

# ДОСЛІДЖЕННЯ МЕТОДІВ РОЗПІЗНАВАННЯ ОБЛИЧ

Ляшенко Г.Є<sup>1</sup>., Даниленко О.І.<sup>2</sup>.

<sup>1</sup>Кафедра інформаційно-мережної інженерії, Харківський національний університет радіоелектроніки, м. Харків, Україна, E-mail: halina.liashenko@nure.ua

<sup>2</sup>Кафедра інфокомунікаційної інженерії, Харківський національний університет радіоелектроніки, м. Харків, Україна, E-mail [oksana.danylenko@nure.ua](mailto:oksana.danylenko@nure.ua)

**Анотація** – В роботі проведено аналіз методів біометричної автентифікації. Досліджена ефективність роботи методів розпізнавання облич за допомогою програми, в якій реалізовані поширені методи біометричної ідентифікації за обличчям. Проведено аналіз методів за швидкістю роботи, якістю розпізнавання при різних впливах на зображення.

**Ключові слова** – біометрична автентифікація, розпізнавання облич.

## I. Вступ

Необхідність забезпечення розмежування доступу до інформації постійно зростає, що робить актуальним питання поліпшення безпеки перевірки автентичності користувача. Причинами несанкціанованого доступу третіх осіб до конфіденційної інформації часто стає робота інсайдерів і хакерів. Тому проблеми ідентифікації та автентифікації особистості мають велике значення.

У багатьох комп'ютерних системах перевірка особи користувача все ще здійснюється за допомогою введення логіна і пароля, але набирають популярності і методи біометричної автентифікації, які, потенційно більш надійні.

Однак необхідно зазначити, що такі технології також вразливі до атак.

У даній роботі проведено аналіз таких методів розпізнавання облич, як EigenFaces, FisherFaces та LBPН. Зроблено оцінку швидкості їх роботи, якості розпізнавання облич.

## II. Огляд методів розпізнавання облич

В якості методів розпізнавання облич було обрано такі методи, як EigenFaces [1], FisherFaces[1], LBPН [2,3].

Метод EigenFaces заснований на методі головних компонент, який застосовується, зазвичай, для представлення зображення обличчя вектором малої розмірності (головних компонент), який потім порівнюється з еталонними векторами, закладеними в базу даних. Отриманий один раз на навчальній вибірці зображень обличчя набір власних векторів використовується для кодування всіх інших зображень осіб, які представляються злагодженою комбінацією таких власних векторів[1].

FisherFaces є покращеною версією алгоритму EigenFace. Відмінність полягає у кластеризації навчальних векторів, для цього проводяться розрахунки внутрішньокласових та міжкласових коваріаційних матриць. На відміну від Eigenface, цей метод стійкий до змін умов освітленості[1].

Ці методи були порівняні при використанні класифікатора Хаара та LBP.

Класифікатор Хаара використовується в методі Віолі-Джонса [4]. LBP представляє кожен піксель зображення у вигляді бінарного числа, яке залежить від інтенсивності сусідніх пікселів зображення. Він також є ефективним в обчислювальному плані, так як працює тільки з цілочисельною арифметикою – це дозволяє досягати високої продуктивності, а також він інваріантний до змін яскравості на зображенні, викликаних зйомкою в різних умовах освітлення [2,3].

## III. Отримані результати

В рамках досліджень було розроблено програму для розпізнавання осіб на зображеннях або у відео-потоці, яка дозволяє приймати рішення, обґрунтовані на порівнянні обличч людей серед масиву фотографій.

Для програмної реалізації системи використовувались наступні засоби: мова програмування Python, PyCharm, OpenCV[5].

На вхід системи розпізнавання обличчя поступає зображення або відеопотік, в якому знаходиться обличчя, потім здійснюється оцінка положення обличчя, виділення особистих ознак обличчя (очі, ніс, ріт та контур обличчя), порівняння цих ознак з шаблонами в базі даних, а на виході системи здійснюється ідентифікація (порівняння отриманого зображення з шаблонами з бази даних).

При тренуванні алгоритмів була підрахована кількість секунд виконання програми. Найкращі показники при тренуванні з будь-яким алгоритмом отримання головних компонентів зображення виявився LBPН.

На рисунках 1, 2 наведено порівняння швидкості виконання програм при детектуванні різної кількості облич. Кращий результат отриманий при тренуванні з використанням алгоритму LBPН.

Також було досліджено якість роботи алгоритмів при зміні характеристик зображення, а саме при дії шуму Гауса, при розмитті Гауса, при затемненні та висвітленні зображення.

Використання класифікатора LBP робить систему більш стійкою до шуму: поріг шуму, при якому система робить вірне розпізнавання обличчя у двічі вищий, ніж при використанні класифікатора Хаара для всіх методів. Метод LBP LBPН має найбільший поріг вірного розпізнавання особи (32-35%).

