

УДК 004.93

DOI: 10.31474/2415-7902-2019-1(2)-2(3)-12-20

Н.О. Маслова, Д.О. Полуніна

МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ПРИ ІДЕНТИФІКАЦІЇ ОСОБИ

Галузь безпеки висуває підвищені вимоги до методів і алгоритмів, які застосовуються в процесі ідентифікації особи. В статті наведено результати досліджень методів біометричної автентифікації, що застосовуються в системах контролю доступу за показниками достовірності, точності та часу навчання. Розглянуто доцільність застосування згорткових нейронних мереж, методів опорних векторів, k-найближчих сусідів, норма Фробеніуса. Отримано порівняльні характеристики, наведено результати тестування обраних методів.

Ключові слова: ідентифікація, біометричні системи, автентифікація, метод опорних векторів, K-найближчих сусідів, норма Фробеніуса, системи захисту, класифікація зображень.

Вступ. Методи біометричної автентифікації – одна з сучасних технологій ідентифікації особи. Термін «біометрія» пов'язаний з використанням унікальних фізіологічних даних індивіда, застосовує біологічні характеристики або поведінкові особливості для розпізнавання людини. Системи біометричних даних аналізують відбитки пальців, геометрію обличчя, розпізнавання голосу, контуру тіла й так далі [1]. Застосування біометричної автентифікації в системах безпеки замість текстових або графічних паролів є актуальним та сучасним напрямком, розвиток якого пов'язаний з застосуванням мобільних пристроїв та повсюдним застосуванням комп'ютерно-інформаційних технологій.

Метою дослідження є огляд та аналіз сучасних технологій біометричної автентифікації при ідентифікації особи за рисами обличчя, аналіз існуючих засобів програмної реалізації та вибір методів та алгоритмів, найбільш ефективних за характеристиками достовірності, точності та швидкодії.

Класична процедура ідентифікації та автентифікації складається з суб'єкту, який проходить процедуру, його унікальних особливостей, обраної системи сертифікації та принципу її роботи (біометрична автентифікація), механізму контролю доступу при наданні конкретних прав доступу суб'єктам [2].

Біометрична автентифікація є процесом підтвердження достовірності даних, шляхом представлення користувачем його біометричного зображення, а також процесу перетворення цього зображення відповідно до заздалегідь визначеного протоколу автентифікації [3].

В процесі біометричної автентифікації еталонний зразок і зразок, який подає користувач порівнюються з деякими попередньо встановленими допусками.

Існують два основні недоліки, які заслуговують особливої уваги при застосуванні біометричної автентифікації: підроблена атака на інтерфейс користувача та витік з бази даних шаблонів.

Підроблена атака на інтерфейс користувача полягає у заміні реального відбитку пальця чи обличчя підробленим біометричним зображенням. Підроблені атаки порушують основний принцип роботи систем розпізнавання, безпека системи серйозно порушується.

Витік з бази даних шаблонів виникає, коли інформація про законний шаблон користувача стає доступна зловмиснику. У цьому випадку зловмиснику набагато простіше відновити біометричний малюнок шляхом зворотної інженерії шаблону, що збільшує ризик підробки. Але порушник не має можливості замінити реальний шаблон на підроблений, як у випадку з паролем й це є перевагою біометричних методів.

1. Методи біометричної автентифікації.

Загалом методи біометричної ідентифікації підрозділяють на два основних типи: статичні та динамічні.

Статичні методи біометричної автентифікації засновані на фізіологічних (статичних) властивостях людини, тобто на унікальних властивостях, які надані особі від народження і невіддільні від нього. Такими властивостями є відбитки пальців людини, мережа кровоносних судин під шкірою, рисунок райдужної оболонки ока, контури обличчя, й тому подібне [4].

