinking Scanning Strategies with Vision Mamba in Semantic Segmentation of Remote Sensing Imagery: An Experimental Study,” ArXiv, 2024, abs/2405.08493.

7. O. Bychkov, K. Merkulova and Y. Zhabska, “Software Application for Biometrical Person’s Identification by Portrait Photograph Based on Wavelet Transform,” 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 253-256, doi: 10.1109/ATIT49449.2019.9030462.

8. Бичков О., Меркулова К., Жабська Є. Створення системи розпізнавання облич на основі вейвлет-перетворень. Проблеми інформаційних технологій, №26, 2019, с. 32-43, doi: 10.35546/2313-0687.2019.26.32-43.

9. O. Bychkov, K. Merkulova and Y. Zhabska, “Information Technology of Person’s Identification by Photo Portrait,” 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020, pp. 786-790, doi: 10.1109/TCSET49122.2020.235542.

10. G. P. Dimitrov, O. Bychkov, P. Petrova, K. Merkulova, Y. Zhabska et al., “Creation of Biometric System of Identification by Facial Image,” 2020 3rd International Colloquium on Intelligent Grid Metrology (SMAGRIMET), Cavtat, Croatia, 2020, pp. 29-34, doi: 10.23919/SMAGRIMET48809.2020.9263995.

11. O. Bychkov, O. Ivanchenko, K. Merkulova and Y. Zhabska, “Mathematical Methods for Information Technology of Biometric Identification in Conditions of Incomplete Data”, Proceedings of the 7th International Conference "Information Technology and Interactions" (IT&I-2020), CEUR Workshop Proceedings, vol. 2845, 2020, pp. 336-349. [Online]. Available: https://ceur-ws.org/Vol-2845/Paper_31.pdf

12. O. Bychkov, K. Merkulova, Y. Zhabska and A. Shatyrko, “Development of information technology for person identification in video stream”, Proceedings of the II International Scientific Symposium “Intelligent Solutions” (IntSol-2021), CEUR Workshop Proceedings, 2021, pp. 70-80. [Online]. Available: https://ceur-ws.org/Vol-3018/Paper_7.pdf

13. O. Bychkov, K. Merkulova and Y. Zhabska, “Information Technology for Person Identification by Occluded Face Image,” 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2022, pp. 147-151, doi: 10.1109/TCSET55632.2022.9766867.

14. Жабська Є. Інформаційна технологія ідентифікації особи за зображенням обличчя в умовах оклюзії. Енергетика і автоматика, 0(1), 2023, с. 136-149, doi: 10.31548/energiya1(65).2023.136.

15. O. Bychkov, K. Merkulova and Y. Zhabska, “Improvement of Information Technology for Person Identification for Usage in Energy Smart Systems,” 2022 IEEE

8th International Conference on Energy Smart Systems (ESS), Kyiv, Ukraine, 2022, pp. 199-203, doi: 10.1109/ESS57819.2022.9969307.

16. O. Bychkov, K. Merkulova, Y. Zhabska, “Preprocessing Methods Study to Improve Information Technology for Person Identification by Occluded Image, Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), CEUR Workshop Proceedings, vol. 3309, 2022, pp. 66-76. [Online]. Available: https://ceur-ws.org/Vol-3309/paper6.pdf

17. K. Merkulova and Y. Zhabska, “Investigating Methods of Input Data Preparation for Person Identification Information Technology,” 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2022, pp. 495-498, doi: 10.1109/CSIT56902.2022.10000539.

18. O. Bychkov, K. Merkulova and Y. Zhabska, “Research of Image Preprocessing Methods for Enhancement of Information Technology for Person Identification,” 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 293-296, doi: 10.1109/PICST57299.2022.10238550.

19. O. Bychkov, O. Ivanchenko, K. Merkulova and Y. Zhabska, “Enhancement of Information Technology for Person Identification Based on Image Quality Features,” Selected Papers of the IX International Scientific Conference “Information Technology and Implementation” (IT&I-2022), CEUR Workshop Proceedings, vol. 3347, 2022, pp. 1-10. [Online]. Available: https://ceur-ws.org/Vol-3347/Paper_1.pdf

20. V. Martsenyuk, O. Bychkov, K. Merkulova and Y. Zhabska, “Exploring Image Unified Space for Improving Information Technology for Person Identification,” in IEEE Access, vol. 11, pp. 76347-76358, 2023, doi: 10.1109/ACCESS.2023.3297488.

21. Жабська Є. О. Дослідження параметрів вхідних зображень для вдосконалення інформаційної технології ідентифікації особи. Зв'язок, №4, 2023, с. 7-12. doi: 10.31673/2412-9070.2023.042030.

22. K. Merkulova and Y. Zhabska, “Input Data Requirements for Person Identification Information Technology,” Proceedings of the 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023), CEUR Workshop

Proceedings, 2023, pp. 24-37. [Online]. Available: https://ceur-ws.org/Vol-3468/paper3.pdf

23. O. Bychkov, Y. Zhabska, K. Merkulova and M. Merkulov, “Research and Comparative Analysis of Person Identification Information Technology,” Selected Papers of the III International Scientific Symposium “Intelligent Solutions” (IntSol-2023), CEUR Workshop Proceedings, vol. 3538, 2023, pp. 54-64. [Online]. Available: https://ceur-ws.org/Vol-3538/Paper_6.pdf

24. O. Bychkov, K. Merkulova, Y. Zhabska, “Exploring Conditions of Image Samples Formation for Person Identification Information Technology”, Selected Papers of the X International Scientific Conference “Information Technology and Implementation" (IT&I 2023), CEUR Workshop Proceedings, vol. 3646, 2023, pp. 33-42. [Online]. Available: https://ceur-ws.org/Vol-3646/Paper_4.pdf

25. International standard ISO/IEC 2382937:2022. Information techology – Vocabulary – Part 37: Biometrics. [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:-37:ed-3:v1:en

26. D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, “Handbook of Fingerprint Recognition,” Springer London, 2nd edition, 2014, 494 p., doi: 10.1007/978-1-84882-254-2.

27. I. Adjabi, A. Ouahabi, A. Benzaoui and A. Taleb-Ahmed, “Past, Present, and Future of Face Recognition: A Review,” Electronics 2020, 9, 1188, doi: 10.3390/electronics9081188.

28. A. K. Jain , A. A. Ross and K. Nandakumar, “Introduction to Biometrics”, Springer New York, NY, 2011, 312 p., doi: 10.1007/978-0-387-77326-1.

29. Face++. [Online]. Available: https://www.faceplusplus.com/

30. Amazon Rekognition. [Online]. Available: https://aws.amazon.com/rekognition/

31. Azure AI Vision. [Online]. Available: https://azure.microsoft.com/en-us/products/ai-services/ai-vision

32. FaceFirst. [Online]. Available: https://www.facefirst.com/

33. NEC Face Recognition. [Online]. Available: https://www.nec.com/en/global/solutions/biometrics/face_recognition.html

34. S. Brodsky, "The Air Force's Drones Can Now Recognize Faces. Uh-Oh," Popular Mechanics, February 24, 2023. [Online]. Available: https://www.popularmechanics.com/military/a43064899/air force drones facial recognition/

35. S. Ahmed, "Dubai Police Will Now Track Careless Drivers With AI Drones," ProPakistani, February 17, 2023. [Online]. Available: https://propakistani.pk/2023/02/17/dubai-police-will-now-track-careless-drivers-with-ai-drones/

36. Clearview AI. War in Ukraine. [Online]. Available: https://www.clearview.ai/ukraine

37. N. Singh, S. S. Rathore and S. Kumar, "Towards a super-resolution based approach for improved face recognition in low resolution environment", Multimed Tools Appl, 2022, doi: 10.1007/s11042-022-13160-z

38. S. Li, Z. Liu, D. Wu, H. Huo, H. Wang and K. Zhang, "Low-resolution face recognition based on feature-mapping face hallucination", Computers and Electrical Engineering, Volume 101, 2022, 108136, ISSN 0045-7906, doi: 10.1016/j.compeleceng.2022.108136.

