Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження методів та засобів оптимальної оцінки біометричного розпізнавання індивідуальних особливостей візерунка пальців

Виконав: студент VI курсу, групи СНм-61
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Мацюк Н.Л.
(підпис) (прізвище та ініціали)

Керівник _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Дуда О.М.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«___» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Мацюку Назару Любомировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів та засобів оптимальної оцінки біометричного розпізнавання індивідуальних особливостей візерунка пальців

Керівник роботи Никитюк Вячеслав Вячеславович, к.т.н., доцент, доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «24» листопада 2023 року № 4/7-1099

2. Термін подання студентом завершеної роботи 26 грудня 2023р.

3. Вихідні дані до роботи Наукові публікації щодо систем біометричної ідентифікації

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Дослідження та аналіз проблематики біометричної ідентифікації даних.
2 Засоби оцінки біометричного розпізнавання індивідуальних особливостей візерунка пальців.
3 Автентифікація на основі відбитків пальців і служби для мобільних систем навчання.
4 Охорона праці та безпека в надзвичайних ситуаціях. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сторінка 2. Актуальність дослідження. 3. Мета, Об'єкт, Предмет дослідження. 4. Завдання дослідження. 5 Стан досліджень в області біометричної ідентифікації та аутентифікації. 6 Обгрунтування вибору біометричного розпізнавання індивідуальних особливостей візерунка пальців. 7. Порівняння відомих методів опрацювання. 8. Засоби оцінки біометричного розпізнавання індивідуальних особливостей користувачів. 9. Служби для мобільних систем навчання. 10. Результати проведених досліджень.11. Висновки. 12. Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин В.С., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач.		

7. Дата видачі завдання 21 вересня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	09.10.2023-13.20.2023	*Виконано*
2.	Підбір наукових джерел про методи	23.10.2023-27.11.2023	*Виконано*
	біометричної ідентифікації користувачів		
3.	Переклад та опрацювання наукових джерел про	30.10.2021-03.11.2023	*Виконано*
	методи біометричної ідентифікації користувачів		
	та методи ідентифікації		
4.	Аналіз способів опису, вибір їхньої та аналіз методу	06.11.2023-10.11.2023	*Виконано*
	опрацювання для біометричної ідентифікації		
	користувачів		
5.	Оформлення розділу «Дослідження та аналіз	13.11.2023-17.11.2023	*Виконано*
	проблематики біометричної ідентифікації даних»		
6.	Оформлення розділу «Засоби оцінки біометричного	20.11.2023-24.11.2023	*Виконано*
	розпізнавання індивідуальних особливостей візерунка		
	пальців»		
7.	Оформлення розділу «Автентифікація на основі	27.11.2023-01.12.2023	*Виконано*
	відбитків пальців і служби для мобільних систем		
	навчання»		
8.	Виконання завдання до підрозділу «Охорона праці»	04.12.2023-08.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	04.12.2023-08.12.2023	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	11.12.2023-15.12.2023	*Виконано*
11.	Нормоконтроль	11.12.2023-15.12.2023	*Виконано*
12.	Перевірка на плагіат	16.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	18.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	26.12.2023	

Студент _____ Мацюк Н.Л.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження методів та засобів оптимальної оцінки біометричного розпізнавання індивідуальних особливостей візерунка пальців// Кваліфікаційна робота освітнього рівня «Магістр» // Мацюк Назар Любомирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кафедра комп’ютерних наук, група СНм-61 // Тернопіль, 2023 // С. 70, рис. – 14, табл. – 2, кресл. – 0, додат. – 2, бібліогр. – 48.

Ключові слова: біометрія, ідентифікація, математична модель, база даних

Дипломна робота присвячена методам та засобам оптимальної оцінки біометричного розпізнавання індивідуальних особливостей візерунка пальців.

В першому розділі дипломної роботи проаналізовано проблематику біометричної індентифікації.

В другому розділі дипломної роботи проаналізовано засоби оцінки біометричного розпізнавання індивідуальних особливостей візерунка пальців.

В третьому розділі дипломної роботи проаналізовані автентифікація на основі відбитків пальців і служби для мобільних систем навчання опрацювання та отримання нових інформативних ознак для біометричної ідентифікації.

