

## АНАЛІЗ ДВОХ МЕТОДІВ АВТЕНТИФІКАЦІЇ ОСОБИ ДЛЯ ЗАСТОСУВАННЯ В ЕЛЕКТРОНОМУ БІОМЕТРИЧНОМУ ПАСПОРТІ

### Вступ

В проекті закону України “ Про державний демографічний реєстр ” в якості основних способів запропоновано два способи автентифікації особи на основі підпису і біометричних ознак геометрії обличчя. Перший зі способів запропонований давно і набув широкого застосування в дактилоскопії та перший випадок відноситься до 1900 р. Перше застосування автоматизованого розпізнавання осіб по геометрії обличчя відноситься до 60-х років минулого століття. На наш погляд і нині актуальним є аналіз та порівняння цих методів з метою вибору більш ефективного. Зрозуміло, що вживання ефективного вимагає введення показників ефективності і це також актуальна задача. Більш актуальною являється є задача ефективності двох способів, коли вони застосовуються одночасно.

Метою статті є оцінка і порівняльний аналіз методів біометричної автентифікації, що базуються на використанні підписів та геометрії обличчя, а також оцінка ефективності у випадках, коли для автентифікації застосовуються два методи одночасно.

### Основні галузі застосування біометричних даних

Інтеграція Україні до Європи зачіпає не лише економічну і політичну, але і соціальну сферу життя наших громадян. Європейський союз визначив набір протоколів для реалізації ЕАС (доступу до критичних даних (біометричних даних) в своїх електронних паспортах (ЕП, ePassport)). В Україні і в країнах ЄС ведеться робота з впровадження біометричних паспортів.

Основними російськими стандартами з біометричної автентифікації є ГОСТ Р ISO/IEC 19794-6-2006, ГОСТ Р ISO/IEC 19794-5-2006, ГОСТ Р ISO/IEC 19794-2-2005, ГОСТ Р ISO/IEC 19794-4-2006, ГОСТ Р ISO/IEC 19785-1-2008, ГОСТ Р ISO/IEC 19794-7-2009, ГОСТ Р ISO/IEC 19795-2-2006.

Біометричний паспорт – це документ, що дає право на виїзд за межі країни і в'їзд до іноземних країн. Основною відмінністю електронних документів від існуючих паперових аналогів є те, що в них може бути внесений біометричний набір характеристик, замінити які важче ніж надрукований набір даних, і відповідно набагато важче видавати себе за власника паспорта. Біометричні дані є особливо критичною інформацією, доступ до якої мають отримувати виключно ті системи перевірки, які можуть підтвердити свої повноваження на дані дії. Основними джерелами з питань біометричного паспорта є різноманітні публікації організації цивільної авіації ICAO.

Автентифікація на основі біометричних даних – це засіб автоматичного розпізнавання особи на базі унікальних фізичних або поведінкових параметрів людини. Автентифікація виконується за допомогою порівняння отриманих біометричних характеристик і шаблонів (еталонів), що зберігаються у базі даних, в залежності від характеристик, які при цьому використовуються.

Біометричні системи поділяються на статичні та динамічні. До методів першої групи відносяться такі види автентифікації: за відбитком пальця, за формою долоні, за розташуванням вен на лицьовій стороні долоні, по сітківці ока, по райдужній оболонці ока, за геометрією обличчя, за термограмою обличчя, за ДНК, інші методи. До динамічних методів відносять автентифікацію за рукописним почерком (динамічний підпис), за клавіатурним почерком, за голосом, інші методи. В даний час активно використовуються такі біометричні ознаки, як відбитки пальців, геометрія обличчя, особливості голосу, райдужна оболонка ока, рукописний (динамічний) підпис.

## Автентифікація осіб за біометричними ознаками геометрії обличчя

Обличчя – це передня частина голови, на ньому знаходяться: очі, брови, ніс, рот, щоки, лоб і підборіддя. Обличчя дуже чітко висловлює (міміка) людські емоції, такі як біль, радість, розчарування, втому, неспокій, злість. Обличчя є найбільш індивідуальною частиною тіла людини, тому саме по його цілісному сприйняттю відбувається ідентифікація однієї особи іншою [1]. Автоматизоване розпізнавання осіб – відносно нове поняття. Початок розвитку бере з 60-х років минулого століття, перша напівавтоматична система для розпізнавання осіб прагнула, щоб адміністратор визначив місцезнаходження особливостей обличчя (таких як очі, вуха, ніс і рот) на фотографіях перш, ніж було розраховано відстані і відношення до загального орієнтуру (еталонного зображенням на даний момент), які були тоді, в порівнянні з сьогоденням, довідковими даними.