39. Y. Peng, L. J. Spreeuwers and R. N. Veldhuis, "Low-resolution face recognition and the importance of proper alignment", IET Biom., 8: pp. 267-276, doi: 10.1049/iet-bmt.2018.5008.

40. M. Kim, A. K. Jain and X. Liu, "AdaFace: Quality Adaptive Margin for Face Recognition," 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), New Orleans, LA, USA, 2022, pp. 18729-18738, doi: 10.1109/CVPR52688.2022.01819.

41. D. Heinsohn, E. Villalobos, L. Prieto, and D Mery, "Face Recognition in Low-Quality Images using Adaptive Sparse Representations", Image and Vision Computing, vol. 85, 2019, pp. 46-58, ISSN 0262-8856, doi: 10.1016/j.imavis.2019.02.012.

42. R. Gao, F. Yang, W. Yang and Q. Liao, “Margin Loss: Making Faces More Separable,” in IEEE Signal Processing Letters, vol. 25, no. 2, 2018, pp. 308-312, doi: 10.1109/LSP.2017.2789251.

43. F. Yang, W. Yang, R. Gao and Q. Liao, “Discriminative Multidimensional Scaling for Low-Resolution Face Recognition,” in IEEE Signal Processing Letters, vol. 25, no. 3, 2018, pp. 388-392, doi: 10.1109/LSP.2017.2746658.

44. S. P. Mudunuri and S. Biswas, “Dictionary Alignment for Low-Resolution and Heterogeneous Face Recognition,” 2017 IEEE Winter Conference on Applications of Computer Vision (WACV), 2017, pp. 1115-1123, doi: 10.1109/WACV.2017.129.

45. M. Haghighat and M. Abdel-Mottaleb, “Low Resolution Face Recognition in Surveillance Systems Using Discriminant Correlation Analysis,” 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), 2017, pp. 912-917, doi: 10.1109/FG.2017.130.

46. G. Gao, P. Huang, Q. Zhou, Z. Hu and D. Yue, “Low-Rank Representation and Locality-Constrained Regression for Robust Low-Resolution Face Recognition”, Artificial Intelligence and Robotics, Studies in Computational Intelligence, vol. 752, Springer, Cham, doi: 10.1007/978-3-319-69877-9_3.

47. P. Li, L. Prieto, D. Mery and P. J. Flynn, “On Low-Resolution Face Recognition in the Wild: Comparisons and New Techniques,” in IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, 2019, pp. 2000-2012, doi: 10.1109/TIFS.2018.2890812.

48. Z. Lu, X. Jiang, and A. Kot, “Deep coupled ResNet for low-resolution face recognition,” IEEE Signal Process. Lett., vol. 25, no. 4, pp. 526–530, Apr. 2018, doi: 10.1109/LSP.2018.2810121.

49. F. Vakhshiteh, A. Nickabadi and R. Ramachandra, “Adversarial Attacks Against Face Recognition: A Comprehensive Study,” in IEEE Access, vol. 9, pp. 92735-92756, 2021, doi: 10.1109/ACCESS.2021.3092646.

50. A. Zolfi, S. Avidan, Y. Elovici and A. Shabtai, “Adversarial Mask: Real-World Universal Adversarial Attack on Face Recognition Models,” In: Amini, MR., Canu, S., Fischer, A., Guns, T., Kralj Novak, P., Tsoumakas, G. (eds) Machine Learning and

Knowledge Discovery in Databases. ECML PKDD 2022. Lecture Notes in Computer Science(), vol. 13715. Springer, Cham, doi: 10.1007/978-3-031-26409-2_19.

51. A. Guesmi, M. A. Hanif, B. Ouni and M. Shafique, “Physical Adversarial Attacks for Camera-Based Smart Systems: Current Trends, Categorization, Applications, Research Challenges, and Future Outlook,” in IEEE Access, vol. 11, pp. 109617-109668, 2023, doi: 10.1109/ACCESS.2023.3321118.

52. Q. L. Roux, E. Bourbao, Y. Teglia and K. Kallas, “A Comprehensive Survey on Backdoor Attacks and their Defenses in Face Recognition Systems,” in IEEE Access, doi: 10.1109/ACCESS.2024.3382584.

53. Facial recognition market - growth, trends, Covid-19 impact, and forecasts (2022 - 2027). Mordor Intelligence. [Online]. Available: https://www.mordorintelligence.com/industry-reports/facial-recognition-market

54. Facial Recognition Market Size, Share & Trends Analysis Report, 2021 – 2028. Grand View Research. May 2021. 92 p. Report ID: 978-1-68038-311-9. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/facial-recognition-market

55. A. Benzaoui, A. Boukrouche, H. Doghmane and H. Bourouba, “Face recognition using 1DLBP, DWT and SVM,” 2015 3rd International Conference on Control, Engineering & Information Technology (CEIT), Tlemcen, Algeria, 2015, pp. 1-6, doi: 10.1109/CEIT.2015.7233002.

56. World Health Organization, “Mask use in the context of COVID-19: interim guidance,” World Health Organization, p. 22, 1 December 2020. [Online]. Available: https://www.who.int/publications/i/item/advice on the use of masks in the community during home care and in healthcare settings in the context of the novel coronavirus-(2019-ncov)-outbreak

57. M. Ngan, P. Grother and K. Hanaoka, “Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre- COVID-19 algorithms,” NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, doi: 10.6028/NIST.IR.8311.

58. F. Boutros, N. Damer, J. Kolf, K. Raja, F. Kirchbuchner, R. Ramachandra, A. Kuijper, P. Fang, C. Zhang, F. Wang and D. Montero, et al., “MFR 2021: Masked Face Recognition Competition,” 2021 IEEE International Joint Conference on Biometrics, IJCB 2021, 2021, doi:10.1109/IJCB52358.2021.9484337.

59. M. Ngan, P. Grother and K. Hanaoka, “Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms”, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2020, doi: 10.6028/NIST.IR.8331.

60. D. Ait Aouit and A. Ouahabi, “Suivi de fissuration de matériaux par thermographie,” Comptes Rendus Mécanique, vol. 336, no. 8, 2008, pp. 677–683, doi: 10.1016/j.crme.2008.06.001.

61. S. Arya, N. Pratap and K. Bhatia, “Future of Face Recognition: A Review,” Procedia Computer Science, vol. 58, 2015, pp. 578–585, doi: 10.1016/j.procs.2015.08.076.

62. S. Zafeiriou, C. Zhang and Z. Zhang, “A survey on face detection in the wild: Past, present and future,” Computer Vision and Image Understanding, vol. 138, 2015, pp. 1–24, doi: 10.1016/j.cviu.2015.03.015.

63. G. Guo and N. Zhang, “A survey on deep learning based face recognition,” Computer Vision and Image Understanding, vol. 189, 2019, 10285, doi: 10.1016/j.cviu.2019.102805.

64. R. Min, S. Xu and Z. Cui, “Single-Sample Face Recognition Based on Feature Expansion,” in IEEE Access, vol. 7, pp. 45219-45229, 2019, doi: 10.1109/ACCESS.2019.2909039.

65. Dx. Zhang, P. An and Hx. Zhang, “Application of robust face recognition in video surveillance systems,” Optoelectronics Letters, vol. 14, 2018, pp. 152–155, doi: 10.1007/s11801-018-7199-6.

66. A.K. Jain and A. Kumar, “Biometric Recognition: An Overview”, In: Mordini, E., Tzovaras, D. (eds) Second Generation Biometrics: The Ethical, Legal and Social Context, The International Library of Ethics, Law and Technology, vol. 11. Springer, Dordrecht, 2012, pp. 49-79, doi: 10.1007/978-94-007-3892-8_3.

67. P. Viola and M. J. Jones, “Rapid Object Detection using a Boosted Cascade of Simple Features”, Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 1, 2001, pp. 511-518.

68. B. Boser, I. M. Guyon and V. Vapnik, “A training algorithm for optimal margin classifiers,” ACM Workshop on Conference on Computational Learning Theory (COLT), 1992, pp. 142-152.