Динамічні методи ґрунтуються на аналізі поведінкових особливостей, які підсвідомо застосовуються людиною в процесі відтворення певної нормальної поведінки (класичний почерк, особливості руху, послідовність виконання стандартних дій). З точки зору мережевих технологій особливо важливі методи автентифікації на основі підписів і рукописного вводу клавіатури. Приклади динамічних методів наведено в [5].

На глобальному ринку найбільше розповсюдження отримали статичні системи біометричного захисту. Система розпізнавання обличчя – це технологія, здатна ідентифікувати або перевірити особу з цифрового зображення або відеокадру з відео. Відноситься до статичних методів. Існує кілька систем, в яких закладено системи розпізнавання осіб, але в цілому вони працюють, порівнюючи вибрані риси обличчя з даним зображенням особи в базі даних. Метод також описується як біометричний додаток на основі штучного інтелекту, який може однозначно ідентифікувати людину шляхом аналізу моделей на основі текстур обличчя та форми голови людини.

Задачі біометричної автентифікації можна віднести до розділу задач класифікації зображень. Основним підходом до рішення задачі розпізнавання та класифікації зображень вважаються нейронні мережі [6]. Серед основних підходів до побудови нейронних мереж слід виділити так звану згорткову або глибоку нейронну мережу (ConvNets або CNNs). Глибокі нейронні мережі і глибоке навчання застосовуються в сучасності в системах комп'ютерного зору, розпізнавання мови, класифікації зображень. Нейронна мережа зазвичай включає велику кількість нейронів, що працюють паралельно і розташовані в окремих шарах, тому очікуваним результатом є досить висока швидкість роботи методів цього класу. Нейронні мережі цього виду адаптивні, модифікують себе, добре навчаються навіть без початкової підготовки.

Другим методом, що застосовується для розв'язання задачі класифікації є метод опорних векторів (Support Vector Machines, SVM).

Метод опорних векторів (Support Vector Machines, SVM) відноситься до низки лінійних класифікаторів. У цьому сімействі рішення про належність об'єкта x до класу $\hat{t}$ приймається за законом лінійного вирішального правила:

$$f(x) = \sum_{j=1}^d w_j x(j) + b = w^T x + b, \hat{t}(x) = \begin{cases} +1, & \text{якщо } f(x) \geq 0, \\ -1, & \text{якщо } f(x) < 0. \end{cases}$$

де $b \in R$ - параметр зсуву, $w_j \in R$ - деякі ваги.

Метод опорних векторів базується на побудові оптимальної роздільної гіперплощини. Навчання в самому методі зводиться до вирішення задачі квадратичного програмування, яке має єдине рішення. Розв'язок має різні властивості, зокрема – розрідженості: положення гіперплощини залежить від малої долі навчальних об'єктів. Саме ці об'єкти являються опорними векторами, завдяки яким метод отримав свою назву [7].

Третім методом, який було включено в дослідження, є метод K -найближчих сусідів. Це також метод проведення класифікації осіб на основі їх зображень [8].

При використанні k -NN класифікатора важливо, щоб серед k найближчих сусідів була відносна або абсолютна більшість образів свого класу серед інших образів. Розглянемо більш простий випадок, який передбачає відносну більшість. Успішна

робота k-NN класифікатора полягає в тому, що для k найближчих сусідів виконується умова:

$$|U_i \tilde{l}_i| > |U_i \tilde{m}_i|, i = 1, 2, 3 \dots,$$

де $\tilde{l}_i, \tilde{m}_i$ – групи, які утворюються після зниження інформаційного покриття класів. Під групою розуміється однорідна послідовність елементів. Схема обчислювального процесу у разі застосування методу k-найближчих сусідів наведена на рисунку 1.

