УДК 004.056.53

ОГЛЯД СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА ГЕОМЕТРІЄЮ ОБЛИЧЧЯ

І. В. Струнін[1], А. І. Кісіоглова[1], Д. О. Прогонов[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Забезпеченню надійної автентифікації користувачів сьогодні приділяється особлива увага при розробці, впровадженні та супроводі комплексних систем захисту інформації. До систем автентифікації висуваються вимоги щодо низько рівня помилок та стійкості до змін зовнішніх умов, зокрема, зміни освітлення, ракурсу з'йомки. В роботі проведено огляд сучасних комерційних рішень та методів автентифікації користувачів за геометрією обличчя. За результатами аналізу встановлено, що комплексне застосування декількох методів обробки забезпечує високу точність автентифікації користувачів в умовах значної варіативності зовнішніх умов.

Ключові слова: автентифікація, обличчя, нейронні мережі, ідентифікація, захист інформації

Вступ

В державних установах та приватних організаціях особлива увага приділяється захисту конфіденційних даних (КД). Одним із елементів захисту є управління доступом до КД (авторизація користувачів), зокрема, з використанням систем контролю та управління доступом (СКУД). Впровадження таких систем потребує значних капіталовкладень, зокрема, на придбання ліцензійного програмного забезпечення, встановлення технічних засобів (відеокамери, модулі зчитування відбитків пальців користувачів тощо).

До сучасних СКУД висуваються високі вимоги щодо рівня помилок першого (хибне надання доступу, англ. False Acceptance Rate, FAR) та другого (хибна відмова в доступі, англ. False Rejection Rate, FRR) роду. Забезпечення низького рівня даних помилок (FAR $\sim 10^{-5}$, FRR $\sim 10^{-2}$) вимагає комплексного використання декількох ознак (факторів автентифікації), що призводить до зростання часу автентифікації користувачів та, відповідно, ускладнює застосування даних систем на великих підприємствах. Тому актуальною задачею є розробка СКУД, які дозволяють швидко проводити автентифікацію користувачів при забезпеченні низького рівня помилок FAR/FRR.

Вирішення поставленої задачі потребує проведення огляду існуючих рішень, зокрема, в галузі біометричних систем автентифікації. Дані системи дозволяють суттєво скоротити тривалість автентифікації (не потребують додаткових дій від користувачів) при збереженні відносно низького рівня помилок. Особливий інтерес становлять системи біометричної автентифікації за геометрією обличчя, що можуть використовуватися як в складі систем периметрального відеонагляду організацій, так і на мобільних пристроях користувачів.

Дана робота присвячена огляду сучасних систем автентифікації за геометрією обличчя та аналізу принципів їх роботи.

1. Комерційні рішення в області біометричної автентифікації за геометрією обличчя

В системах відеонагляду зазвичай застосовують одночасно декілька камер, розташованих під різним ракурсом. Це дозволяє забезпечити як огляд обличчя користувачів незалежно від кута нахилу камери та орієнтації користувача відносно камери, так і побудувати тривимірне зображення обличчя користувача. Отримане зображення використовується для визначення та локалізації контрольних точок та подальшого порівняння отриманого шаблону з базою шаблонів користувачів.

Сучасні системи відеонагляду є чутливими до незначних змін зовнішності користувача (кольору волосся, наявності окулярів), зовнішніх умов освітлення та положення обличчя користувача відносно камери.

Компанія Identix в 2019 році розробила технологію, що заснована на використанні хмарного сервісу для розпізнавання облич в реальному часі. Особливість даної технології полягає у використанні великого пакету тестових зображень різної якості та защумленості, отриманих з використанням декількох типів камер. Це дозволило суттєво зменшити рівень помилок (FAR=$3 \cdot 10^{-7}$) у порівнянні з існуючими системами розпізнавання користувачів. Запропонована технологія [1] є адаптованою до використання лише на IP та Web-камерах, що ускладнює її застосування в системах периметрального відеонагляду.

Компанія Cortica у 2019 році створила систему Corsight [2], що дозволяє підвищити якість роботи

СКУД в умовах слабкого освітлення. Corsight дозволяє використовувати камери зовнішнього відеоспостереження для роботи в умовах слабкого освітлення, та наявності оклюзій. Дана технологія базується на створенні шаблону біометричних даних користувача та методу їх швикого оновлення при зміні зовнішіх умов.

Компанія NtechLab розробила схожу систему розпізнавання обличчя FindFace, що базується на шаблонах. [3]. Дана технологія відрізняється тим, що використовує надвеликі бази користувачів (від 250 млн. до 1 млрд. зображень) та полягає в проведенні аналізу кожного кадру відеоряду.

2. Автентифікація користувача методом гнучкого порівняння на графах

Одним з поширених методів автентифікації користувачів за геометрією обличчя є метод гнучкого порівняння на графах (elastic graph matching algorithm) [4]. В якості ознак користувача використовуються коефіцієнти вейвлет-перетворення зображення та положення вузлів графу, побудованого з використанням характерних точок обличчя (англ. Point of Interests, PoI).