Об’єкт дослідження: процес аналізу розпізнавання індивідуальних особливостей даних людини.

Предмет дослідження: методи та засоби оптимальної оцінки даних .

Мета роботи: вибір процесу розпізнавання та обґрунтування методик опрацювання біометричної ідентифікації користувачів.

ANNOTATION

Research of methods and means of optimal assessment of biometric recognition of individual features of finger patterns // Qualification work of the educational level "Master" // Matsyuk Nazar Lyubomirovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Computer of computer sciences, group SNm-61 // Ternopil, 2023 // C. 70, fig. - 14, tab. - 2, chair. - 0, add. – 2, bibliography - 48.

Keywords: biometrics, identification, mathematical model, database

The thesis is devoted to methods and means of optimal evaluation of biometric recognition of individual features of the pattern of fingers.

In the first chapter of the thesis, the problem of biometric identification is analyzed.

In the second chapter of the diploma work, the means of assessment of biometric recognition of individual features of the pattern of fingers are analyzed.

In the third chapter of the thesis, authentication based on fingerprints and services for mobile learning systems are analyzed for processing and obtaining new informative features for biometric identification.

The object of research: the process of analyzing the recognition of individual characteristics of human data.

Research subject: methods and means of optimal data evaluation.

The purpose of the work: the selection of the process of recognition and justification of the methods of processing the biometric identification of users.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

ВП – випадковий процес

ОТ – основний тон

ІТ – інформаційні технології

ШІ – штучний інтелект

ОС – операційна система

ПЗ – програмне забезпечення

ІК – ідентифікація користувача

ЗМІСТ

ВСТУП

Актуальність роботи. Світ справді став меншим з точки зору зв’язку та впливу технологій. У сучасному суспільстві люди більш мобільні, ніж будь-коли раніше, і вони постійно підключаються один до одного за допомогою різних засобів, таких як смартфони, соціальні мережі та інші комунікаційні платформи. Цей рівень зв’язку змінив спосіб нашого життя та мав значний вплив на різні аспекти суспільства.

Однією із значних змін, викликаних цим підключенням, є надання послуг в електронному вигляді. До багатьох послуг, які традиційно надавалися особисто, тепер можна отримати віддалений доступ через інтелектуальні машини та онлайн-платформи. Ця зміна революціонізувала численні сектори, включаючи банківську справу, електронну комерцію, державні послуги, подорожі, охорону здоров’я, освіту, бізнес і соціальні відносини.

Наприклад, у банківському секторі фізичні особи можуть здійснювати транзакції, перевіряти баланси на рахунках і навіть подавати заявки на кредити через системи онлайн-банкінгу або мобільні додатки. Платформи електронної комерції зробили можливим купувати товари та послуги з будь-якого місця та доставляти їх до наших порогів. Уряди також запровадили електронне надання послуг, надаючи громадянам онлайн-портали для доступу до важливих документів, сплати податків і взаємодії з різними державними установами.

У туристичній індустрії люди можуть бронювати авіаквитки, готелі та орендувати автомобілі онлайн, що робить процес більш зручним і доступним. Платформи соціальних мереж змінили наш спосіб спілкування та взаємодії з іншими, дозволяючи нам підтримувати стосунки, ділитися досвідом і співпрацювати в глобальному масштабі.

Ці технологічні досягнення також мали глибокий вплив на такі галузі, як оборона та освіта. В обороні інтелектуальні машини використовуються для спостереження, зв’язку та аналізу даних, підвищуючи можливості збройних

сил. В освіті онлайн-платформи та засоби електронного навчання зробили освіту більш доступною та гнучкою, дозволяючи людям навчатися у своєму власному темпі та з будь-якої точки світу.

Загалом інтеграція технологій у різні аспекти нашого життя зробила наш світ більш взаємопов’язаним і ефективним. Однак важливо враховувати проблеми та наслідки, пов’язані з таким рівнем зв’язку, як-от питання конфіденційності, ризики кібербезпеки та необхідність забезпечити справедливий доступ до цих технологій.