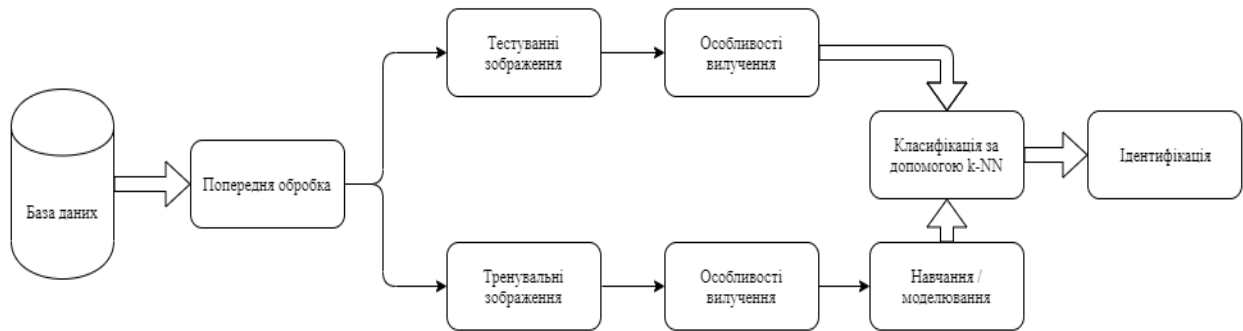


Рисунок 1 – Схема реалізації методу k-найближчих сусідів

Ще одним поширеним способом розв’язання задачі класифікації є застосування норми Фробеніуса. Неформально норма Фробеніуса вимірює дисперсію або мінливість (яка може бути інтерпретована за розміром) матриці [8]. У нашому випадку будемо використовувати її для апроксимації та розраховувати за формулою:

$$\|A\|_F = \sqrt{\sum_{j=1}^n \sum_{i=1}^m A_{ij}^2} = \sqrt{\text{Tr}(A^T A)}$$

де $\text{Tr}(A^T A)$ означає трасу матриці (траса квадратної матриці визначається як сума елементів головної діагоналі).

Проведення ідентифікації особи потребує, щоб методи, застосовані в процесі розпізнавання та класифікації, вдовольняли ряду вимог, а саме: швидкість та висока точність, отримувана на малих даних [9].

Перша вимога системи розпізнавання осіб (швидкість) полягає в тому, що вона має надавати результат за найкоротший час. Наприклад, при розпізнаванні осіб з застосуванням смартфона, зазвичай потрібно використовувати фронтальну камеру в телефоні, щоб сканувати обличчя під різними кутами для навчання, й наступні розпізнавання повинні відбуватися за лічені секунди.

Слід зауважити, що виявилось, що згорткові нейронні мережі (ConvNets або CNNs), не можуть надати оптимальне рішення для розпізнавання осіб в подібних системах.

Друга вимога - висока точність на малих даних, а саме - система повинна бути достатньо точною (отже, безпечною) при роботі з невеликою кількістю навчальних даних. Виявилось, що CNN досить точна в завданнях класифікації зображень, тільки за рахунок необхідності величезного тренувального набору. Тому й за цим параметром метод не задовольняє вимогам й, як висновок, не може бути застосований в системах ідентифікації осіб за методом біометричної автентифікації за рисами обличчя.

Крім того, біометричні методи можуть бути класифіковані та порівняні за кількома факторами та показниками, які описано в [10].

FAR (False Acceptance Rate, частота помилкового прийняття) – показує, як часто система визнає особу, що не має дозволу, як уповноважена, вимірюється у відсотках.

FRR (False Rejection Rate, частота помилкового відхилення) – показує, як часто система буде неправильно обробляти довірену особу як несанкціоновану та відхиляти доступ, вимірюється у відсотках.

GFRR (узагальнений FRR) – показує з допомогою та розширеннями, що надаються дослідженням СБА – FRR пристрою в реальних обставинах, включаючи помилки користувача, вимірюється у відсотках.

FTE (не вдається зареєструватися) – показує кількість людей, які не можуть бути зареєстровані в системі, і тому не можуть використовувати її, вимірюється у відсотках.

Ризик помилки – він показує, як легко можна обійти систему за допомогою певного методу (наприклад, замість фактичного відбитка пальця, показуючи лише його фото оптичного сканера відбитків пальців).