Фотографія та цифровий опис особи заносяться в базу даних, з якої згодом порівнюється розпізнаване особа. На основі набору біометричних даних і їх обробки формується якийсь електронний зразок як унікальне у своєму роді число, що відноситься до конкретної особистості.

Вибір і виділення ознак грають в розпізнаванні образів ключову роль. Є три категорії ознак: фізичні, структурні і математичні.

Фізичні та структурні ознаки виражаються через форми обличчя (овал особи, геометрія його основних частин), його колір, а також колір волосся і т.д. Найбільш часто використовуваною ознакою – яскравість. До фізичних і структурних ознак можна віднести також координати точок обличчя в місцях, відповідних зміні контрасту (брови, очі, ніс, вуха, рот і овал).

До математичних ознак належать спектри вихідних образів, характеристики, градієнти зміни яскравості та інше, статистичні отримані в результаті математичного перетворення вихідних ознак [Біометрія. Зображення обличчя [2].

Інформаційні знаки обличчя [2]:

- форма обличчя;
- співвідношення частин обличчя між собою (лоб, середня і нижня частини обличчя);
- форма чола, скул і підборіддя;
- симетрія / асиметрія особи;
- форма і розмір вуха, спосіб його прикріплення, форма частин вуха
- форма, величина, розташування очей, рота, носа;
- лінії зморшок.

Методи автентифікації [5]:

### 1. Метод збирання характеристик

Способи виділення розрізняються залежно від використовуваного способу представлення і способу його редукції (скорочення).

Ознаки яскравості збираються в вектор з допомогою перерахуванням значень яскравості кожного пікселя. Для образу  $112 \times 92$  пікселів виходить матриця порядку 10304. У такому просторі пошук практично неможливий, тому зображення попередньо зменшується до прийнятних розмірів.

Серед математичних ознак найчастіше використовуються спектральні ознаки, отримані в результаті перетворення Фур'є. Розмір початкового простору ознак може скласти до 200 елементів. При цьому для більш високого рівня розпізнавання перетворення Фур'є застосовуються не для усередненого образу, а для кожного окремо.

Аналіз локальних ознак. На образі виділяються координати особи і локальних ознак (наприклад, куточки рота, ніс, очі і т.д.) Координати ознак і відстані між ними дозволяють описати особа за допомогою точок і параметрів, які потім будуть використовуватися при розпізнаванні.

## 2. Кореляційний метод

Найпростіший з вище перелічених методів. Якщо умови отримання нових образів відповідають умовам отримання еталона (освітлення, пункт спостереження обличчя, нахил, масштаб, фон і т.д.), то кореляція (відповідність) між ними близька до одиниці. Рівень розпізнавання доходить до 96 %.

## 3. Метод на основі перетворень Карунена – Лоєва (ПКЛ)

Цей метод дозволяє значно скоротити розмір еталона, залишаючи тільки ті ознаки, які мають принципове значення для конкретного образу. Рівень правильного розпізнавання стабільно досягає 80 %, навіть при сильних змінах умов. На рис. 1 приведена структурна схема даного методу.

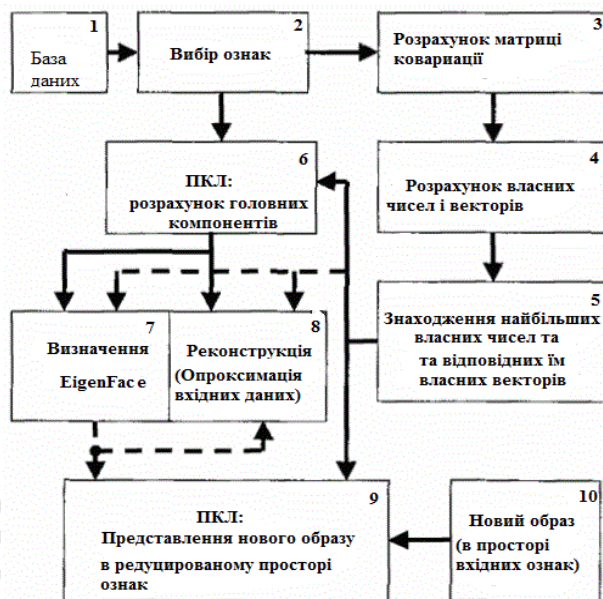


Рис. 1. Схема ідентифікації за допомогою ПКЛ

## 4. Метод на основі лінійного дискримінантного аналізу (ЛДА)

LDA – статистичний підхід для того, щоб класифікувати зразки по класах, що засновані на навчальних зразках з відомими класами [3]. Даний метод, як і попередній, дозволяє скоротити кількість ознак, при цьому істотно покращує класифікацію образів (розрізнення одного від другого). Це дозволяє збільшити рівень розпізнавання – до 99%, навіть при різних умовах.