Мета і задачі дослідження. Мета роботи – дослідження оптимальної оцінки та аналіз методик для біометричної ідентифікації користувачів по візерунку відбитка пальців. Задачі дослідження:

- Провести аналіз стану проблеми біометричної ідентифікації користувачів;

- Обґрунтувати оптимальної оцінки ідентифікації користувачів;

- Обґрунтувати аналіз опрацювання змін та отримання нових інформативних ознак ідентифікації користувачів за візерунком пальців.

Об’єкт дослідження: процес аналізу розпізнавання індивідуальних особливостей даних людини.

Предмет дослідження: методи та засоби оптимальної оцінки даних .

Мета роботи: вибір процесу розпізнавання та обґрунтування методик опрацювання біометричної ідентифікації користувачів.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що для задач ідентифікації використано оптимальну оцінку підстановки візерунка пальців користувачів, які взяті з інформаційної бази даних для верифікації ідентифікованого підтвердження користувача за прогнозованою зміною візерунка.

Практичне значення одержаних результатів. Отримані результати можуть бути інтегровані в інтелектуальні системи контролю доступу підвищеної надійності через процедуру ідентифікації користувачів.

Апробація результатів магістерської роботи. Результати роботи були представлені на XI Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 7-8 грудня 2022 року та XI науково-технічна конференція «Інформаційні моделі, системи та технології» – Тернопіль, 13-14 грудня 2023 року

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додаток А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 80 найменування та 2 додатків. Загальний обсяг кваліфікаційної роботи складає 70 сторінок, з них 58 сторінок основного тексту, який містить 14 рисунків.

1. ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПРОБЛЕМАТИКИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ДАНИХ

1.1 Проблема ідентифікації даних

Послуги тепер набагато простіші та оперативніші. Споживання послуг зазвичай базується на парадигмі клієнт-сервер, де машина є сервером, а клієнт – окремим користувачем. Безпека таких систем має бути дуже уважною, оскільки послуга має надаватися лише законному користувачеві, який має бути спочатку ідентифікований. Традиційно ці системи використовували і досі використовують класичні схеми автентифікації на основі облікових даних, що містять секретну інформацію (наприклад, паролі) та/або володіють маркерами (сертифікати, смарт-карти). На жаль, такі системи недостатньо безпечні, оскільки облікові дані можуть бути забуті, викрадені або скопійовані. Фактично, серйозні занепокоєння були пов’язані з безпекою таких систем, оскільки їх вразливість широко використовувалася зловмисниками, щоб шахрайським шляхом отримати доступ до привілейованих прав. Ці випадки шахрайства мають обмежений масштаб у таких країнах, як Алжир, де електронні послуги знаходяться на перших стадіях; однак повідомляється, що понад 17 мільйонів жителів США стали жертвами одного або кількох випадків крадіжки особистих даних у 2014 році (Harrell & Langton, 2015). Статистика підтверджує, що державні та великі приватні організації є найбільш цільовими. З року в рік кількість зростає. Відповідальними за такі незручності можуть бути три основні суб’єкти: і) користувача звинувачують у недостатній обережності для захисту своїх облікових даних, іі) хакер, який скористався необережністю користувача, а також деякими недоліками безпеки в і ііі) стратегія безпеки, прийнята системою ідентифікації. Здається, що система несе відповідальність за більшість пов’язаних збоїв безпеки, оскільки вона повинна враховувати перші два недоліки. Насправді прийнята стратегія

ідентифікації не пов’язана з самим користувачем, скоріше вона базується на тому, що він повинен знати або що є в його розпорядженні. Це основне джерело вразливості та подальших проблем безпеки. Проблема встановлення особи не обмежується лише системами електронних послуг, вона особливо виникає в контрольованих зонах, таких як аеропорти, вокзали, урядові та приватні приміщення, де особи повинні бути ідентифіковані на основі деяких зібраних даних. Проблема гостро постає під час судово-медичної експертизи, де необхідно ідентифікувати трупи та зібрати докази злочину. Цілком зрозуміло, що класичні системи ідентифікації в таких ситуаціях марні. У будь-якому випадку уряди, приватні організації, а також окремі особи глибоко стурбовані зростанням шахрайства з особистими даними.