69. M. Nilsson, J. Nordberg and I. Claesson, “Face Detection using Local SMQT Features and Split up Snow Classifier,” 2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07, Honolulu, HI, USA, 2007, pp. II-589-II-592, doi: 10.1109/ICASSP.2007.366304.

70. K.-K. Sung and T. Poggio, “Example-based learning for view-based human face detection,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 1, pp. 39-51, Jan. 1998, doi: 10.1109/34.655648.

71. K. Dang and S. Sharma, “Review and comparison of face detection algorithms,” 2017 7th International Conference on Cloud Computing, Data Science & Engineering – Confluence, Noida, India, 2017, pp. 629-633, doi: 10.1109/CONFLUENCE.2017.7943228.

72. K. Dharavath, G. Amarnath, F. A. Talukdar and R. H. Laskar, “Impact of image preprocessing on face recognition: A comparative analysis,” 2014 International Conference on Communication and Signal Processing, Melmaruvathur, India, 2014, pp. 631-635, doi: 10.1109/ICCSP.2014.6949918.

73. K. Dharavath, F. A. Talukdar and R. H. Laskar, “Improving Face Recognition Rate with Image Preprocessing,” Indian Journal of Science and Technology, vol. 7, no. 8, 2014, pp. 1170-1175, doi: 10.17485/ijst/2014/v7i8.26.

74. B. Zhang, S. Shan, X. Chen and W. Gao, “Histogram of Gabor Phase Patterns (HGPP): A Novel Object Representation Approach for Face Recognition,” in IEEE Transactions on Image Processing, vol. 16, no. 1, pp. 57-68, Jan. 2007, doi: 10.1109/TIP.2006.884956.

75. S. Anila and Dr. N. Devarajan, “Preprocessing Technique for Face Recognition Applications under Varying Illumination Conditions,” Global Journal of Computer Science and Technology, Graphics & Vision, vol. 12, no. 11, 2012.

76. R. L. Jyothi and M. Abdul Rahiman, “Comparative Analysis Of Wavelet Transforms In The Recognition Of Ancient Grantha Script,” International Journal of Computer Theory and Engineering, vol. 9, no. 4, 2017, pp. 235–241.

77. S. Sridhar, P. Rajesh Kumar and K. V. Ramanaiah, “Wavelet Transform Techniques For Image Compression – An Evaluation,” I.J. Image, Graphics and Signal Processing, vol. 2, 2014. pp. 54–67, doi: 10.5815/ijigsp.2014.02.07.

78. I. Daubechies, “Orthonormal bases of compactly supported wavelets,” Communications on Pure and Applied Mathematics, vol. 41, 1988, pp. 909–996.

79. A. Cohen, I. Daubechies and J. C. Feauveau, “Biorthogonal bases of compactly supported wavelets,” Communications on Pure and Applied Mathematics, vol. 45(5), 1992, pp. 485-500.

80. D. Gabor, “Theory of Communication,” Journal of the Institution of Electrical Engineers—Part III: Radio and Communication, vol. 93, pp. 429-457, doi: 10.1049/ji-3-2.1946.0076.

81. D. J. Field, “Relation between the statistics of natural images and the response properties of cortical cells,” Journal of the Optical Society of America. A, Optics and image science, vol. 4(12), 1987, pp. 2379-2394.

82. R. Srinivasa Perumal and P. V. S. S. R. Chandra Mouli, “A Comparative Analysis of Local Pattern Descriptors for Face Recognition,” Knowledge Computing and its Applications, Springer, Singapore, 2018, pp. 129-154, doi: 10.1007/978-981-10-8258-0_7.

83. J. Lizé, V. Débordès, H. Lu, K. Kpalma and J. Ronsin, “Local Binary Pattern and Its Variants: Application to Face Analysis,” Advances in Smart Technologies Applications and Case Studies, Lecture Notes in Electrical Engineering, vol. 684, Springer, Cham, 2020, doi: 10.1007/978-3-030-53187-4_11.

84. A. Eleyan, “Statistical local descriptors for face recognition: a comprehensive study,” Multimedia Tools and Applications, vol. 82, 2023, pp. 32485-32504, doi: 10.1007/s11042-023-14482-2.

85. M. Ghorbani, A. T. Targhi and M. M. Dehshibi, “HOG and LBP: Towards a robust face recognition system,” 2015 Tenth International Conference on Digital Information Management (ICDIM), Jeju, Korea (South), 2015, pp. 138-141, doi: 10.1109/ICDIM.2015.7381860.

86. I. Chhabra and G. Singh, “Effective and Fast Face Recognition System Using Complementar OC-LBP and HOG Feature Descriptors With SVM Classifier,” Journal of Information Technology Research, vol. 11, no. 1, 2018, pp. 91-110, doi: 10.4018/JITR.2018010106.

87. S. Adnan, F. Ali and A. A. Abdulmunem, “Facial Feature Extraction For Face Recognition,” Journal of Physics: Conference Series, vol. 1664, 2020, doi: 10.1088/1742-6596/1664/1/012050.

88. T. Chen, T. Gao, S. Li, X. Zhang, J. Cao, D. Yao and Y. Li. “A novel face recognition method based on fusion of LBP and HOG”, IET Image Processing, vol. 15, 2021, pp. 3559-3572, doi: 10.1049/ipr2.12192.

89. V. Panditpautra, A. Goswami, A. Khavare and S. Ambadekar, “Biometric Attendance Management System Using Raspberry Pi”, 2nd International Conference on Advances in Science & Technology (ICAST), 2019, doi: 10.2139/ssrn.3368163.

90. A. Budiman, Fabian, R. A. Yaputera, S. Achmad and A. Kurniawan, “Student attendance with face recognition (LBPH or CNN): Systematic literature review,” Procedia Computer Science, vol. 216, 2023, pp. 31-38, doi: 10.1016/j.procs.2022.12.108.

91. A. P. Rajan and A. R. Mathew, “Evaluation and Applying Feature Extraction Techniques for Face Detection and Recognition,” Indonesian Journal of Electrical Engineering and Informatics (IJEEI), Vol. 7, No. 4, 2019, pp. 742-749, doi: 10.52549/ijeei.v7i4.935.

92. C. Li, Y. Huang, W. Huang and F. Qin, “Learning features from covariance matrix of gabor wavelet for face recognition under adverse conditions,” Pattern Recognition, Vol. 119, 2021, doi: 10.1016/j.patcog.2021.108085.

93. B. Attallah, A. Serir, Y. Chahir and A. Boudjelal, “Histogram of gradient and binarized statistical image features of wavelet subband-based palmprint features extraction," Journal of Electronic Imaging, vol. 26, no. 6, 063006, 2017, doi: 10.1117/1.JEI.26.6.063006.

94. T. Ojala, M. Pietikainen and D. Harwood, “A comparative study of texture measures with classification based on featured distribution,” Pattern Recognition, vol. 29, no. 1, 1996, pp. 51-59, doi: 10.1016/0031-3203(95)00067-4.

95. A. Benzaoui and A. Boukrouche, “1DLBP and PCA for face recognition,” 2013 11th International Symposium on Programming and Systems (ISPS), Algiers, Algeria, 2013, pp. 7-11, doi: 10.1109/ISPS.2013.6581486.

96. A. Hajraoui, M. Sabri and M. Fakir. “Face recognition: synthesis of classification methods,” International Journal of Computer Science and Information Security, vol. 14, no. 2, 2016.

97. P. Viola and M. J. Jones, “Robust real-time face detection”, International Journal of Computer Vision, vol. 57(2), 2004, pp. 137-154.

98. P. Perona and J. Malik, “Scale-space and edge detection using anisotropic diffusion,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, no. 7, pp. 629-639, July 1990, doi: 10.1109/34.56205.

99. T. M. Abhishree, J. Latha, K. Manikantan and S. Ramachandran, “Face Recognition Using Gabor Filter Based Feature Extraction with Anisotropic Diffusion as a Pre-processing Technique,” Procedia Computer Science, vol. 45, 2015, pp. 312-321, ISSN 1877-0509, doi: 10.1016/j.procs.2015.03.149.