Для біометричного методу ідентифікації особи за біометричними ознаками геометрії обличчя розглянемо всі ймовірні переваги та недоліки, які містяться в даному методі (дивитись табл.1).

Таблиця 1

Переваги та недоліки методу

Переваги методу	Недоліки методу
<ul style="list-style-type: none"> <li>- низька ціна пристрою отримання зображення;</li> <li>- безконтактність;</li> <li>- зручна і швидка обробка даних;</li> <li>- можливість використання самонавчальючихся систем (нейроні мережі).</li> </ul>	<ul style="list-style-type: none"> <li>- складність реалізації системи;</li> <li>- залежність відеообразів від перешкод;</li> <li>- повина забезпечуватись висока якість зображення.</li> </ul>

## Автентифікація осіб за рукописним підписом

Підпис – один із класичних способів ідентифікації, застосовуваний вже кілька століть в юридичній практиці, банківській справі і торгівлі.

Перші згадки про даний метод датуються приблизно 1900 роком в одній з перших виданих робіт Осборна.

Автоматична перевірка підпису є важливою областю досліджень у зв'язку з соціальними та правовими поняттями та широке використання рукописного підпису як особистий метод перевірки автентичності особи. Даний метод легкий у використанні – це основна його перевага. Є два види підпису: випадкова (ненавмисна) підписка підпису та навмисна (з використанням в корисних цілях).

Є два незалежних способу ідентифікації по підпису:

1. Ідентифікація по малюнку підпису на документі.
2. Ідентифікація по динаміці підпису, що вводиться в комп'ютер.

У першому способі порівнюються два зображення. З цим краще справляється людина. У другому способі є дані про коливання пера при відтворенні підпису в тривимірному просторі ( $X$ ,  $Y$  – координати і  $Z$  – тиск на папірець/планшет). З цим може справитися тільки комп'ютер. На рис. 2 наведено динаміку написання підпису.

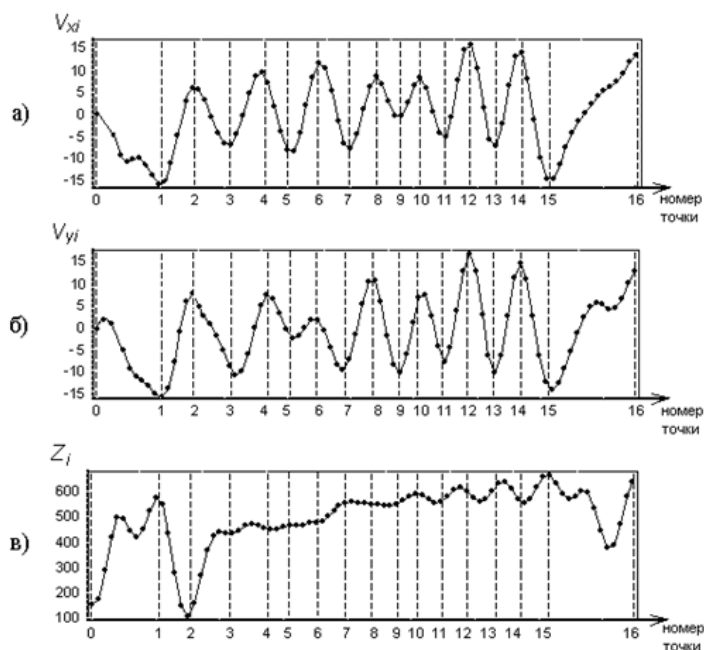


Рис. 2. Криві, що характеризують динаміку написання підпису

Методи перевірки підпису можуть бути класифіковані відповідно з вхідним відомостями про підпис, поділяються на два класи [5]:

1. Он-лайн.
2. Офф-лайн.

Он-лайн метод відноситься до використання функції часу динамічного процесу підписання (наприклад, тиск на ручку залежно від часу), яка отримується за допомогою пристроїв, таких як сенсорні екрани або планшети.

Off-лайн метод відноситься до використання статичного зображення підпису.