Обробка зображення згідно даного методу проводиться в декілька етапів. На першому етапі проводиться вейвлет-перетворення заданого зображення з використанянм вейвлету Габора.

$$\Psi_j\left(\overrightarrow{x}\right) = \frac{k_j^2}{\sigma^2}\exp\left(-\frac{k_j^2 \times x^2}{2\sigma^2}\right) \times \\ \times\left(\exp\left(\overrightarrow{ik_j}\overrightarrow{x}\right) - \exp\left(-\frac{\sigma^2}{2}\right)\right) \quad (1)$$

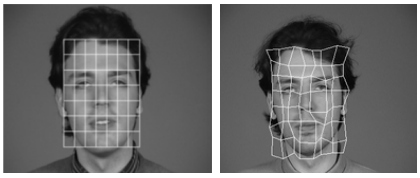
де $\overrightarrow{k_i} = k_v\left[\cos\left(\varphi_\mu\right) + i\sin\left(\varphi_\mu\right)\right]$, $\left(\overrightarrow{x}\right) = (x, y)$ – вектор координат пікселів зображення, $\overrightarrow{k_j}$ – хвильовий вектор плоских хвиль, що обмежений гаусіаном. v – індекс частоти (в методі гнучкого порівняння на графах [4]] $v \in [0..3]$), μ – індекс напрямку в площині зображення, $\mu \in [0..7]$.

На другому етапі на задане зображення накладається прямокутна регулярна решітка (Рис. 1). Елементами даної решітки є PoI, попередньо визначені з використанням сторонніх методів.

Автентифікація користувачів з використанням методу гнучкого порівняння на графах проходить в два етапи. На першому етапі проводиться обробка бази даних зображень користувачів, зроблених в контрольованих умовах (отримані в анфас та з рівномірно освітленими обличчями) [4].

При автентифікації користувача проводиться обчислення характеристик для отриманої фотографії користувача (коефіцієнтів двовимірного дискретного вейвлет перетворення та положення вузлів графа). Отримані характеристики порівнюються з шаблонами користувачів з бази даних для оцінки відмінностей Δ між ними. Якщо для i-того шаллону отримано, що відмінності є меншими за заданий поріг ε, то досліджуване фото відноситься до i-того користувача. В протилежному випадку відбуваться деформація графу для заданого фото (зміни положення вузлів графу) та повторне порівняння з шаблонами з бази даних корисувачів. Дана процедура ітеративно повторюється до виконання умови $\Delta < \varepsilon$, а індекс користувача u_{curr} визначається наступим чином $u_{curr} = argmin\left(\Delta\right)_i$.

Приклади застосування даного методу для обробки фотографій користувачів наведені на Рис. 1



а) б)

Рис. 1. Приклад застосування методу гнучкого порівняння для розпізнаваня обличчя: а) оригінал зображення користувача та регулярна решітка; б) зображення із деформованим графом

Метод гнучкого порівняння на графах забезпечує високу точність розпізнавання користувачів, навіть в умовах афінних поворотів обличчя користувача навколо вертикальної осі – в межах $89 - 96\%$ при ручному розташуванні антропометричних точок та $67 - 72\%$ за автоматичного розташування [4]. Обмеженням даного методу є велика ресурсоємність внаслідок обчислення значних об'ємів данних при виконанні деформації графа по всіх можливих напрямках.

3. Метод головних компонент

Метод головних компонент (МГК, англ. Principal Component Analysis, PCA)[5] є одним із класичних методів машинного навчання. Суть даного методу полягає в розкладі досліджуваного зображення на ортогональні компоненти. Даний метод потребує попередньої обробки зображень – масштабування до однакового розміру та видалення фону навколо обличчя користувача.

Обчислення компонент розкладу заданих зображень згідно з МГК проводиться в делька етапів. На першому етапі отримані напівтонові зображення $I_1, ..., I_k$ розміром $h \times w$ перетворюються на векторирядки. Дані рядки об'єднуються в матрицю плану – кожен рядок даної матриці відповідає окремому зображенню, а стовпчик відповідає окремим пікселям зображенння. Також проводиться нормалізація даної матриці: $\mathbf{\Phi} = \boldsymbol{A} - E[A]$, де $E[\cdot]$ – оператор обчислення середнього значення.

На наступному етапі проводиться обчислення матриці коваріації $\mathbf{C}$ нормалізованої матриці плану $\mathbf{\Phi}$: $\mathbf{C} = \frac{1}{M}\sum_{i=1}^{M}\Phi_i\Phi_i^T = BB^T$, де $B = \{\Phi_1, \Phi_2, ..., \Phi_M\}$.

На останньому етапі проводиться обчислення власних чисел та власних векторів матриці коваріації $\mathbf{C}$. Окремі компоненти розкладу вихідних зображень $I_1, ..., I_k$ відповідають добуткам відповідних

власних чисел $\Lambda = diag\{\lambda_1, \ldots, \lambda_r\}$ та власних векторів $V = \{v_1, \ldots, v_r\}$.