100. C. Yu and Y. Jia, “Anisotropic Diffusion-based Kernel Matrix Model for Face Liveness Detection,” ArXiv, 2017, abs/1707.02692.

101. J. Weickert, “Anisotropic Diffusion in Image Processing,” B. G. Teubner Stuttgart, 1998, 198 p.

102. J. G. Daugman, “Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression,” in IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 36, no. 7, 1988, pp. 1169-1179, doi: 10.1109/29.1644.

103. J. R. Movellan, “Tutorial on Gabor Filters,” 2002, 23 p. [Online]. Available: https://inc.ucsd.edu/mplab/tutorials/gabor.pdf

104. V. Dakshayani, G. R. Locharla, P. Pławiak, V. Datti and C. Karri, “Design of a Gabor Filter-Based Image Denoising Hardware Model”, Electronics, vol. 11, no. 7, 1063, 2022, doi: 10.3390/electronics11071063.

105. J. P. Jones and L. A. Palmer, “An evaluation of the two-dimensional Gabor filter model of simple receptive fields in cat striate cortex,” J. Neuropkysiol, vol. 58(6), 1987, pp. 1233-1258, doi: 10.1152/jn.1987.58.6.1233.

106. J. G. Nicholls et al., “From neuron to brain,” Sinauer Associates is an imprint of Oxford University Press, 5th edition, 2011, 768 p.

107. L. Wiskott, N. Krüger, N. Kuiger and C. von der Malsburg, “Face recognition by elastic bunch graph matching,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, 1997, pp. 775-779, doi: 10.1109/34.598235.

108. F. S. Samaria and A. C. Harter, “Parameterisation of a stochastic model for human face identification,” Proceedings of 1994 IEEE Workshop on Applications of Computer Vision, Sarasota, FL, USA, 1994, pp. 138-142. doi: 10.1109/ACV.1994.341300.

109. P. J. Phillips, H. Moon, S. A. Rizvi and P. J. Rauss, “The FERET Evaluation Methodology for Face Recognition Algorithms,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, 2000, pp. 1090-1104, doi: 10.1109/34.879790.

110. M. Grgic, K. Delac and S. Grgic, “SCface – surveillance cameras face database,” Multimedia Tools and Applications Journal, vol. 51, no. 3, 2011, pp. 863-879.

111. S. Moschoglou, A. Papaioannou, C. Sagonas, J. Deng, I. Kotsia and S. Zafeiriou, “AgeDB: The First Manually Collected, In-the-Wild Age Database,” 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA, 2017, pp. 1997-2005, doi: 10.1109/CVPRW.2017.250.

112. S. Sengupta, J. -C. Chen, C. Castillo, V. M. Patel, R. Chellappa and D. W. Jacobs, “Frontal to profile face verification in the wild,” 2016 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Placid, NY, USA, 2016, pp. 1-9, doi: 10.1109/WACV.2016.7477558.

113. G. B. Huang, M. Ramesh, T. Berg and E. Learned-Mille, “Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments,” University of Massachusetts, Amherst, Technical Report 07-49, October, 2007.

114. Z. Cheng, X. Zhu and S. Gong, “TinyFace: Face Recognition in Native Low-resolution Imagery”. [Online]. Available: https://qmul-tinyface.github.io/

115. P. Li, L. Prieto, D. Mery and P. J. Flynn, “Face Recognition in Low Quality Images: A Survey,” ArXiv, 2018, abs/1805.11519, 2018.

116. World Health Organization, “Coronavirus disease (COVID-19): Masks,” World Health Organization, 5 January 2022. [Online]. Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19-masks

117. H. Dadi and P.G. Mohan, “Enhancement of Face Recognition Rate by Data Base Pre-processing”, International Journal of Computer Science and Information Technologies, vol. 6(3), 2015m pp. 2978-2984.

118. N. Dalal and B. Triggs, “Histograms of oriented gradients for human detection,” 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), vol. 1, 2005, pp. 886-893 doi: 10.1109/CVPR.2005.177.

119. S. Brahnam, L. C. Jain, L. Nanni & A. Lumini, “Local Binary Patterns: New Variants and Applications,” Studies in Computational Intelligence, Springer Berlin, Heidelberg, vol. 506, 2014, 271 p., doi: 10.1007/978-3-642-39289-4.

120. M. Miranda-Viana, D. V. Madlum, N. Oliveira-Santos et al., “Influence of the image file format of digital periapical radiographs on the diagnosis of external and internal root resorptions”, Clinical Oral Investigations, vol. 25 (8), 2021, pp. 4941–4948, doi: 10.1007/s00784-021-03803-0.

121. Y. Zhou, D. Liu and T. Huang, “Survey of Face Detection on Low-Quality Images,” 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), 2018, pp. 769-773, doi: 10.1109/FG.2018.00121.

122. A. Eleyan, “Statistical local descriptors for face recognition: a comprehensive study,” Multimedia Tools and Applications, vol. 82, 2023, pp. 32485-32504, doi: 10.1007/s11042-023-14482-2.

ДОДАТОК А

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. O. Bychkov, K. Merkulova and Y. Zhabska, “Software Application for Biometrical Person’s Identification by Portrait Photograph Based on Wavelet Transform,” 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 253-256, doi: 10.1109/ATIT49449.2019.9030462.

2. Бичков О., Меркулова К., Жабська Є. Створення системи розпізнавання облич на основі вейвлет-перетворень. Проблеми інформаційних технологій, №26, 2019, с. 32-43, doi: 10.35546/2313-0687.2019.26.32-43.

3. G. P. Dimitrov, O. Bychkov, P. Petrova, K. Merkulova, Y. Zhabska et al., “Creation of Biometric System of Identification by Facial Image,” 2020 3rd International Colloquium on Intelligent Grid Metrology (SMAGRIMET), Cavtat, Croatia, 2020, pp. 29-34, doi: 10.23919/SMAGRIMET48809.2020.9263995.

4. O. Bychkov, K. Merkulova and Y. Zhabska, “Information Technology for Person Identification by Occluded Face Image,” 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2022, pp. 147-151, doi: 10.1109/TCSET55632.2022.9766867.

5. V. Martsenyuk, O. Bychkov, K. Merkulova and Y. Zhabska, “Exploring Image Unified Space for Improving Information Technology for Person Identification,” in IEEE Access, vol. 11, pp. 76347-76358, 2023, doi: 10.1109/ACCESS.2023.3297488.

6. K. Merkulova and Y. Zhabska, “Input Data Requirements for Person Identification Information Technology,” Proceedings of the 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023), CEUR Workshop Proceedings, 2023, pp. 24-37. [Online]. Available: https://ceur-ws.org/Vol-3468/paper3.pdf

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. O. Bychkov, K. Merkulova and Y. Zhabska, “Information Technology of Person’s Identification by Photo Portrait,” 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020, pp. 786-790, doi: 10.1109/TCSET49122.2020.235542.

2. O. Bychkov, K. Merkulova, Y. Zhabska and A. Shatyrko, “Development of information technology for person identification in video stream”, Proceedings of the II International Scientific Symposium “Intelligent Solutions” (IntSol-2021), CEUR Workshop Proceedings, 2021, pp. 70-80. [Online]. Available: https://ceur-ws.org/Vol-3018/Paper_7.pdf

3. O. Bychkov, K. Merkulova and Y. Zhabska, “Improvement of Information Technology for Person Identification for Usage in Energy Smart Systems,” 2022 IEEE 8th International Conference on Energy Smart Systems (ESS), Kyiv, Ukraine, 2022, pp. 199-203, doi: 10.1109/ESS57819.2022.9969307.

4. K. Merkulova and Y. Zhabska, “Investigating Methods of Input Data Preparation for Person Identification Information Technology,” 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2022, pp. 495-498, doi: 10.1109/CSIT56902.2022.10000539.

