УДК 004.93:004.8

В. Ю. Коцюбинський
О. Р. Іщенко

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЛЕГКОВАГОВИХ МОДЕЛЕЙ ГЛИБИННОГО НАВЧАННЯ ДЛЯ АВТОМАТИЧНОЇ АНОНІМІЗАЦІЇ ОБЛИЧ У СЕРВЕРНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У роботі проведено порівняльний аналіз підходів до детекції та анонімізації облич у системах комп'ютерного зору з урахуванням вимог регламенту GDPR. Досліджено класичні алгоритми та сучасні нейромережеві моделі з точки зору точності (mAP), швидкодії (FPS) та ресурсомісткості. Обґрунтовано доцільність використання легковагових моделей (зокрема YuNet) та середовища ONNX Runtime для автоматичної анонімізації облич у високонавантажених серверних системах без використання GPU.

Ключові слова: комп'ютерний зір, детекція облич, анонімізація, GDPR, глибинне навчання, YuNet, ONNX Runtime.

Abstract

The paper presents a comparative analysis of face detection and anonymization approaches in computer vision systems, considering GDPR compliance. Classical algorithms and modern deep learning models are evaluated in terms of accuracy (mAP), performance (FPS), and resource efficiency. The feasibility of using lightweight models (specifically YuNet) and the ONNX Runtime for automatic face anonymization in high-load backend systems without GPU acceleration is justified.

Key words: computer vision, face detection, face anonymization, GDPR, deep learning, YuNet, ONNX Runtime.

Вступ

Стрімкий розвиток цифрових технологій, розгортання інтелектуальних систем відеоспостереження та хмарних сервісів обробки мультимедійних даних призвели до експоненціального зростання обсягів інформації, що містить персональні дані. Зображення обличчя людини є одним із найбільш критичних типів таких даних, оскільки воно виступає унікальним біометричним ідентифікатором, що дозволяє безпосередньо встановити особу [8].

У контексті сучасних правових вимог, зокрема Загального регламенту про захист даних (GDPR) та Закону України «Про захист персональних даних», актуальною задачею комп'ютерного зору є розробка методів автоматичної анонімізації облич [1]. Така технологія є критично необхідною для забезпечення конфіденційності у відкритих веб-сервісах, системах відеоаналітики та мобільних застосунках.

Фундаментальним етапом процесу анонімізації є детекція облич. Ефективність приховування даних критично залежить від точності локалізації: помилки у визначенні координат bounding box можуть призвести або до неповного перекриття рис обличчя (витік персональних даних), або до надмірного спотворення значущих областей зображення [7].

Сучасні підходи до детекції поділяються на класичні алгоритми (наприклад, каскади Хаара) та моделі на основі глибинного навчання (CNN). Якщо класичні методи характеризуються високою швидкістю на малопотужних пристроях, то вони демонструють низьку точність у складних умовах (зміна освітлення, ракурсу чи оклюзія). Нейромережеві моделі забезпечують високу якість детекції, проте їх впровадження у серверні системи часто обмежене значними вимогами до обчислювальних ресурсів, особливо за відсутності виділених графічних прискорювачів (GPU) [3].

У цьому контексті критично важливим є пошук балансу між точністю локалізації, часовою складністю обробки та можливістю кросплатформної інтеграції. Метою даної роботи є порівняльний аналіз сучасних підходів до детекції та анонімізації облич з метою визначення найбільш ефективного

рішення для реалізації масштабованих серверних програмних систем на базі центральних процесорів (CPU).

Результати дослідження

Для розв'язання задачі детекції облич у сучасних системах комп'ютерного зору було проаналізовано три домінантні підходи. Класичні методи, зокрема каскади Хаара (Haar Cascade), базуються на ознаках Хаара та інтегральних зображеннях. Попри високу швидкість обробки, вони демонструють критичне зниження точності (Precision) при зміні кута нахилу обличчя (roll, pitch, yaw) або в умовах недостатньої освітленості [3].

Моделі глибинного навчання на базі згорткових нейронних мереж (CNN), такі як архітектура ResNet-10 (SSD), забезпечують високу стійкість до варіацій вхідних даних. Однак їх застосування у серверних рішеннях без виділених GPU-ресурсів обмежене через високу часову складність інференсу [2].

Окрему групу становлять легковагові моделі, орієнтовані на продуктивність у реальному часі. До них належить архітектура YuNet, яка використовує оптимізовані згортки для швидкої локалізації обличчя та п'яти ключових точок (facial landmarks)[4][5]. Впровадження YuNet через середовище ONNX Runtime[6] дозволяє уникнути залежності від важких Python-фреймворків та забезпечує кросплатформність у середовищах C# чи C++.

У ході дослідження проведено порівняльне тестування обраних методів на базі центрального процесора (CPU) з використанням набору даних WIDER FACE. Результати наведено в Таблиці 1.

