

Наприклад, для  $K = 3$ ,  $L = 3$ ,  $N = 100 \approx 3 \cdot 10^{253}$  різних ключів. На сьогоднішній день така атака неможлива.

### *Список літератури*

1. *Security evaluation of Tree Parity Re-keying Machine implementations utilizing side-channel emissions* Jonathan Martínez Padilla, Uwe Meyer-Baese and Simon Foo
2. *AES Cryptosystem Development Using Neural Networks* Siddeeq. Y. Ameen and Ali H. Mahdi *International Journal of Computer and Electrical Engineering*, Vol. 3, No. 2, April, 2011 1793-8163
3. *Neural Cryptography Based on Generalized Tree Parity Machine for Real-Life Systems* Sooyong Jeong, Cheolhee Park, Dowon Hong, Changho Seo, and Namsu Jho
4. *Dynamics of neural cryptography* Andreas Ruttor, Wolfgang Kinzel, and Ido Kanter *Phys. Rev. E* 75, 056104 – Published 9 May 2007
5. *A neural cryptography approach for digital image security using Vigenère cipher and tree parity machine* M.A Budiman, Handrizal, William 5<sup>th</sup> International Conference on Computing and Applied Informatics (ICCAI 2020)

**УДК 004.931**

*Гуменний Б.О., здобувач освіти  
Загоруйко Л.В., к.т.н., доцент, доцент  
кафедри інформаційних технологій*

## **АВТОМАТИЧНИЙ ДОДАТОК РОЗПІЗНАВАННЯ І ІДЕНТИФІКАЦІЇ ОСІБ ДЛЯ ІОТ**

*Донецький національний університет імені Василя Стуса, м. Вінниця*

Анотація. Показана можливість використання стандартних скриптів та бібліотек для розроблення автоматичного додатка розпізнавання та ідентифікації осіб для IoT.

Abstract. The possibility is shown, using standard scripts and libraries for development of the automatic application of recognition and identification of persons for IoT.

Розробка і впровадження додатків, таких як розпізнавання обличчя й ідентифікація осіб, нещодавно стала важливою в розумних містах та домах. Як відомо, найбільш використовуваним типом входу для систем безпеки є пароль. Однак завдяки розвитку інформаційних технологій та алгоритмів безпеки багато систем починають використовувати біометричні фактори для завдань розпізнавання й ідентифікації [1,2]. Ці біометричні фактори дозволяють ідентифікувати людей за їх фізіологічними або поведінковими характеристиками. Ці системи мають ряд переваг, наприклад, достатньо присутності людини перед датчиком, і більше не потрібно запам'ятовувати кілька паролів або конфіденційних кодів. У цьому контексті останніми роками було розроблено багато систем розпізнавання на основі різних біометричних факторів, таких як райдужна оболонка ока, відбитки пальців, голос та обличчя.

Системи, які ідентифікують людей за їхніми біологічними характеристиками, дуже привабливі, оскільки вони прості у використанні. Обличчя людини складається з різних структур і характеристик. З цієї причини в останні роки вона стала однією з найбільш широко використовуваних систем біометричної аутентифікації та ідентифікації, враховуючи її потенціал у багатьох додатках і сферах (спостереження, безпека будинку, прикордонний контроль тощо). Система розпізнавання обличчя як ідентифікатор (ідентифікація), вже пропонується споживачам за межами телефонів, у тому числі під час реєстрації в аеропортах, на спортивних стадіонах та на концертах. Крім того, ця система не вимагає втручання людей для роботи, що дає можливість ідентифікувати людей лише за зображеннями, отриманими з камери. Крім того, багато біометричних систем, розроблених з використанням різних типів пошуку, забезпечують високу точність ідентифікації.

Завдяки величезному об'єму даних і швидкому розвитку методів штучного інтелекту традиційні обчислювальні моделі стали неефективними для обробки великої кількості великих масивів інформації даних, особливо для складних додатків, таких як ті, що пов'язані з розпізнаванням і ідентифікацією обличчя. Для ефективного виконання складних обчислювальних завдань необхідні графічні процесори (*GPU*) [2], центральний процесор (*CPU*) і програмовані вентильні матриці (*FPGA*). Графічні процесори мають обчислювальні ядра, які на кілька порядків більше, ніж традиційні ЦП, і дозволяють виконувати паралельні обчислення з більшою потужністю. На відміну від графічних процесорів, *FPGA* мають гнучку апаратну конфігурацію та пропонують кращу продуктивність, ніж графічні процесори, з точки зору енергоефективності. Однак *FPGA* мають серйозний недолік, пов'язаний з часом програмування, який вищий, ніж у *CPU* та *GPU*. Враховуючи наведенні вище недоліки та переваги, в запропонованому додатку використовуються сучасні методи та підходи та апаратне забезпечення до задачі розпізнавання обличчя, а саме:

- *OpenCV* — бібліотека для розпізнавання зображень та машинного навчання з відкритим кодом. До неї входять понад 2500 алгоритмів, у яких є як класичні, і сучасні алгоритми для розпізнавання зображень та машинного навчання. Ця бібліотека має інтерфейси різними мовами, серед яких є *Python*, *Java*, *C++* та ін.