5. O. Bychkov, O. Ivanchenko, K. Merkulova and Y. Zhabska, “Enhancement of Information Technology for Person Identification Based on Image Quality Features,” Selected Papers of the IX International Scientific Conference “Information Technology and Implementation” (IT&I-2022), CEUR Workshop Proceedings, vol. 3347, 2022, pp. 1-10. [Online]. Available: https://ceur-ws.org/Vol-3347/Paper_1.pdf

6. O. Bychkov, Y. Zhabska, K. Merkulova and M. Merkulov, “Research and Comparative Analysis of Person Identification Information Technology,” Selected Papers of the III International Scientific Symposium “Intelligent Solutions” (IntSol-2023), CEUR Workshop Proceedings, vol. 3538, 2023, pp. 54-64. [Online]. Available: https://ceur-ws.org/Vol-3538/Paper_6.pdf

7. O. Bychkov, K. Merkulova, Y. Zhabska, “Exploring Conditions of Image Samples Formation for Person Identification Information Technology”, Selected Papers of the X International Scientific Conference “Information Technology and Implementation" (IT&I 2023), CEUR Workshop Proceedings, vol. 3646, 2023, pp. 33-42. [Online]. Available: https://ceur-ws.org/Vol-3646/Paper_4.pdf

Наукові праці, які додатково відображають наукові результати дисертації:

1. O. Bychkov, O. Ivanchenko, K. Merkulova and Y. Zhabska, “Mathematical Methods for Information Technology of Biometric Identification in Conditions of Incomplete Data”, Proceedings of the 7th International Conference "Information Technology and Interactions" (IT&I-2020), CEUR Workshop Proceedings, vol. 2845, 2020, pp. 336-349. [Online]. Available: https://ceur-ws.org/Vol-2845/Paper_31.pdf

2. Жабська Є. Інформаційна технологія ідентифікації особи за зображенням обличчя в умовах оклюзії. Енергетика і автоматика, 0(1), 2023, с. 136-149, doi: 10.31548/energiya1(65).2023.136.

3. O. Bychkov, K. Merkulova, Y. Zhabska, “Preprocessing Methods Study to Improve Information Technology for Person Identification by Occluded Image,” Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), CEUR Workshop Proceedings, vol. 3309, 2022, pp. 66-76. [Online]. Available: https://ceur-ws.org/Vol-3309/paper6.pdf

4. O. Bychkov, K. Merkulova and Y. Zhabska, “Research of Image Preprocessing Methods for Enhancement of Information Technology for Person Identification,” 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 293-296, doi: 10.1109/PICST57299.2022.10238550.

5. Жабська Є. О. Дослідження параметрів вхідних зображень для вдосконалення інформаційної технології ідентифікації особи. Зв'язок, №4, 2023, с. 7-12. doi: 10.31673/2412-9070.2023.042030.

Відомості про апробацію результатів дисертації:

1. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT 2019, Київ, 18-20 грудня 2019 року);
2. 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (Славське, 25-29 лютого 2020 року);
3. 3rd International Colloquium on Intelligent Grid Metrology (SMAGRIMET 2020, Дубровнік, 20-23 жовтня 2020 року);
4. 7th International Conference “Information Technology and Interactions” (IT&I 2020, Київ, 2-3 грудня 2020 року);
5. 2nd International Scientific Symposium “Intelligent Solutions” (IntSol 2021, Київ-Ужгород, 28-30 вересня 2021);
6. 16th IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET 2022, Львів-Славське, 22-26 лютого 2022 року);
7. 8th IEEE International Conference on Energy Smart Systems (ESS 2022, Київ, 12-14 жовтня 2022 року);
8. 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022, Тернопіль, 22-24 листопада 2022 року);
9. 17th IEEE International Conference on Computer Science and Information Technologies (CSIT 2022, Львів. 10-12 листопада 2022 року);
10. 4th International Scientific Conference “Information Technology and Implementation” (IT&I 2022, Київ, 30 листопада – 2 грудня 2022 року);
11. 9th IEEE International Conference on Problems of Infocommunications Science and Technology (PICS&T 2022, Харків, 10-12 жовтня 2022 року);
12. 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023, Тернопіль, 14-16 червня 2023 року);
13. 3rd International Scientific Symposium “Intelligent Solutions” (IntSol 2023, Київ, 27-28 вересня 2023 року);
14. 10th International Scientific Conference “Information Technology and Implementation” (IT&I-WS 2023, Київ, 20-21 листопада 2023 року).

ДОДАТОК Б

Результати експериментального дослідження

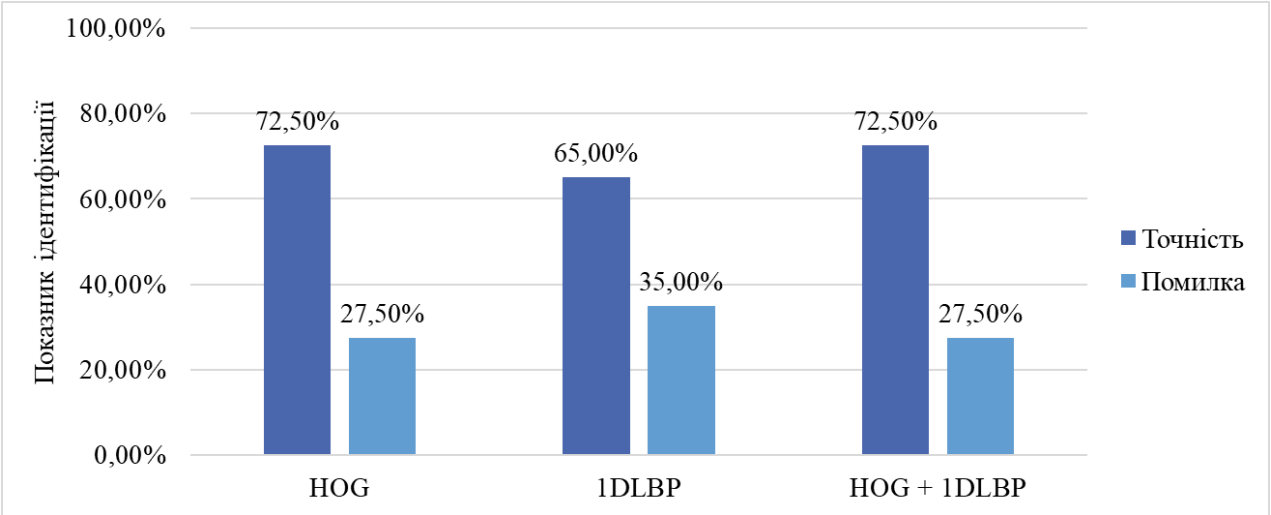


Рисунок Б.1 – Порівняльна діаграма показників точності ідентифікації комплексного методу при застосуванні до зображень з набору даних FERET

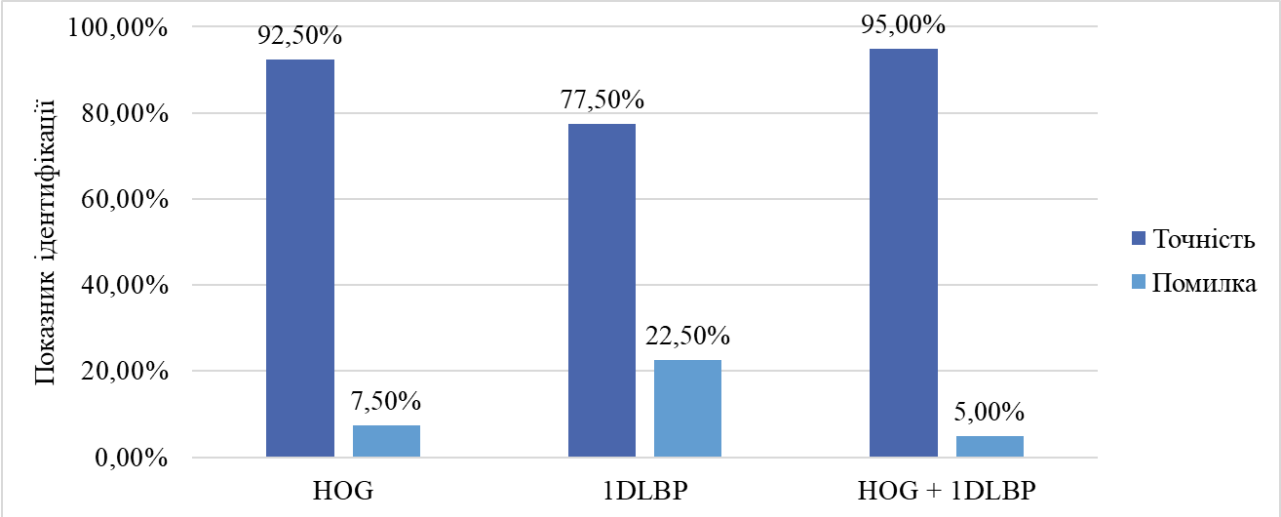


Рисунок Б.2 – Порівняльна діаграма показників точності ідентифікації комплексного методу при застосуванні до зображень з набору даних SCface