Виявлення живого зразка – показує, чи може система відрізнати живого користувача від спроби підмін.

В таблиці 1 наведено теоретичні узагальнені рівні значень параметрів у випадку розпізнавання за рисами обличчя.

Таблиця 1 – Рівні значень параметрів методів автентифікації

Метод автентифікації	FAR	FRR	GFRR	FTE	Ризик помилки	Виявлення живого зразка
Розпізнавання обличчя	10^{-2}	10^{-2}	1-5	1	Низький-середній	Немає

Пояснимо обрані фактори оцінювання. Коефіцієнт помилкового відхилення (FRR) або коефіцієнт помилкової невідповідності (GFRR) – ймовірність що система неправильно визначає збіг між вхідним шаблоном і відповідним шаблоном в базі даних. Він вимірюється у відсотках відхилення допустимих вхідних даних.

Це співвідношення числа помилкових визнань, розділених на кількість спроб ідентифікації. Для цілей цього дослідження було зареєстровано і підтверджено сімсот п'ятдесят зображень осіб, в яких було прийнято одне з незареєстрованих зображень. Отже коефіцієнт помилкового відхилення розраховується за наступною формулою:

$$FRR = \frac{\text{Number of false rejected image}}{\text{Number of registered image}} * 100$$

Частота помилкового прийняття (FAR) – ймовірність того, що система неправильно визначає успішний збіг між вхідним шаблоном і невідповідним шаблоном в базі даних. Цей показник вимірює відсоток недійсних збігів. Ці параметри мають вирішальне значення, так як вони зазвичай використовуються для заборони певних дій забороненими людьми.

Точність розпізнавання системи – це загальний відсоток правильних розпізнавань системи. Точність розпізнавання визначається наступним чином:

$$RA = (100 - (FAR + FRR))\%$$

Побудова залежності відносини FRR від відносини FAR для різних типів систем біометричної автентифікації дає цікаву виставу про компроміси між безпекою та зручністю. Ідеальне зображення має мінімальний FAR, а також FRR, але насправді біометричні системи автентифікації знаходяться десь на кривій, де або високу зручність (низький FRR), але більш низький рівень безпеки (високий FAR) або навпаки.

Коефіцієнт відмови в реєстрації (FTE або FER) – відсоток введення даних які вважаються недійсними і які не вдається ввести в систему. Відмова від реєстрації відбувається, коли дані, отримані датчиком, вважаються недійсними або низької якості.

Коли людина не може зареєструватися в біометричній системі, це називається відмовою в реєстрації. FTE виникає, коли у людини, що використовує систему, недостатньо біометричних даних. Крім того, FTE залежить від дизайну і політики впроваджуваних біометричних систем. Якщо показник FTE вище, виникає проблемна ситуація [11].

FTE (FER) вимірюється за відсотком відмов наступним чином:

$$FER = \frac{\text{Number of unsuccessful enrollment attempts for a person}}{\text{Number of all enrollment attempts for a person}}$$

Точність результатів будемо розраховувати за наступною формулою:

$$\frac{\text{Кількість невдалих перевірок}}{\text{Кількість вдалих перевірок}} * 100\% ,$$

де кількість невдалих перевірок – це випадок, коли не повинно було автентифікувати, але змогло; кількість вдалих перевірок – це сума тих кого повинно було автентифікувати та тих кого не повинно, але це є вірним.

Час навчання (T) = Кінцевий час навчання – Початковий час навчання (секунди).

Параметри FRR, FAR, FTE, точність розпізнавання та час навчання обрані у якості основних порівняльних характеристик в процесі аналізу вищеописаних методів розпізнавання.

2. Особливості реалізації системи біометричної автентифікації за розпізнаванням рис обличчя.

Розпізнавання обличчя – це метод, який автоматично ідентифікує або перевіряє людину за допомогою цифрового зображення або відео-рамки. Одним із способів зробити це є порівняння зображення особи з прикладами в базі даних.