Біометрія даних та аналіз даних. Біометрія, здається, цілком готова для ефективного вирішення вищезазначених проблем. Це стосується використання фізіологічних та/або поведінкових характеристик для ідентифікації особи. Оскільки біометрична ідентифікація залежить від самої людини, вона надійніша за традиційні системи. Насправді біометрична ідентифікація базується на тому, ким «є» користувач або що він «робить». Ці характеристики невід'ємно пов'язані з самим користувачем і не можуть бути відокремлені від нього; передача чи копіювання біометричних характеристик для використання замість когось абсолютно неможлива. Таким чином, ми можемо надійно перевірити особу, заявлену користувачем. Біометрія революціонізувала спосіб ідентифікації. Це стає питанням будь-якої системи безпеки, особливо в системах контролю доступу, урядових і судово-медичних додатках. Декілька біометричних ознак використовуються для ідентифікації осіб, зокрема: обличчя, райдужка, голос, відбиток пальця, підпис, геометрія руки, вухо тощо. Найбільш домінуючим методом є відбиток пальця. Останнє становить центральну точку нашої дисертації.

Розпізнавання відбитків пальців. Відбиток пальця є найстарішим і найбільш використовуваним біометричним ознакою в проблемах

ідентифікації завдяки широкому прийняттю, точності, безпеці, а також відносній недорогій вартості. Аналіз відбитків пальців можна виконати на трьох рівнях деталізації: на глобальному рівні корисна інформація пов’язана з орієнтованим малюнком, який демонструє хребтовий потік. На локальному рівні дрібниці є найбільш помітними ознаками, що забезпечують індивідуальність відбитка пальця; вони визначаються місцями з локальними розривами хребтів. На більш тонкому рівні розглядаються пори та контури хребта. Алгоритм аналізу відбитків пальців може використовувати інформацію одного або кількох рівнів для розробки процесу розпізнавання. Експлуатація відбитків пальців виходить за межі доменів ідентифікації та безпеки та включає деякі конкретні програми, такі як ідентифікація статі (Rattani, Chen, & Ross, 2014) та визначення індивідуальних предків (Fournier & Ross, 2015). Автоматизація розпізнавання відбитків пальців була абсолютною необхідністю через величезну кількість даних, які щодня обробляються шляхом ручної перевірки. Передові технології, зареєстровані в електронних датчиках і обчислювальних технологіях, зробили автоматизацію реальністю. Автоматизована система ідентифікації за відбитками пальців — це, в основному, процес, заснований на дрібницях, який проходить через кілька етапів, починаючи від отримання, покращення зображення, сегментації, виділення ознак і закінчуючи зіставленням. Системне рішення приймається залежно від результатів відповідності.

Основні проблеми систем ідентифікації відбитків пальців. Хоча автоматизовані системи ідентифікації відбитків пальців (AFIS) є зрілими технологіями, все ж деякі складні завдання потребують додаткового вдосконалення та постійних досліджень. У цій дипломній роботі ми в основному зацікавлені в AFIS на основі деталей; зокрема, ми зосередимося на трьох основних відкритих проблемах у розпізнаванні відбитків пальців:

1- Проблема виявлення сингулярності: сингулярні точки є особливими місцями в глобальному шаблоні відбитків пальців, де структура гребня має

високу кривизну. Існують два основних типи сингулярностей: ядро і дельта точки; перший є центром конвергенції хребтового потоку, тоді як другий є центром його розходження. Традиційно експерти використовували розташування особливих точок (ядра та дельти) для візуальної класифікації та вирівнювання відбитків пальців. Автоматизація такого завдання для точного виявлення як розташування, так і типів, а також кількості існуючих особливих точок не є тривіальним завданням, особливо коли відбиток пальця має низьку якість або розмір корисної гребневої структури зменшений. У цій дисертації ми розробили ефективний алгоритм виявлення особливих точок відбитків пальців на основі оцінки варіацій локального поля орієнтації (Belhadj, Akrouf, Harous, & Ait-Aoudia, 2015).