Таблиця Б.1 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних The Database of Faces, FERET і SCface з перетворенням формату

	Оригінальне зображення		BMP		PNG		JPG	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	The Database of Faces							
Всього зображень / суб'єктів	120 / 40		120 / 40		120 / 40		120 / 40	
Кількість суб'єктів	28	12	26	14	28	12	26	14
Показник ідентифікації	70%	30%	65%	35%	70%	30%	65%	35%
	FERET							
Всього зображень / суб'єктів	99 / 40		99 / 40		99 / 40		99 / 40	
Кількість суб'єктів	29	11	29	11	29	11	28	12
Показник ідентифікації	72,5%	27,5%	72,5%	27,5%	72,5%	27,5%	70%	30%
	SCface							
Всього зображень / суб'єктів	160 / 40		160 / 40		160 / 40		160 / 40	
Кількість суб'єктів	38	2	38	2	38	2	38	2
Показник ідентифікації	95%	5%	95%	5%	95%	5%	95%	5%

Таблиця Б.2 – Результати експериментального дослідження методів перетворення роздільної здатності зображень

	Всього зображень / суб'єктів		Показник ідентифікації	Кількість суб'єктів
thumbnail()				
The Database of Faces	120 / 40	Точність	75%	30
		Помилка	25%	10
FERET	99 / 40	Точність	62,5%	25
		Помилка	37,5%	15
SCface	160 / 40	Точність	77,5%	31
		Помилка	22,5%	9

Продовження Таблиці Б.2

	Всього зображень / суб'єктів		Показник ідентифікації	Кількість суб'єктів
resizing()				
The Database of Faces	120 / 40	Точність	60%	24
		Помилка	40%	16
FERET	99 / 40	Точність	67,5%	27
		Помилка	32,5%	13
SCface	160 / 40	Точність	72,5%	29
		Помилка	27,5%	11

Таблиця Б.3 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних The Database of Faces, FERET і SCface з перетворенням роздільної здатності

	ширина×91		*ширина*×100		*ширина*×128		*ширина*×144	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	The Database of Faces							
Всього зображень / суб'єктів	120 / 40		120 / 40		120 / 40		120 / 40	
	BMP							
Кількість суб'єктів	31	9	26	14	27	13	28	12
Показник ідентифікації	77,5%	22,5%	65%	35%	67,5%	32,5%	70%	30%
	PNG							
Кількість суб'єктів	31	9	26	14	28	12	28	12
Показник ідентифікації	77,5%	22,5%	65%	35%	70%	30%	70%	30%
	JPG							
Кількість суб'єктів	30	10	24	16	22	18	29	11
Показник ідентифікації	75%	25%	60%	40%	55%	45%	72,5%	27,5%
	FERET							
Всього зображень / суб'єктів	99 / 40		99 / 40		99 / 40		99 / 40	
	BMP, PNG							
Кількість суб'єктів	21	19	24	16	29	11	29	11
Показник ідентифікації	52,5%	47,5%	60%	40%	72,5%	27,5%	72,5%	27,5%
	JPG							
Кількість суб'єктів	22	18	25	15	27	13	30	10
Показник ідентифікації	55%	45%	62,5%	37,5%	67,5%	32,5%	75%	25%

Продовження Таблиці Б.3

	SCface							
Всього зображень / суб'єктів	160 / 40		160 / 40		160 / 40		160 / 40	
	BMP, PNG							
Кількість суб'єктів	25	15	27	13	33	7	37	3
Показник ідентифікації	62,5%	37,5%	67,5%	32,5%	82,5%	17,5%	92,5%	7,5%
	JPG							
Кількість суб'єктів	25	15	31	9	35	5	38	2
Показник ідентифікації	62,5%	37,5%	77,5%	22,5%	87,5%	12,5%	95%	5%

Таблиця Б.4 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних The Database of Faces, FERET і SCface з перетворенням роздільної здатності області обличчя

	32×32		47×47		64×64		78×78		128×128	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	The Database of Faces									
Всього зображень / суб'єктів	120 / 40		120 / 40		120 / 40		120 / 40		120 / 40	
	BMP, PNG									
Кількість суб'єктів	1	39	1	39	18	22	18	22	10	30
Показник ідентифікації	2,5%	97,5%	2,5%	97,5%	45%	55%	45%	55%	25%	75%
	JPG									
Кількість суб'єктів	1	39	1	39	21	19	17	23	11	29
Показник ідентифікації	2,5%	97,5%	2,5%	97,5%	52,5%	47,5%	42,5%	57,5%	27,5%	72,5%
	FERET									
Всього зображень / суб'єктів	99 / 40		99 / 40		99 / 40		99 / 40		99 / 40	
	BMP, PNG									
Кількість суб'єктів	1	39	13	27	27	13	28	12	28	12
Показник ідентифікації	2,5%	97,5%	32,5%	67,5%	67,5%	32,5%	70%	30%	70%	30%

Продовження Таблиці Б.4

	JPG									
Кількість суб'єктів	1	39	13	27	27	13	28	12	26	14
Показник ідентифікації	2,5%	97,5%	32,5%	67,5%	67,5%	32,5%	70%	30%	65%	35%
	SCface									
Всього зображень / суб'єктів	160 / 40		160 / 40		160 / 40		160 / 40		160 / 40	
	BMP, PNG									
Кількість суб'єктів	1	39	26	14	34	6	33	7	34	6
Показник ідентифікації	2,5%	97,5%	65%	35%	85%	15%	82,5%	17,5%	85%	15%
	JPG									
Кількість суб'єктів	1	39	27	13	37	3	36	4	32	8
Показник ідентифікації	2,5%	97,5%	67,5%	32,5%	92,5%	7,5%	90%	10%	80%	20%

Таблиця Б.5 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних The Database of Faces, FERET і SCface в умовах неповної видимості рис облич з перетворенням формату

	Оригінальне зображення		BMP		PNG		JPG	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	The Database of Faces							
Всього зображень / суб'єктів	120 / 40		120 / 40		120 / 40		120 / 40	
Кількість суб'єктів	26	14	26	14	26	14	29	11
Показник ідентифікації	65%	35%	65%	35%	65%	35%	72.5%	27.5%

Продовження Таблиці Б.5

	FERET							
Всього зображень / суб'єктів	99 / 40		99 / 40		99 / 40		99 / 40	
Кількість суб'єктів	26	14	26	14	26	14	31	9
Показник ідентифікації	75%	25%	75%	25%	75%	25%	77.5%	22.5%
	SCface							
Всього зображень / суб'єктів	160 / 40		160 / 40		160 / 40		160 / 40	
Кількість суб'єктів	33	7	33	7	33	7	33	7
Показник ідентифікації	82.5%	17.5%	82.5%	17.5%	82.5%	17.5%	82.5%	17.5%

Таблиця Б.6 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних The Database of Faces, FERET і SCface в умовах неповної видимості рис облич з перетворенням формату та роздільної здатності

	ширина×91		*ширина*×100		*ширина*×128		*ширина*×144	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	The Database of Faces							
Всього зображень / суб'єктів	120 / 40		120 / 40		120 / 40		120 / 40	
	BMP							
Кількість суб'єктів	27	13	27	13	28	12	25	15
Показник ідентифікації	67.5%	32.5%	67.5%	32.5%	70%	30%	62.5%	37.5%