- *Numpy* — розширення мови *Python*, що підтримує обробку великих багатовимірних масивів і матриць, разом з великою бібліотекою високорівневих математичних функцій для операцій з цими масивами.

- *Imutils* — серія зручних функцій для полегшення основних функцій обробки зображень, таких як розпізнавання, поворот, зміна розміру, відображення зображень *Matplotlib*, сортування контурів, виявлення країв і багато іншого з *OpenCV* і *Python 2.7* і *Python 3*.

Існує багато підходів, запропонованих для вирішення завдань виявлення або розпізнавання обличчя з високою надійністю, таких як локальний, цілісний та гібридний підходи [3,4,5]. Однак через різні проблеми, такі як орієнтація голови, умови освітлення та вираз обличчя, потребують подальшого вирішення. Основна проблема полягає в тому, що розпізнавання обличчя вимагає

збільшеного часу обробки та великий обсяг пам'яті. На рис. 1 наведена типова структурна схема системи розпізнавання обличчя, яка складається з чотирьох модулів: виявлення, оцінка положення, виділення ознак та зіставлення — це етапи попередньої обробки, що виконуються безпосередньо перед тим, як проводиться розпізнавання обличчя (виділення ознак обличчя та зіставлення його з шаблонами з бази даних).

В розробленому додатку розпізнавання та ідентифікації осіб застосовується метод заздалегідь навчених каскадів Хаара *OpenCV*.

На рис. 2 наведена структурна схема розробленого автоматичного додатка розпізнавання та ідентифікації осіб для *IoT*, яка використовує зазначені вище технології.

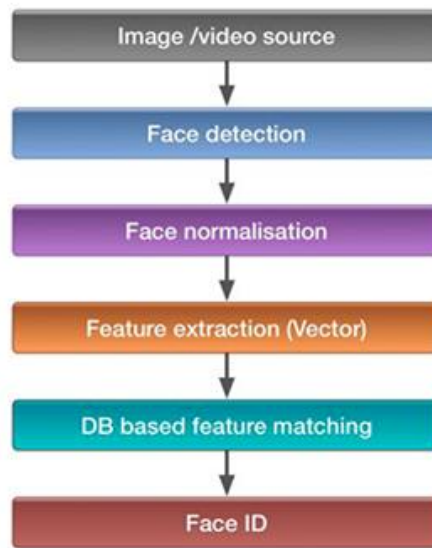


Рисунок 1. Структурна схема типової системи розпізнавання обличчя[6].

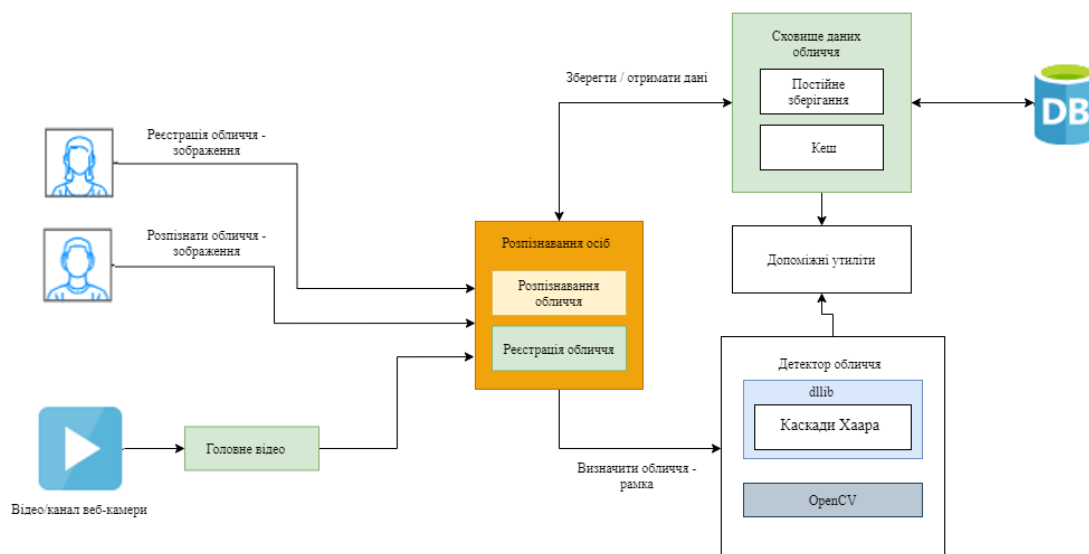


Рисунок 2. Структурна схема розробленого автоматичного додатку розпізнавання і ідентифікації осіб для *IoT*