Для навчання та тестування обрана Georgia Tech face database. Попередня обробка зображень в базі даних не виконується. Вона містить в загальній складності 750 зображень, по 15 зображень на 50 осіб. Зображення знаходяться в форматі JPEG, і всі вони мають різні розміри. З 15 зображень на людину – 4 зображення було взято в якості навчальної вибірки, а решта 11 зображень було взято в якості тестових зображень. В цілому 200 зображень є тестовими зображеннями, а 550 зображень – навчальна вибірка. Зображення, розміщені в базі даних мають роздільною здатністю 640×480 пікселів. Середній розмір осіб на зображеннях становить 150×150 пікселів.

Зображення показують особу фронтально, тобто мінімально спотворює його зовнішність, а також лівий профіль та правий профіль (приходящий профіль (кінчик носа виходить за обриси щоки, при цьому ніс закриває очі) та минаючий профіль) з різними виразами обличчя, а також з різними аксесуарами (окуляри, макіяж, татування тощо), умовами освітлення і масштабом.

Слід визначити, що обличчя людини має численні відмінні риси. Це понад 80 точок, деякі з яких можуть бути виміряні за допомогою програмного забезпечення. За цими вимірами створюється спеціальний числовий код, який називається Aface Print, і саме цей код представляє обличчя в базі даних.

Найбільш ефективним способом біометрії за рисами обличчя вважається 2-d ідентифікація.

3. Застосування обраних методів до розв'язання задачі ідентифікації особи.

З метою розв'язання задачі ідентифікації було розроблено діаграми варіантів використання та діаграму класів, спроектовано програмний додаток й обрано апаратні

й програмні засоби його реалізації (мова програмування Python, оболонка Jupyter, спеціальні бібліотеки). Для проведення машинного навчання встановлено середовище розробки та тестування Anaconda з механізмом Jupyter Notebook.

Біометрична система розпізнавання може працювати в двох різних режимах: ідентифікація або перевірка. Ідентифікація – це процес встановлення особистості людини шляхом вивчення біометричної моделі, розрахованої на основі біометричних характеристик людини.

У разі ідентифікації система навчається за шаблонами кількох людей. Для кожної людини на цьому етапі навчання розраховується біометричний шаблон . Шаблон, який буде ідентифікований, зіставляється з кожним відомим шаблоном, розраховується відстань, що описує схожість між шаблоном та зображенням. Система присвоює шаблон людині з найбільш схожими біометричними параметрами. Для запобігання правильного визначення шаблонів самозванця (в даному випадку всіх шаблонів осіб, не відомих системі) схожість повинна перевищувати певний рівень. Якщо цей рівень не досягнутий, шаблон відхиляється.

Перевірений шаблон порівнюється з індивідуальним шаблоном людини. Подібно ідентифікації, перевіряється, чи достатньо подібності між шаблоном і зображенням для забезпечення доступу до захищеної системи.

Використовуємо оцінки параметрів, щоб виявити схожість між шаблоном і біометричним шаблоном, які описано у першому розділі. Чим вище бал, тим вище схожість між ними. Доступ до системи надається тільки в тому випадку, якщо оцінювальні параметри для навченої системи (ідентифікація особи), вище певного порогового значення.

Експеримент проводився на тестовій базі даних, у якій є 50 фотографій людей по 15 зображень для кожного. Навчання проходило послідовно від 2 до 12 зображень, де, наприклад два - це зображення на яких проходить навчання та 13 зображень для тестування, і так далі, нарощуючи кількість зображень для навчання. Усі результати оцінюються за кількістю тестових зображень.

У рамках дослідження було вирішено оцінювати параметри FAR, FRR, точність та час розпізнавання зображень. Додатковою особливістю стало застосування при дослідженнях алгоритму для створення цифрового макіяжу.