Системи перевірки рукописного підпису [5]:

1. Збір даних і первинна обробка. Збір даних можливий при наявності відповідних пристроїв – таблетки переводу підпису в цифрову форму, сенсорні екрани або планшети. Спеціальні засоби для визначення тиску ручки на папір під час підписання. Кроки попередньої обробки підпису перед виділенням ознак – фільтрування шумів (наприклад, з гаусівськими вікнами [4]) і передискретизація.

1.1. Реєстрація, запис. Залежно від стратегії відповідно реєстрація може бути розділена на два класи: заснована на пошуку та заснована на моделі.

Реєстрація заснована на пошуку – зображення вхідного підпису (еталонного) по черзі порівнюється з базою підписів.

Реєстрація заснована на моделі – використовується набір (база даних) підписів для оцінки статистичної моделі, яка описує поведінку особливості виконання підпису особою. Велика проблема, пов'язана зі стадією реєстрації, є зміна часу підпису.

### 1.2. Обчислення подібності

1.2.1. Попереднє вирівнювання. Стадії відповідності взагалі передують попереднє вирівнювання між вхідним підписом та зареєстрованим шаблоном / моделлю (еталонним підписом) дивись рисунок 3.

#### 1.2.2. Узгодження

1.2.3. Оцінка нормалізації. Оцінки одержаної відповідності відбувається шляхом порівняння вхідного підпису з шаблоном, як правило, нормований на загальний діапазон, такий як  $[0, 1]$ , перш ніж порівнюючи їх з порогом ухвалення рішення, використовуються різні функції відображення. Цей крок розрахунку нормалізації використовується при об'єднанні різних обчислювачів в біометричному підході.

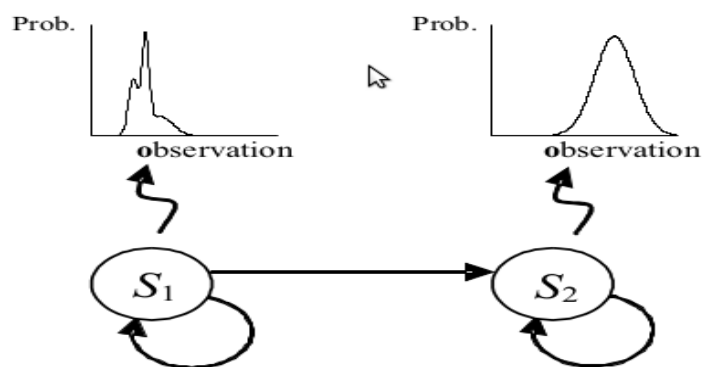


Рис. 3. Ілюстрація вирівнювання

2. Скелетне уявлення рукописної кривої. В основі методу аналізу динамічних кривих лежить ідея виділення характерних або екстремальних точок [1]. При цьому ключове значення мають так звані «вертикальні» екстремуми, що характеризують зміну напрямку руху пера у вертикальній площині. На рис. 4 наводиться приклад «скелетного» уявлення рукописного підпису, отриманий шляхом з'єднання екстремальних точок кривої.



Рис. 4. Зразок скелетного уявлення підпису

Заміна вихідної кривої ламаною лінією досить точно описує поведінку траєкторії дозволяє формалізувати процедуру зіставлення двох кривих.

3. Загальна схема підпрограми пошуку еталонного підпису. З метою дотримання оптимального балансу між продуктивністю підсистеми пошуку і якістю її роботи був реалізований ієрархічний, багаторівневий підхід.

Першим кроком підпрограми пошуку був відбір можливих кандидатів для наступного аналізу. При цьому брався до уваги наступний набір характеристик:

- пропорції (ширина і висота) підпису;
- координати центру мас підпису;
- кількість сегментів;
- кількість петель;
- максимальна довжина штриха в вертикальному та горизонтальному напрямках;
- кількість вертикальних екстремумів;
- відношення числа ліво орієнтованих штрихів до право орієнтованим.

На наступному кроці алгоритму знайдені кандидати передавалися на вхід процедури пошук. Алгоритм пошуку відбирає три кандидати, які доставляють мінімальні штрафи за невідповідність. На третьому кроці знайдені три гіпотези перевіряються на структурну відповідність з пред'явленим зразком. І тільки на заключному етапі порівнюювані рукописні криві представляються за допомогою сплайнів Безье, і таким чином робиться спроба оцінити ступінь схожості еталона і зразка по їх формі. У табл. 2 проаналізовано та наведено можливі недоліки та переваги методу автентифікації особи за рукописним підписом.