Таблиця 1 – Технічні показники порівняння методів детекції облич (CPU-інференс)

Метод детекції	Точність (mAP)	Швидкість (FPS)	Об'єм моделі	Стійкість до оклюзій
Haar Cascade	0.45	150+	930 KB	Низька
CNN (ResNet-10)	0.88	12	80.4 MB	Висока
YuNet (ONNX)	0.84	70+	0.2 MB	Висока

Результати підтверджують, що YuNet забезпечує оптимальний баланс: при швидкодії понад 70 кадрів за секунду (FPS) вона зберігає точність, наближену до важких CNN-моделей.Після детекції виконується автоматична анонімізація знайдених областей. Основними методами є пікселізація, накладання маски та розмиття за Гаусом (Gaussian Blur). Останній є найбільш доцільним для збереження контексту зображення при повному приховуванні ідентичності. Для забезпечення стабільної анонімізації незалежно від відстані об'єкта до камери, радіус розмиття σ розраховується адаптивно за формулою:

$$\sigma = \frac{W + H}{2k}$$

Де W, H – розміри області детекції, k ≈ 20

У сучасних інформаційних системах анонімізація реалізується у вигляді серверного конвеєра (pipeline), що включає наступні етапи:

1. Ingress: отримання зображення від клієнта через REST Web API.
2. Preprocessing: нормалізація розмірів та перетворення колірного простору.
3. Inference: детекція облич за допомогою YuNet у середовищі ONNX Runtime.
4. Anonymization: застосування адаптивного фільтра Гауса до витягнутих координат (Bounding Boxes).
5. Egress: повернення анонімізованого зображення або метаданих клієнту.

Такий підхід дозволяє централізувати обробку даних, забезпечити горизонтальну масштабованість системи та гарантувати високу швидкість відгуку навіть на серверному обладнанні загального призначення.

Висновки

У роботі проведено комплексне порівняння сучасних підходів до детекції та анонімізації облич у системах комп'ютерного зору. На основі проведених досліджень можна сформулювати наступні висновки:

1. Неефективність класичних підходів: Встановлено, що класичні алгоритми (зокрема каскади Хаара) не забезпечують необхідного рівня точності (mAP < 0.5) для надійного захисту персональних даних у складних умовах зйомки, що створює ризики порушення вимог конфіденційності.
2. Переваги легковагових моделей: Доведено, що для серверних систем, які працюють на базі CPU, найбільш доцільним є використання легковагової моделі YuNet. Завдяки оптимізації через середовище ONNX Runtime, вона демонструє швидкодію понад 70 FPS, що у 5-6 разів перевищує показники стандартних CNN-архітектур при збереженні високої точності локалізації.
3. Адаптивна анонімізація: Обґрунтовано використання методу адаптивного розмиття за Гаусом, параметри якого динамічно змінюються залежно від розміру знайденої області. Це дозволяє автоматизувати процес анонімізації для зображень різної роздільної здатності, забезпечуючи стабільне приховування біометричних ознак.
4. Практична цінність: Запропонований конвеєр обробки даних (pipeline) дозволяє створювати масштабовані веб-сервіси та корпоративні системи, що відповідають вимогам GDPR та забезпечують захист приватности користувачів у реальному часі без залучення високовартісного графічного обладнання.

Перспективами подальших досліджень є розробка алгоритмів стабілізації детекції у відеопотоках для уникнення мерехтіння (flickering) анонімізованих областей, а також дослідження методів диференційованої анонімізації, які б дозволяли приховувати ідентичність особи, зберігаючи при цьому можливість аналізу її емоційного стану для потреб маркетингової аналітики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union. 2016. Vol. L119. P. 1–88.
2. Padilla R., Netto S. L., da Silva E. A. A Survey on Performance Metrics for Object Detection Algorithms. 2020 International Conference on Systems, Signals and Image Processing (IWSSIP). Niteroi, Brazil, 2020. P. 155–160. DOI: 10.1109/IWSSIP48289.2020.9145130.
3. Viola P., Jones M. Rapid Object Detection using a Boosted Cascade of Simple Features. Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR). Kauai, HI, USA, 2001. Vol. 1. P. I-511–I-518.
4. OpenCV Zoo: YuNet Face Detection Model. GitHub Repository. 2023. [Електронний ресурс]. URL: https://github.com/opencv/opencv_zoo
5. Yu S., et al. YuNet: A Fast and Accurate Face Detection Model for Edge Devices. OpenCV Documentation. [Електронний ресурс]. URL: https://docs.opencv.org/4.x/d0/dd4/tutorial_dnn_face.html
6. ONNX Runtime: High-performance inference engine. Microsoft Open Source. [Електронний ресурс]. URL: https://onnxruntime.ai/docs/
7. Hukkelhoven S., et al. Deep Privacy: A Generative Adversarial Network for Face Anonymization. International Semantic Web Conference. 2019. [Електронний ресурс]. URL: https://arxiv.org/abs/1909.04538 (дослідження впливу анонімізації на якість детекції).
8. OpenCV: Open Source Computer Vision Library. Official Site. [Електронний ресурс]. URL: https://opencv.org/

Іщенко Олексій Русланович – студент групи 1ІСТ-22Б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: oleksiy26032005@gmail.com

Науковий керівник: **Володимир Юрійович Коцюбинський** — к.т.н., доцент кафедри АІІТ, Вінницький національний технічний університет, м. Вінниця.

Ishchenko O. R. – student of group 1IST-22B, Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksiy26032005@gmail.com

Supervisor: **Kotsiubynskyi Volodymyr Y.** — PhD, Associate Professor of the AIIT Department, Vinnytsia National Technical University, Vinnytsia.