Результати дослідження основних характеристик алгоритмів класифікації зображень наведено в таблицях 2-5.

Таблиця 2 – Характеристика FAR (%)

Метод	Кількість зображень особи					
	2	4	6	8	10	12
SVM	0,792	0,281	0,373	0,232	0,566	0,098
k-NN	0,192	0,281	0,373	0,232	0,566	0,478
Норма Фробеніуса	0,081	0,001	0,073	0,051	0,093	0,095

З огляду на унікальні вимоги і обмеження, з якими стикаються системи розпізнавання, парадигма навчання CNN не підходить для ідентифікації. Ця невідповідність методу вимогам швидкості та точності в умовах малих оперативних вибірок була виявлена на початкових етапах дослідження.

Таблиця 3 – Характеристика FRR (%)

Метод	Кількість зображень особи					
	2	4	6	8	10	12
SVM	0,793	0,687	0,475	0,58	0,475	0,273
k-NN	0,981	0,602	0,152	0,013	0,016	0,125
Норма Фробеніуса	0,294	0,182	0,312	0,209	0,046	0,113

Параметри FRR, і FAR показують тенденцію до зниження, при збільшенні даних (зображень), які поступають у систему.

Таблиця 4 – Точність розпізнавання (%)

Метод	Кількість зображень особи					
	2	4	6	8	10	12
SVM	98,415	99,032	99,152	99,188	98,959	99,629
k-NN	98,827	99,117	99,475	99,755	99,418	99,397
Норма Фробеніуса	99,625	99,817	99,615	99,74	99,861	99,792

Проаналізувавши отримані результати можна зробити висновок, що ймовірність того, що система неправильно визначає збіг між вхідним шаблоном і відповідним шаблоном в базі даних має найгірший показник у метода К-найближчих сусідів(помилкові прийняття), а норма Фробеніуса та метод опорних векторів, дають близький результат.

Ймовірність що система неправильно визначає збіг між вхідним шаблоном і відповідним шаблон в базі даних має 0,27% помилок у метода опорних векторів, це непоганий показник, але в порівнянні з методом К-найближчих сусідів та нормою Фробеніуса у яких нульовий відсоток помилки, метод опорних векторів не є найкращим рішенням.

Тож сумарно за трьома параметрами можна сказати, що найкраще рішення для задачі класифікації це – норма Фробеніуса.

Таблиця 5 – Час навчання для 3х методів (сек)

Метод	Кількість зображень особи					
	2	4	6	8	10	12
SVM	50	100	120	140	160	200
k-NN	20	40	60	80	100	120
Норма Фробеніуса	25	50	75	125	150	175

Відносно точності розпізнавання, найкращі результати були виявлені у метода опорних векторів і норми Фробеніуса. Але, якщо за основу вибирати показник швидкості, то метод К-найближчих сусідів буде найшвидшим [12].

Висновки

У роботі проведено аналіз існуючих методів біометричної автентифікації, у тому числі методу опорних векторів, К-найближчих сусідів, норм Фробеніуса й згорткових нейронних мереж.

Проведено тестування вказаних методів. Для цього обрана база даних з заздалегідь підготованими зображеннями. У ній зібрані різні можливі варіанти зміни

обличчя людини (окуляри, нахил голови і так далі). Виконано аналіз помилок, які можуть з'являтися при роботі систем. Для покращення роботи системи та зменшення помилок було вирішено для навчання алгоритмів та тестування використовувати дублікатні зображення - з алгоритмом цифрового макіяжу та без означеного. Застосовано авторський алгоритм попередньої обробки цифровим макіяжем.

Проаналізовано отримані результати.

Метод згорткових нейронних мереж було вилучено, як нездатний вдовольнити основним вимогам, що висуваються до ідентифікації осіб з застосуванням методу біометричної ідентифікації за рисами обличчя. CNN не надала задовільних результатів, так як швидкість навчання та точність виявилися неприйнятними.