2- Наявність фіктивних деталей і відсутність справжніх деталей і її вплив на ефективність узгодження: процес вилучення деталей може забезпечити деякі помилково виявлені дрібниці, які називаються фальшивими, оскільки він також може пропустити справжні, які називаються справжніми дрібницями. Незважаючи на те, що надійність цього процесу значною мірою залежить від якості вхідного відбитка пальця та подальших застосованих кроків покращення, наявність фальшивих дрібниць може ввести процес зіставлення в оману для визначення помилкових проміжних відповідностей, що може серйозно вплинути на остаточне рішення про зіставлення, отже, глобальна продуктивність системи ідентифікації. Щоб вирішити цю проблему, ми описали алгоритм зіставлення на основі адаптивного дескриптора дрібниць, який має здатність динамічно адаптувати свої функції відповідно до локального контексту дрібниць. На відміну від більшості найсучасніших алгоритмів зіставлення, створення дескриптора виконується на етапі зіставлення, щоб забезпечити більш гнучку адаптацію.

3- Проблема віддаленої автентифікації за відбитками пальців: хоча AFIS розгортаються в усіх регіонах, вони працюють локально. Тобто етапи отримання та підбору, а також прийняття рішення здійснюються локально.

Розповсюдження електронних послуг передбачає необхідність дистанційної ідентифікації користувача. Сучасні рішення для віддаленої автентифікації на основі біометрії ще недостатньо встановлені, останні ще не використовують весь потенціал біометрії та все ще покладаються на схеми автентифікації на основі паролів, обернуті навколо інфраструктури PKI. Деякі розширені потрібні послуги, такі як невідмова, не можуть бути гарантовані. У цій дипломній роботі ми описали схему віддаленої автентифікації на основі відбитків пальців, застосовану до мобільного навчання. Він заснований на прогресі в системах знімання відбитків пальців (Belhadj, Ait-Aoudia, & Akrouf, 2015). Незважаючи на те, що запропонований алгоритм має справу з контекстом мобільного навчання, його можна розглядати як загальну структуру для забезпечення віддаленої автентифікації на основі відбитків пальців.

1.2 Аналіз та огляд біомедичної автентифікації на основі відбитків пальців

Міжнародна організація стандартизації (ISO) визначає термін біометрія, або біометричне розпізнавання, як «автоматичне розпізнавання осіб на основі їхніх біологічних і поведінкових характеристик» (ISO/IEC2382-37, 2012). У визначенні використовується слово «автоматичний», щоб означати розробку алгоритмів, які повинні виконуватися машинною системою для розпізнавання осіб. Для отримання кращих результатів системі може допомогти людина. «Розпізнавання» має на меті пов’язати особистість з особою на основі деяких фізичних характеристик, властивих частинам її тіла, та/або деяких поведінкових характеристик, створених тілом. Ці характеристики називаються «ідентифікаторами» або «рисами». Приклади фізичних характеристик включають серед іншого: відбитки пальців, обличчя, райдужну оболонку ока тощо. З іншого боку, поведінкові характеристики можуть включати: підпис,

голос, динаміку натискання клавіш тощо. На відміну від класичних систем ідентифікації, які встановлюють особу на основі що він знає (таємна інформація, як-от паролі) та/або що він має (володіння такими об'єктами, як токени, смарт-карти, ліцензії тощо); біометричні системи базуються на тому, ким є людина (біологічні властивості) та/або що вона робить (поведінкові властивості). Ці ідентифікатори безпосередньо пов'язані з особою, тому їх не можна забути, ані скопіювати, ані передати. Біометричні системи використовують різноманітні біометричні характеристики, включаючи відбитки пальців, обличчя, вуха, райдужну оболонку ока, сітківку ока, відбитки долоні, вени, голос, підпис, ходу, запах та інш.

Біометрична характеристика — це вимірювана фізична чи поведінкова характеристика особи, яку можна розрізнити. Він визначає, як буде розпізнаватися особа. Важливим питанням при розробці практичної біометричної системи є відповідь на питання: які характеристики повинна використовувати система, щоб прийняти рішення про індивідуальну ідентичність? Кожна біометрична ознака має свої сильні та слабкі сторони, вибір зазвичай залежить від області застосування та, іноді, від популяції, яку потрібно ідентифікувати. У деяких випадках вибирається більше однієї характеристики. (Anil K Jain, Flynn, & Ross, 2007) визначили деякі вимоги, яким мають відповідати типові біометричні характеристики:

1- Універсальність: кожна особа, яка отримує доступ до програми, повинна володіти характеристиками. Наприклад, ми не можемо використовувати характеристики райдужної оболонки ока для ідентифікації сліпих, оскільки ми не можемо використовувати підпис у середовищі, де більшість населення не пише.