Результаті тестування роботи розробленого автоматичного додатку розпізнавання і ідентифікації осіб для *IoT* приведенні на рис. 3, 4, 5. В результаті експериментальних досліджень було встановлено, що із вибірки в 50 зображень обличч було виявлено та ідентифіковано 49, тобто, можна стверджувати що точність розпізнавання і ідентифікації розробленим додатком складає 99%.

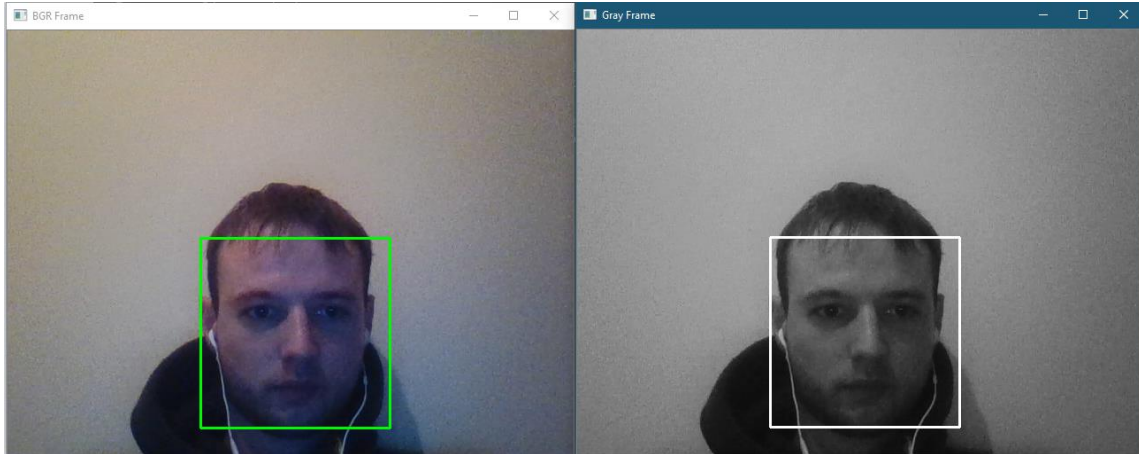


Рисунок 3. Створення каскадного класифікатора Хаара.

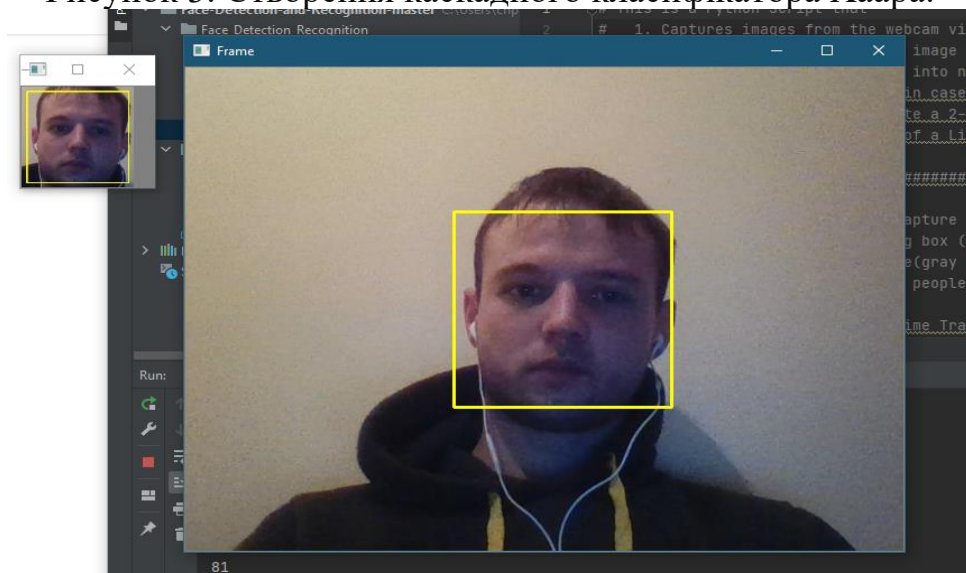


Рисунок 4. Створення цілісних образів.