Виявлено, що метод опорних векторів задовільні результати дав для показників точності, коефіцієнта помилкового відхилення та частоти помилкового прийняття; К-найближчих сусідів – має найкращі показники за часом, але нижчу точність; норма Фробеніуса – незважаючи на те, що цей метод без навчання, показав найкращі результати серед заявлених методів.

Загальний висновок по отриманим результатам – в залежності від того де буде впроваджуватися система треба і обирати метод для розпізнавання, так як кожний алгоритм має як недоліки, так і переваги. Все залежить від того, який показник для системи має бути основним. Якщо це час, то К-найближчих сусідів найкращий, якщо точність чи мале число помилок – норма Фробеніуса.

Список літератури

1. Fingerprint vs. Finger-Vein Biometric Authentication [Електронний ресурс]. – Режим доступу: <https://www.bayometric.com/fingerprint-vs-finger-vein-biometric-authentication/> – Заголовок з екрану.
2. Ворона В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – М.: Горячая линия – Телеком, 2013. — 272 с.
3. Trokielewicz M. Cross-spectral Iris Recognition for Mobile Applications using High-quality Color Images / M. Trokielewicz, E. Bartuzi // Journal of telecommunications and information technology(2016). – pp. 91-97
4. Лакин Г. Ф. Биометрия / Г. Ф. Лакин. – М.: Высшая школа, 1990.- 352 с.
5. Understanding of Convolutional Neural Network (CNN) — Deep Learning [Електронний ресурс]. – Режим доступу: <https://medium.com/@RaghavPrabhu/understanding-of-convolutional-neural-network-cnn-deep-learning-99760835f148> – Заголовок з екрану.
6. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – Диалектика-Вильямс, 2018. – 1103 с.
7. Whitehill, J., Serpell, Z., Lin, Y. C., Foster, A., & Movellan, J. R. (2014). The faces of engagement: Automatic recognition of student engagement from facial expressions. Affective Computing, IEEE Transactions on, 5(1), 86-98.
8. Gamboa H., Fred A. A behavioral biometric system based on human-computer interaction. Proc. SPIE. 2004; 5404:381–393.
9. U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, “Facerecognition systems under morphing attacks: A survey,” IEEE Access, 2019.
10. S.S. Keerthi, C.-J. Lin. Asymptotic Behaviors of Support Vector Machines for Gaussian Kernel // Neural Computation, V. 15, 2003, pp. 1667–1689.
11. Draper B.A., Baek K., Bartlett M.S., Beveridge J.R. Recognizing faces with PCA and ICA. Comput. Vis. Image Underst. 2003; 91:115–137.
12. Маслова Н.О., Полуніна Д.О. Дослідження методів ідентифікації особи в системах біометричної автентифікації (ПМІ-2019): Тези другої всеукраїнської науково-практичної інтернет-конференції, Бахмут : Навчально-науковий професійно-педагогічний інститут української інженерно-педагогічної академії, 2019. с. 115-116.

References

1. Fingerprint vs. Finger-Vein Biometric Authentication [Yelektronniy resurs]. - Rezhim dostupu: <https://www.bayometric.com/fingerprint-vs-finger-vein-biometric-authentication/> – Zagolovok z yekranu.
2. Vorona V. A. Sistemy kontrolya i upravleniya dostupom A. Vorona, V. A. Tikhonov. - M .: Goryachaya liniya - Telekom, 2013. – 272p.