2- Унікальність: базові характеристики мають бути достатньо різними для різних людей, щоб можна було розрізнити двох осіб.

3- Постійність: біометричні характеристики повинні бути стійкими до змін у часі принаймні щодо періоду роботи системи розпізнавання. Характеристика, яка суттєво змінюється з часом, не є корисною біометрією.

4- Можливість вимірювання: біометричні характеристики повинні бути кількісно виміряними, щоб їх можна було обробляти машиною. Відповідні пристрої, підключені до машини, можуть бути використані для отримання та оцифрування біометричних ознак, які пізніше будуть передані в систему розпізнавання.

5-Продуктивність: програма, яка використовує біометричні характеристики, повинна забезпечувати прийнятний рівень продуктивності. Це включає в себе точність зіставлення/час, а також ресурси, виділені для створення загальної системи розпізнавання.

6- Прийнятність: це вказує на те, скільки людей, які мають бути ідентифіковані за допомогою цих характеристик, готові співпрацювати з системою, надавши свої біометричні дані.

7- Обхід: вимірює надійність системи; тобто наскільки легко обдурити систему, щоб вона прийняла неправильне рішення або скомпрометувала інформацію про біометричні дані користувачів. Важко знайти одну біометричну характеристику, яка б відповідала всім вимогам. Практична біометрична система повинна мати прийнятну точність і швидкість розпізнавання з розумними вимогами до ресурсів, нешкідлива для користувачів, прийнятна цільовою аудиторією та достатньо стійка до різноманітних шахрайських атак (Maltoni, Maio, Jain, & Prabhakar, 2009).

Архітектура біометричної системи. Типова біометрична система складається з чотирьох основних модулів (рис. 1.1):

1- Біометричний датчик: він відповідає за фіксацію біометричних характеристик біометричного об’єкта та перетворення їх у цифрову форму для передачі. до наступного модуля. Продуктивність загального процесу значною мірою залежить від якості отриманих необроблених даних. Насправді ці дані

є результатом перетворення реального безперервного явища (наприклад, обличчя) у цифрову дискретну форму (зображення обличчя), що призводить до втрати даних. Якість отриманих даних залежить від технології зчитувача, доданого шуму та ступеня сумісності користувача з системою.

2- Реєстрація: отримані необроблені дані спочатку попередньо обробляються для підвищення їх якості. Після цього субмодуль екстрактора виділяє деякі відповідні дискримінаційні ознаки, щоб створити компактне представлення під назвою «шаблон», яке ефективно відновлює біометричні характеристики. Потім створений шаблон надсилається до системи зберігання. Загалом етап реєстрації дозволяє системі розпізнавання біометричних даних дізнаватися ідентичність справжніх осіб у робочому середовищі.