Продовження Таблиці Б.6

	PNG							
Кількість суб’єктів	27	13	27	13	27	13	25	15
Показник ідентифікації	67.5%	32.5%	67.5%	32.5%	67.5%	32.5%	62.5%	37.5%
	JPG							
Кількість зображень	27	13	24	16	22	18	27	13
Показник ідентифікації	67.5%	32.5%	60%	40%	55%	45%	67.5%	32.5%
	FERET							
Всього зображень / суб’єктів	99 / 40		99 / 40		99 / 40		99 / 40	
	BMP, PNG							
Кількість суб’єктів	21	19	22	18	27	13	29	11
Показник ідентифікації	52.5%	47.5%	55%	45%	67.5%	32.5%	72.5%	27.5%
	JPG							
Кількість суб’єктів	21	19	22	18	28	12	29	11
Показник ідентифікації	52.5%	47.5%	55%	45%	70%	30%	72.5%	27.5%
	SCface							
Всього зображень / суб’єктів	160 / 40		160 / 40		160 / 40		160 / 40	
	BMP, PNG							
Кількість суб’єктів	15	25	18	22	29	11	34	6
Показник ідентифікації	37.5%	62.5%	45%	55%	72.5%	27.5%	85%	15%
	JPG							
Кількість суб’єктів	10	30	23	17	25	15	32	8
Показник ідентифікації	25%	75%	57.5%	42.5%	62.5%	37.5%	80%	20%

Таблиця Б.7 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних The Database of Faces, FERET і SCface в умовах неповної видимості рис облич з перетворенням формату та роздільної здатності області обличчя на зображеннях

	32×32		47×47		64×64		78×78		128×128	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	The Database of Faces									
Всього зображень / суб'єктів	120 / 40		120 / 40		120 / 40		120 / 40		120 / 40	
	BMP, PNG									
Кількість суб'єктів	1	39	1	39	17	23	16	24	10	30
Показник ідентифікації	2.5%	97.5%	2.5%	97.5%	42.5%	57.5%	40%	60%	25%	75%
	JPG									
Кількість суб'єктів	1	39	2	38	17	23	19	21	7	33
Показник ідентифікації	2.5%	97.5%	5%	95%	42.5%	57.5%	47.5%	52.5%	17.5%	82.5%
	FERET									
Всього зображень / суб'єктів	99 / 40		99 / 40		99 / 40		99 / 40		99 / 40	
	BMP, PNG									
Кількість суб'єктів	1	39	12	28	26	14	28	12	27	13
Показник ідентифікації	2.5%	97.5%	30%	70%	65%	35%	70%	30%	67.5%	32.5%
	JPG									
Кількість суб'єктів	1	39	17	23	27	13	27	13	28	12
Показник ідентифікації	2.5%	97.5%	42.5%	57.5%	67.5%	32.5%	67.5%	32.5%	70%	30%
	SCface									
Всього зображень / суб'єктів	160 / 40		160 / 40		160 / 40		160 / 40		160 / 40	
	BMP, PNG									
Кількість суб'єктів	1	39	20	20	24	16	20	20	20	20
Показник ідентифікації	2.5%	97.5%	50%	50%	60%	40%	50%	50%	50%	50%

Продовження Таблиці Б.7

	32×32		47×47		64×64		78×78		128×128	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	SCface									
	JPG									
Кількість суб'єктів	1	39	21	19	26	14	23	17	24	16
Показник ідентифікації	2.5%	97.5%	52.5%	47.5%	65%	35%	57.5%	42.5%	60%	40%

Таблиця Б.8 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних AgeDB, CFP, LFW і Tinyface з перетворенням формату

	Оригінальне зображення		BMP		PNG		JPG	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	AgeDB							
Всього зображень / суб'єктів	174 / 40		174 / 40		174 / 40		174 / 40	
Кількість суб'єктів	18	22	18	22	18	22	18	22
Показник ідентифікації	45%	55%	45%	55%	45%	55%	45%	55%
	CFP							
Всього зображень / суб'єктів	202 / 40		202 / 40		202 / 40		202 / 40	
Кількість суб'єктів	24	16	24	16	24	16	24	16
Показник ідентифікації	60%	40%	60%	40%	60%	40%	60%	40%
	LFW							
Всього зображень / суб'єктів	125 / 40		125 / 40		125 / 40		125 / 40	
Кількість суб'єктів	22	18	22	18	22	18	22	18
Показник ідентифікації	55%	45%	55%	45%	55%	45%	55%	45%

Продовження Таблиці Б.8

	Tinyface							
Всього зображень / суб'єктів	89 / 40		89 / 40		89 / 40		89 / 40	
Кількість суб'єктів	4	36	4	36	4	36	4	36
Показник ідентифікації	10%	90%	10%	90%	10%	90%	10%	90%

Таблиця Б.9 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних AgeDB, CFP, LFW і Tinyface з перетворенням роздільної здатності області обличчя

	32×32		47×47		64×64		78×78		128×128	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	AgeDB									
Всього зображень / суб'єктів	174 / 40		174 / 40		174 / 40		174 / 40		174 / 40	
Кількість суб'єктів	10	30	14	26	18	22	14	26	16	24
Показник ідентифікації	25%	75%	35%	65%	45%	55%	35%	65%	40%	60%
	CFP									
Всього зображень / суб'єктів	202 / 40		202 / 40		202 / 40		202 / 40		202 / 40	
Кількість суб'єктів	6	34	8	32	26	14	20	20	22	18
Показник ідентифікації	15%	85%	20%	80%	65%	35%	50%	50%	55%	45%
	LFW									
Всього зображень / суб'єктів	125 / 40		125 / 40		125 / 40		125 / 40		125 / 40	
Кількість суб'єктів	2	38	10	30	18	22	20	20	24	16
Показник ідентифікації	5%	95%	25%	75%	45%	55%	50%	50%	60%	40%
	Tinyface									
Всього зображень / суб'єктів	89 / 40		89 / 40		89 / 40		89 / 40		89 / 40	
Кількість суб'єктів	10	30	10	30	10	30	10	30	10	30
Показник ідентифікації	25%	75%	25%	75%	25%	75%	25%	75%	25%	75%

Таблиця Б.10 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних AgeDB, CFP, LFW і Tinyface в умовах неповної видимості рис облич з перетворенням формату

	BMP		PNG		JPG	
	Точність	Помилка	Точність	Помилка	Точність	Помилка
	AgeDB					
Всього зображень / суб'єктів	174 / 40		174 / 40		174 / 40	
Кількість суб'єктів	10	30	10	30	10	30
Показник ідентифікації	25%	75%	25%	75%	25%	75%
	CFP					
Всього зображень / суб'єктів	202 / 40		202 / 40		202 / 40	
Кількість суб'єктів	20	20	20	20	24	16
Показник ідентифікації	50%	50%	50%	50%	60%	40%
	LFW					
Всього зображень / суб'єктів	125 / 40		125 / 40		125 / 40	
Кількість суб'єктів	10	30	10	30	12	28
Показник ідентифікації	25%	75%	25%	75%	30%	70%
	Tinyface					
Всього зображень / суб'єктів	89 / 40		89 / 40		89 / 40	
Кількість суб'єктів	4	36	4	36	4	36
Показник ідентифікації	10%	90%	10%	90%	10%	90%

Таблиця Б.11 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних AgeDB, CFP, LFW і Tinyface в умовах неповної видимості рис облич з перетворенням роздільної здатності