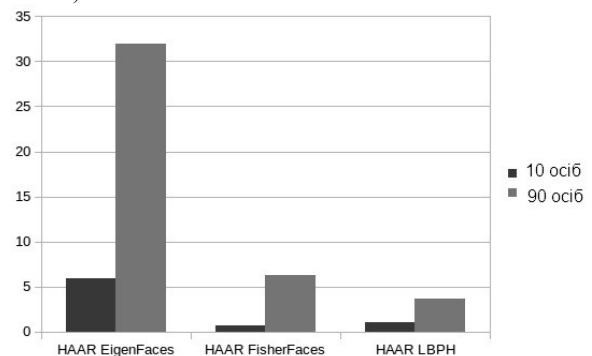


Рис. 1. Порівняння швидкостей при детектуванні за допомогою класифікатора Хаара

Найстійкішим алгоритмом розпізнавання обличчя при розмитті Гауса виявився LBP EigenFace, який дозволяє вірно розпізнати обличчя при рівні розмиття 10 пікселів. Найгірші результати у алгоритмів, які використовують класифікатор Хаара.

До затемнення найбільш стійкий метод LBP LBPН.

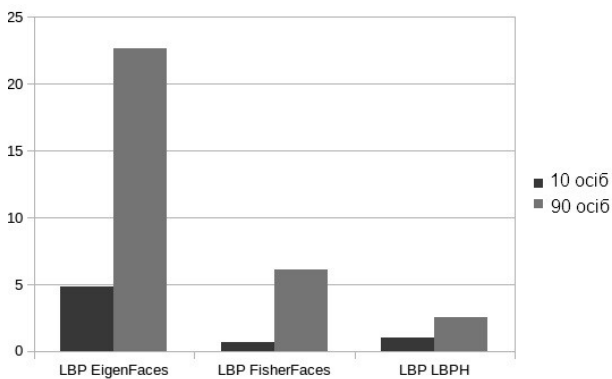


Рисунок 2 – Порівняння швидкостей при детектуванні за допомогою класифікатору LBP

#### IV. Висновки

Під час виконання роботи були проаналізовані біометричні технології розпізнавання обличчя а також досліджена ефективність роботи алгоритмів розпізнавання облич. Дослідження показали, що точність розпізнавання залежить від якості фотографій, кількості персон у вибірці, кількість фотографій на людину (для гарного розпізнавання фотографії повинні бути не однотипні).

Методи FisherFace та LBPН при розпізнаванні облич та є досить швидкими. Зі збільшенням кількість зображень людей збільшується швидкість тренувань алгоритмів та швидкість розпізнавання облич. Точність розпізнавання залежить від кількості персон у вибірці та кількості фотографій на персону; якості фотографій, на які може впливати зовнішні умови, наявність камуфляжу, якість камери.

Тестування алгоритмів розпізнавання облич при різних впливах на зображення показали, що використання класифікатора LBP робить систему більш стійкою до шуму: поріг шуму, при якому система робить вірне розпізнавання обличчя у двічі вищий, ніж при використанні класифікатора Хаара для всіх методів. Метод LBPН з використанням класифікатора LBP має найбільший поріг вірного розпізнавання особи (32-35%). Також, цей метод є найбільш стійким до затемнення. За результатами досліджень зроблені висновки з точки зору надійності, а також виявлені слабкі місця кожного з алгоритмів.

Для підвищення рівня безпеки систем аутентифікації доцільно використовувати мультимодальні біометричні системи, які окрім розпізнавання за обличчям можуть використовувати інші біометричні ознаки (наприклад розпізнавання за райдужною оболонкою ока, відбитком пальця, динамічний підпис) або інші методи аутентифікації (наприклад, смарт-карти, брелоки або слово-пароль, USB-ключі, RFID-карти та інше).

За результатами експериментів був обраний найточніший метод розпізнавання з розглянутих, котрим виявився – LBPН.

Досліджувана система має перспективи для подальшого розвитку, які передбачають реалізації більш ширшого списку алгоритмів та призначеного для користувача інтерфейсу.

#### V. Список літератури

[1] P. Belhumeur, J. Hespanha, D. Kriegman, "Eigenfaces versus Fisherfaces: Recognition Using Class Specific Linear Projection", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 711-720, July 1997.

[2] Ahonen, T., Hadid, A. and Pietikäinen, M., Face Description with Local Binary Patterns: Application to Face Recognition. IEEE Trans. Pattern Analysis and Machine Intelligence 28(12):2037-2041, 2006.

[3] D. Huang, et al., "Local Binary Patterns and its Application to Facial Image Analysis: A Survey," IEEE Trans. Sys-

tems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 41, no. 6, 2011, pp. 1 –17.

[4] Viola, P., Jones, M.: Rapid object detection using a boosted cascade of simple features. In: CVPR, vol. (1), pp. 511–518 (2001)

[5] G. Bradski, A. Kaehler, «Learning OpenCV», O'Reilly Media. – 580 p., 2008.