Компоненти розкладу сортуються за значеннями відповідним їхнім власним числам. При цьому перші компоненти, що відповідають найбільшим сингулярним числам, визначають великі деталі на зображенні (контури обличчя, очей, носа тощо), а інші – дрібним деталям зображення (текстура шкіри).

4. Автентифікація обличчя за допомогою згорткових нейронних мереж

Згорткові нейронні мережі (ЗНМ) широко використовуються [6] в задачах автентифікації користувачів, оскільки є стійкими до зміни масштабу, зміщення, поворотів та змін ракурсу зображення. Дані властивості мають широке застосування в мобільних пристроях, наприклад Face ID [7], DeepFace [8].

Загальна структура згорткових нейронних мереж зображена на Рис. 2

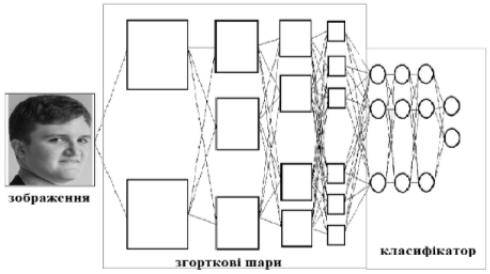


Рис. 2. Загальна структура згорткової нейронної мережі

Характерні ознаки обличчя користувача отримуються з вихідних шарів ЗНМ. Налаштуваня ЗНМ (ваг між нейронами всередині та між шарами нейронів) ітеративно визначається з використанням методу градієнтного спуску.

Процес роботи системи автентифікації на базі ЗНМ містить в собі два етапи. На першому етапі здійснюється виявлення обличчя та локалізація його положення на зображенні (кадрування). Для підвищення точності роботи системи може проводитись нормалізація[9]. На другому етапі підготовлене зображення подається на вхід нейронної мережі. Масив ознак, отриманих на виході ЗНМ, використовуються класифікатором для автентифікації.

5. Оцінка точності сучасних методів автентифікації обличчя з використанням машинного навчання

В роботі досліджено точність автентифікації користувачів за геометрією обличчя при застосуванні розглянутих методів обробки. Результати порівняльного аналізу точності розпізнавання облич на базі даних LFW при використанні сучасних згорткових нейронних мереж [9] наведені в Табл. 1.

Застосування мережі DeepID-2,3 дозволило отримати найбільшу точність розпізнавання користувачів (99.47%, Табл. 1.). Варто зазначити, що розглянуті

Табл. 1. Точність розпізнавання із використанням згорткових нейронних мереж

Назва нейронної мережі	Точність розпізнавання, %
Fisher Vector Faces	93,10
DeepFace	97,35
DeepID-2,3	99,47
Fusion	98,37
FaceNet	98,87

мережі є стійкими до змін зображення з такими особливостями обличчя, як борода, вуса, різні зачіски, окуляри (в тому числі сонячні).

6. Висновки

В роботі проведено аналіз сучасних підходів до автентифікації обличчя. Метод гнучкого порівняння на графах є стійким до афінних поворотів обличчя по вертикальній осі, проте є чутливим до ступеня освітленості обличчя, а також такі особливості обличчя, як, наприклад, борода, окуляри, вуса. Також даний метод є ресурсоємним, що обмежує його застосування в реальних системах автентифікації.

Забезпечення високої точності автентифікації користувачів в умовах значної варіативності зовнішніх умов (зміни освітлення та ракурсу зйомки) потребує комплексного застосування декількох методів обробки.

Перелік використаних джерел

1. Identix. Knowledge base. — Access mode: `https://kb.identix.one/` (online; accessed: 24.04.2020).
2. Corsight. Knowledge base. — Access mode: `https://corsight.ai/technology` (online; accessed: 25.04.2020).
3. FindFace. Knowledge base. — Access mode: `https://findface.pro/en/technology/` (online; accessed: 26.04.2020).
4. Face recognition by elastic bunch graph matching / L. Wiskott, J.-M. Fellous, N. Krüger, C. von der Malsburg. — 1999. — 01. — Vol. 19. — P. 355–396. — ISBN: 0-8493-2055-0.
5. Belhumeur P., Hespanha J., Kriegman D. Eigenfaces vs. Fisherfaces // IEEE Trans. Pattern Anal. Mach. Intell.
6. Duffner S. Face image analysis with convolutional neural networks. — 2007. — 01.
7. Hall Zac. Apple explains how iPhone X facial recognition with Face ID works (and fails) in security paper. — Access mode: `https://9to5mac.com/2017/09/27/face-id-iphone-x-white-paper/` (online; accessed: 23.04.2020).
8. Constine J. FB can unlock your acount with facial recognition. — Access mode: `https://techcrunch.com/2017/09/29/facebook-face-id/` (online; accessed: 19.04.2020).
9. Fisher Vector Faces in the Wild / K. Simonyan, O. Parkhi, A. Vedaldi, A. Zisserman. — 2013. — 01. — P. 8.1–8.11.