	ширина×91		*ширина*×100		*ширина*×128		*ширина*×144	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	AgeDB							
Всього зображень / суб'єктів	174 / 40		174 / 40		174 / 40		174 / 40	
	BMP, PNG							
Кількість суб'єктів	16	24	12	28	12	28	14	26
Показник ідентифікації	40%	60%	30%	70%	30%	70%	35%	65%
	JPG							
Кількість суб'єктів	18	22	12	28	14	26	14	26
Показник ідентифікації	45%	55%	30%	70%	35%	65%	35%	65%
	CFP							
Всього зображень / суб'єктів	202 / 40		202 / 40		202 / 40		202 / 40	
	BMP, PNG							
Кількість суб'єктів	28	12	28	12	30	10	26	14
Показник ідентифікації	70%	30%	70%	30%	75%	25%	65%	35%
	JPG							
Кількість суб'єктів	26	14	30	10	26	14	28	12
Показник ідентифікації	65%	35%	75%	25%	65%	35%	70%	30%
	LFW							
Всього зображень / суб'єктів	125 / 40		125 / 40		125 / 40		125 / 40	
	BMP, PNG							
Кількість суб'єктів	20	20	14	26	16	24	16	24
Показник ідентифікації	50%	50%	35%	65%	40%	60%	40%	60%
	JPG							
Кількість суб'єктів	18	22	16	24	14	26	18	22
Показник ідентифікації	45%	55%	40%	60%	35%	65%	45%	55%
	Tinyface							
Всього зображень / суб'єктів	160 / 40		160 / 40		160 / 40		160 / 40	
	BMP, PNG							
Кількість суб'єктів	16	24	12	28	14	26	10	30
Показник ідентифікації	40%	60%	30%	70%	35%	65%	25%	75%
	JPG							
Кількість суб'єктів	14	26	14	26	12	28	12	28
Показник ідентифікації	35%	65%	35%	65%	30%	70%	30%	70%

Таблиця Б.12 – Результати експериментів із застосуванням комплексного методу біометричної ідентифікації до зображень з наборів даних AgeDB, CFP, LFW і Tinyface в умовах неповної видимості рис облич з перетворенням області обличчя на зображеннях

	32×32		47×47		64×64		78×78		128×128	
	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка	Точність	Помилка
	AgeDB									
Всього зображень / суб'єктів	174 / 40		174 / 40		174 / 40		174 / 40		174 / 40	
	BMP, PNG									
Кількість суб'єктів	10	30	12	28	18	22	14	26	18	22
Показник ідентифікації	25%	75%	30%	70%	45%	55%	35%	65%	45%	55%
	JPG									
Кількість суб'єктів	6	34	12	28	20	20	10	30	16	24
Показник ідентифікації	15%	85%	30%	70%	50%	50%	25%	75%	40%	60%
	CFP									
Всього зображень / суб'єктів	202 / 40		202 / 40		202 / 40		202 / 40		202 / 40	
	BMP, PNG									
Кількість суб'єктів	6	34	6	34	24	16	22	18	24	16
Показник ідентифікації	15%	85%	15%	85%	60%	40%	55%	45%	60%	40%
	JPG									
Кількість суб'єктів	6	34	8	32	30	10	24	16	24	16
Показник ідентифікації	15%	85%	20%	80%	75%	25%	60%	40%	60%	40%

Продовження Таблиці Б.12

	LFW									
Всього зображень / суб'єктів	125 / 40		125 / 40		125 / 40		125 / 40		125 / 40	
	BMP									
Кількість суб'єктів	2	38	12	28	18	22	20	20	20	20
Показник ідентифікації	5%	95%	30%	70%	45%	55%	50%	50%	50%	50%
	PNG									
Кількість суб'єктів	2	38	12	28	16	24	18	22	18	22
Показник ідентифікації	5%	95%	30%	70%	40%	60%	45%	55%	45%	55%
	JPG									
Кількість суб'єктів	2	38	8	32	18	22	20	20	16	24
Показник ідентифікації	5%	95%	20%	80%	45%	55%	50%	50%	40%	60%
	Tinyface									
Всього зображень / суб'єктів	80 / 40		80 / 40		80 / 40		80 / 40		80 / 40	
	BMP, PNG									
Кількість суб'єктів	2	38	2	38	12	28	14	26	14	26
Показник ідентифікації	5%	95%	5%	95%	30%	70%	35%	65%	35%	65%
	JPG									
Кількість суб'єктів	2	38	2	38	10	30	12	28	12	28
Показник ідентифікації	5%	95%	5%	95%	25%	75%	30%	70%	30%	70%

Таблиця Б.13 – Порівняльна таблиця показників точності ідентифікації локально-текстурних дескрипторів зображень

Дескриптор	Набір даних	Роздільна здатність	Кількість суб'єктів / зображень	Точність
LBP	PUT	128×128	100 / 1000	87.22-98.4%
	ORL	92×112	40 / 400	50.44-83.35%
MBP	PUT	128×128	100 / 1000	78.92-96.6%
	ORL	92×112	40 / 400	48.83-80.85%
MBC	PUT	128×128	100 / 1000	93.44-99.8%
	ORL	92×112	40 / 400	70.53-96.25%
LAP	PUT	128×128	100 / 1000	80.92-97.7%
	ORL	92×112	40 / 400	50.64-84.4%

Продовження Таблиці Б.13

GDP	PUT	128×128	100 / 1000	57.9-78.8%
	ORL	92×112	40 / 400	32.28-52.5%
LDN	PUT	128×128	100 / 1000	81.61-97.1%
	ORL	92×112	40 / 400	48.19-78.8%
LDTP	PUT	128×128	100 / 1000	63.72-87.95%
	ORL	92×112	40 / 400	29.58-52.45%
LPQ	PUT	128×128	100 / 1000	86.75-98.55%
	ORL	92×112	40 / 400	67.72-94.25%
LFD	PUT	128×128	100 / 1000	70.89-91.35%,
	ORL	92×112	40 / 400	42.08-67.1%
LGIP	PUT	128×128	100 / 1000	87.25-98.45%
	ORL	92×112	40 / 400	55.08-88.5%
LGP	PUT	128×128	100 / 1000	64.36-85.9%
	ORL	92×112	40 / 400	37.14-62.4%
LMP	PUT	128×128	100 / 1000	89.78-99.25%
	ORL	92×112	40 / 400	56.67-87.85%
LTP	PUT	128×128	100 / 1000	96.58-99.55%
	ORL	92×112	40 / 400	54.72-88.55%
GLTP	PUT	128×128	100 / 1000	92.92-99.25%
	ORL	92×112	40 / 400	48.92-80.4%
MTP	PUT	128×128	100 / 1000	93.33-99.05%
	ORL	92×112	40 / 400	59.69-92.6%
LTrP	PUT	128×128	100 / 1000	56.89-75.1%
	ORL	92×112	40 / 400	31.5-50.75%
PHOG	PUT	128×128	100 / 1000	86.81-99.15%
	ORL	92×112	40 / 400	70.61-94.9%
WLD	PUT	128×128	100 / 1000	83.44-97.55%
	ORL	92×112	40 / 400	57.14-89.3%
1DLBP + HOG	DoF (ORL)	92×112	40 / 120	72.5%
	FERET	256×384	40 / 99	75%
	SCface	108×144	40 / 160	95%

Таблиця Б.14 – Порівняльна таблиця показників точності ідентифікації нейромережевого та локально-текстурного підходів

Підхід	Метод	Точність ідентифікації
Нейронна мережа	CNN	97,35-99,77%
Нейронна мережа	VGGNet	98,06-99,53%
Нейронна мережа	ResNet	99,12-99,86%
Локально-текстурний	1DLBP + HOG	95%

Таблиця Б.15 – Порівняльна таблиця результатів експериментів із зображеннями обличчя за різних положень голови

Підхід	Метод	Положення голови суб'єкта ідентифікації	Точність ідентифікації
Нейронна мережа	CNN	Пряме	81,25%
Нейронна мережа	CNN	Похиле	75%
Нейронна мережа	CNN	Схилене донизу	43,75%
Локально-текстурний	1DLBP + HOG	Пряме	95%
Локально-текстурний	1DLBP + HOG	Похиле	75%
Локально-текстурний	1DLBP + HOG	Схилене донизу	60%

Таблиця Б.16 – Порівняльна таблиця результатів експериментів із зображеннями з різною видимістю обличчя суб'єкта на зображеннях

Підхід	Метод	Видимість обличчя	Точність ідентифікації
Нейронна мережа	ResNet	Повна	97,5%
		Часткова	55%
Нейронна мережа	FaceNet	Повна	98,75%
		Часткова	72,5%
Локально-текстурний	1DLBP + HOG	Повна	95%
		Часткова	82,5%