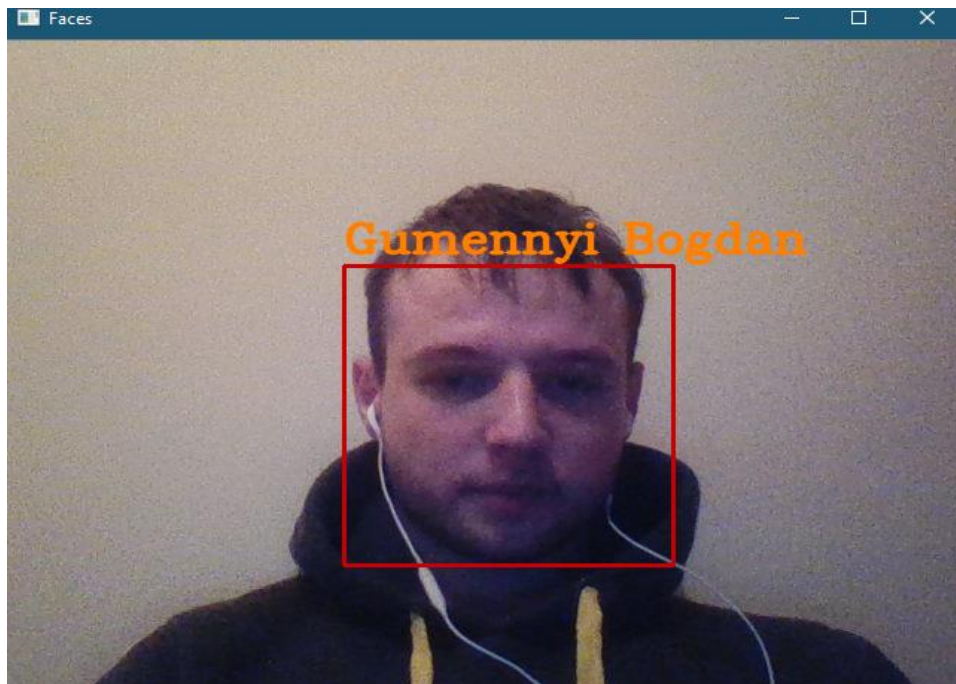


Рисунок 5. Реалізація каскадних класифікаторів.

#### Список літератури

1. Джеріді М., Наполеон Т., Альфалу А. Оптична кореляція однієї лінзи: застосування до розпізнавання обличчя. *Appl. Opt.* 2018;57:2087–2095. DOI: 10.1364/AO.57.002087. [PubMed] [CrossRef] [Google Scholar]
2. Ouerhani Y., Jridi M., Alfalou A. Швидкий підхід до розпізнавання обличчя з використанням графічного процесора «GPU»; Матеріали Міжнародної конференції IEEE 2010 по системах і методах обробки зображень; Салоніки, Греція. 1–2 липня 2010 р.; Піскатавей, Нью-Джерсі, США: IEEE; 2010. С. 80–84. [Google Scholar]
3. Dehai Z., Da D., Jin L., Qing L. 3rd International Conference on Multimedia Technology (ICMT-13) Atlantis Press; Париж, Франція: 2013. Метод розпізнавання обличчя на основі PCA шляхом застосування швидкого перетворення Фур'є під час попередньої обробки. [Google Scholar]
4. Liu W., Wang Z., Liu X., Zeng N., Liu Y., Alsaadi F.E. Огляд глибоких архітектур нейронних мереж та їх застосування. *Нейрокомп'ютерна техніка.* 2017;234:11–26. doi: 10.1016/j.neucom.2016.12.038. [CrossRef] [Google Scholar]
5. Сі М., Чен Л., Полайнар Д., Тонг В. Локальна мережа двійкових шаблонів: підхід глибокого навчання для розпізнавання обличчя; Матеріали Міжнародної конференції IEEE з обробки зображень 2016 року (ICIP); Фенікс, Арізона, США. 25–28 вересня 2016 р.; Піскатавей, Нью-Джерсі, США: IEEE; 2016. С. 3224–3228. [Google Scholar]
6. Waldemar Wójcik. Face Recognition: Issues, Methods and Alternative Applications [Електронний ресурс] / Waldemar Wójcik, Konrad Gromaszek, Muhtar Junisbekov. – 2015. – Режим доступу до ресурсу: <https://www.intechopen.com/chapters/51031>.