3. Trokielewicz M. Cross-spectral Iris Recognition for Mobile Applications using High-quality Color Images / M. Trokielewicz, E. Bartuzi // Journal of telecommunications and information technology(2016). – pp. 91-97.
4. Lakin G. F. Biometriya / G. F. Lakin. - M.: Vysshaya shkola, 1990.- 352 p.
5. Understanding of Convolutional Neural Network (CNN) — Deep Learning [Yelektronniy resurs]. - Rezhim dostupu: <https://medium.com/@RaghavPrabhu/understanding-of-convolutional-neural-network-cnn-deep-learning-99760835f148> – Zagolovok z yekranu.
6. Khaykin S. Neyronnyye seti: polnyy kurs / S. Khaykin. - Dialektika-Vil'yams, 2018. – 1103 p.
7. Whitehill, J., Serpell, Z., Lin, Y. C., Foster, A., & Movellan, J. R. (2014). The faces of engagement: Automatic recognition of student engagement from facial expressions. Affective Computing, IEEE Transactions on, 5(1), 86-98.
8. Gamboa H., Fred A. A behavioral biometric system based on human-computer interaction. Proc. SPIE. 2004; 5404:381–393.
9. U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, “Facerecognition systems under morphing attacks: A survey,” IEEE Access, 2019.
10. S.S. Keerthi, C.-J. Lin. Asymptotic Behaviors of Support Vector Machines for Gaussian Kernel // Neural Computation, V. 15, 2003, pp. 1667–1689.
11. Draper B.A., Baek K., Bartlett M.S., Beveridge J.R. Recognizing faces with PCA and ICA. Comput. Vis. Image Underst. 2003; 91:115–137.
12. Maslova N.O., Polunina D.O. Doslidzhennya metodiv identyfikatsiyi osoby v systemakh biometrychnoyi avtentyfikatsiyi (PMI-2019): Tezy druhoi vseukrayins'koyi naukovo-praktychnoyi internet-konferentsiyi, Bakhmut: Navchal'no-naukovyy profesiyno-pedahohichnyy instytut ukrayins'koyi inzhenerno-pedahohichnoyi akademiyi, 2019. - P 115-116.

Надійшла до редакції 12.09.2019

N.O. Maslova, D.O. Polunina

BIOMETRIC AUTHENTICATION METHODS FOR PERSONAL IDENTIFICATION

The article presents the results of a study of biometric authentication methods used in access control systems in terms of their reliability, accuracy and training time. The feasibility of using convolutional neural networks, methods of support vectors, the method of K-nearest neighbors, and the Frobenius norm is considered.

The testing of these methods has been carried out. For this, a database with pre-prepared images has been selected. It contains various possible options for changing a person's face (glasses, head tilt, and so on). The analysis of errors that may occur during operation has been performed. To improve the system and reduce errors, it was decided to use duplicate images for training algorithms and testing - with and without the digital makeup algorithm. The digital make-up preprocessing algorithm is copyrighted.

The method of convolutional neural networks was excluded, as it did not meet the basic requirements for authentication by the method of biometric identification by facial features, as the speed of training and accuracy were unacceptable.

It has been revealed that the support vector method has satisfactory results for accuracy indicators, the coefficient of false deviation and the frequency of erroneous acceptance, meanwhile the method of K-nearest neighbors has better time performance, but lower accuracy. The Frobenius norm, despite being the method without training, has shown the best results among the claimed methods.

The general conclusion on the results obtained: a method for recognition should be chosen according to the system it is implemented in, since each algorithm has both advantages and disadvantages. Everything depends on the indicator that should be the main one for the system. If it is the time, the method of K-nearest neighbors is the best; if it is the accuracy or a small number of errors, the Frobenius method is the best one.

Keywords: *identification, biometric systems, identification, method of support vectors, K-nearest neighbors, Frobenius norm, protection systems, image classification.*

Відомості про авторів

Маслова Н.О., канд. техн. наук, доцент, ДВНЗ «Донецький національний технічний університет»; natalia.maslova@donntu.edu.ua

Полуніна Д.О., магістрант, ДВНЗ «Донецький національний технічний університет»; polunina.d.97@gmail.com

Maslova N.O., Candidate of Technical Sciences, Associate Professor, SHEE “Donetsk National Technical University”; natalia.maslova@donntu.edu.ua

Polunina N.O., master student, SHEE “Donetsk National Technical University”; polunina.d.97@gmail.com