Таблиця 2

Переваги та недоліки методу

Переваги методу	Недоліки методу
<ul style="list-style-type: none"> <li>- невисока вартість;</li> <li>- підпис- біометричний параметр людини;</li> <li>- процес верифікації дуже швидкий;</li> <li>- для зберігання шаблонів необхідно мало місця;</li> <li>- на результат не впливає мова, якою говорить особа;</li> <li>- стиснення зображення не впливає на результат.</li> </ul>	<ul style="list-style-type: none"> <li>- високий рівень помилок 1 і 2 роду;</li> <li>- час реєстрації близько двох хвилин;</li> <li>- підпис не надійний спосіб автентифікації та захисту;</li> <li>- висока ймовірність підробки підпису.</li> </ul>

## Висновки

Автентифікацію з використанням рукописного (динамічного) підпису не можна використовувати всюди – зокрема, цей метод не підходить для обмеження доступу в приміщення або для доступу в комп'ютерні мережі. Однак у деяких областях, наприклад в банківській сфері, паспорті громадянина України, а також там, де відбувається оформлення важливих документів, перевірка правильності підпису може стати найбільш ефективним, а головне – необтяжливим і непомітним способом.

Імовірність помилки 1-го роду становить близько 0,01 – це цілком прийнятно. Однак для помилок 2-го роду – це багато. Серед переваг можна відзначити невисоку вартість і відносну звичність для людини. До недоліків відносяться високий рівень помилок 1 і 2 роду, тривалий час реєстрації користувача (більше двох хвилин).

Метод розпізнавання з використанням біометричних ознак геометрії обличчя – це єдиний біометричний спосіб ідентифікації особи з точки зору багатоцільового застосування. На відміну від інших біометричних методів, застосованих для контролю доступу або порівняння в базі даних, технологія розпізнавання образу дозволяє детектувати (знаходити) особу для подальшого порівняння з базою даних. Завдяки вбудованим інфрачервоним випромінювачам комп'ютер легко розпізнає каучукову маску як муляж, що імітує особа. Об'єкт, що проходить автентифікацію, повинен мати людську шкіру, природну міміку і бути "живим", в іншому випадку спрацює звуковий сигнал попередження.

Помилкова відмова доступу (помилкове заперечення): від 10 до 20 на 100 звернень, складає приблизно 10 – 20 % [6].

Помилковий доступ (помилкове визнання): від 100 до 1000 на 100000 звернень до системи, це відповідає 0,1 – 1 % [6].

У табл. 3 наводяться характерні оцінки помилок першого та другого роду для автентифікації особи по геометрії обличчя.

Таблиця 3  
Результати методу

Назва методу	FAR	FRR
Марківська модель	2,9 %	31 %
Метод вейвлет Габора	2,9 %	30 %

Як і аналіз по особистому рукописному підпису, визначення ідентичності по фотографії в паспорті громадянина України відносять до найбільш доступного і визнаного методу розпізнавання особистості. Застосування двох методів для автентифікації особи за біометричними ознаками геометрії обличчя та за рукописним (динамічним) підписом в паспорті громадянина України будуть набагато ефективніші, якщо застосовувати їх одночасно. Так як ймовірність подробиці біометричних даних зменшується в декілька разів в порівнянні з окремим застосуванням кожного з методів. Одночасно зменшаться й помилки як першого, так і другого роду, що призведе до підвищення ефективності і надійності розглянутих двох методів.

**Список літератури:** 1. Болл, Р.М. Основні біометричні параметри // Керівництво по біометрії. – Москва, 2007. – Г. 3. – 47-65 с. 2. Електронний ресурс // Режим доступу: <http://wiki.oszone.net/index.php/> Біометрія. Зображення обличчя. 3. Bolme, D, Beveridge, R., Teixeira, M. and Draper B. The CSU Face Identification Evaluation System: Its Purpose, Features and Structure // International Conference on Vision Systems, Graz, Austria, April 1-3, 2003. (Springer-Verlag). – 304-311 p. 4. Baron, R. and Plamondon, R. Acceleration measurement with an instrumented pen for signature verification and handwriting analysis. IEEE Trans. on Instrum. Measurement, 38(6):1132–1138, 1989. 5. Anil, K. Jain. Handbook of Biometrics. Springer Science+Business Media, 2008. 6. Biometrics catalog // Режим доступу: <http://www.biometriccatalog.org/>.

Харківський національний  
університет радіоелектроніки

Надійшла до редколегії 07.09.2012