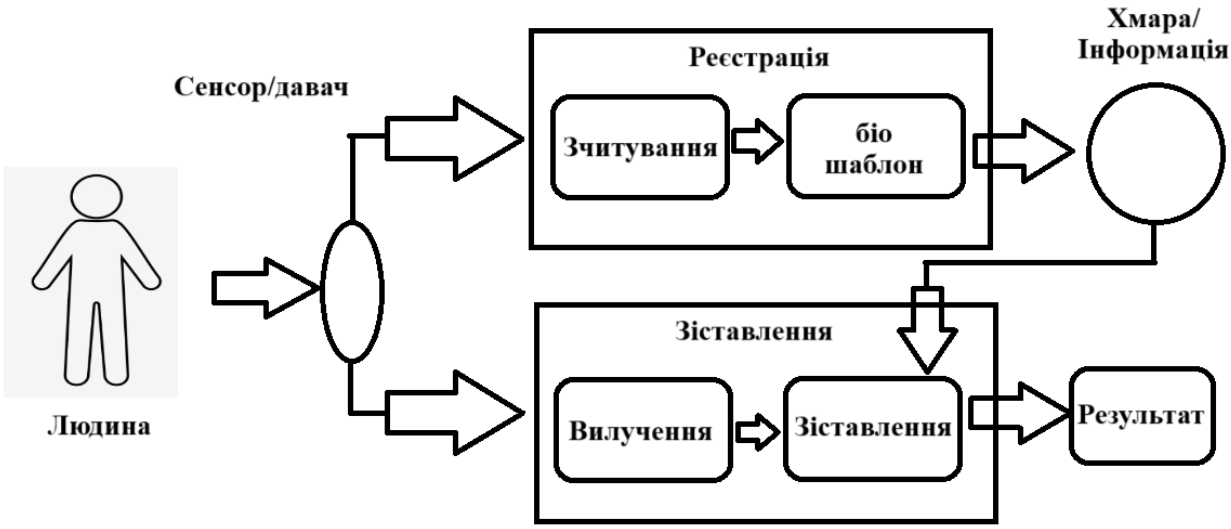

Рис. 1.1 Архітектура біометричної системи

3- Система зберігання: система зберігання може бути простим файлом у простій смарт-картці, оскільки це може бути велика база даних, якою керує SGBD. У зв’язку зі згенерованим шаблоном можна зберігати деякі біографічні відомості (ім’я, паролі, адресу тощо). У будь-якому випадку важливим фактором, з яким потрібно мати справу, є безпека збереженого шаблону.

Зламаний шаблон може допомогти відновити оригінальні біометричні характеристики, що становить реальну загрозу.

4- Модуль відповідності: під час робочої фази системі подається запит на ідентифікацію особи. Він продовжує виділення його дискримінаційних ознак за допомогою підмодуля екстрактора таким же чином, як це було зроблено на етапі реєстрації. Ці витягнуті функції називаються функціями запиту. Після цього збережений шаблон відкликається для порівняння із запитом. Порівняння має на меті підтвердити, що функції запиту та шаблону походять від одного біометричного суб'єкта (особи). Загалом, результатом порівняння є ступінь схожості в діапазоні від 0 (повна невідповідність) до 1 (ідеальний збіг), що дозволяє системі прийняти правильне рішення щодо особи користувача. З іншого боку, біометрична система може працювати як у режимі перевірки, так і в режимі ідентифікації. У режимі перевірки порівняння виконується лише з одним шаблоном у системі шляхом порівняння 1 до 1. Це можливо, коли ми хочемо підтвердити особу, заявлену користувачем. У режимі ідентифікації порівняння здійснюється з усіма записами в базі даних шляхом проведення від 1 до багатьох порівнянь. Це той випадок, коли ми хочемо знати, чи особа вже існує в базі даних. Таким чином, система намагається відповісти на питання «хто є користувачем?»

1.3 Оцінка якості та продуктивності

Система розпізнавання має ідентифікувати два класи користувачів. Користувачі, які зареєстровані в системі, складають «справжній» клас. У них уже є біометричні шаблони, збережені в базі даних. Другий клас, клас «самозванців», складається з усіх інших користувачів, які не є справжніми. Завдання системи — розпізнати справжнього користувача як справжнього, а самозванця — як самозванця. На жаль, це не завжди так. На практиці кілька факторів впливають на отримання біометричних характеристик таким чином,

що два зразки, отримані від одного біометричного суб'єкта користувача, зазвичай не схожі. До них належать: 1- Недосконалості, пов'язані з датчиком: які безпосередньо впливають на якість отриманих даних, таких як шум і роздільна здатність. 2- Умови навколишнього середовища отримання: будь-яка зміна умов навколишнього середовища, таких як освітлення, відстані або технології, відносно початкових умов отримання може призвести до відмінностей між отриманими зразками. 3- Взаємодія користувачів із датчиком: спосіб взаємодії користувача з датчиком може змінюватися від одного отримання до іншого. Це стосується, наприклад, більшого чи меншого тиску на зчитувач відбитків пальців, що впливає на еластичність шкіри. Варіативність, що спостерігається в наборі біометричних ознак індивіда, називається внутрішньокласовою варіативністю, вона має тенденцію бути невеликою; і мінливість між наборами ознак, що походять від двох різних індивідів, відома як міжкласова варіація, яка має тенденцію бути великою.

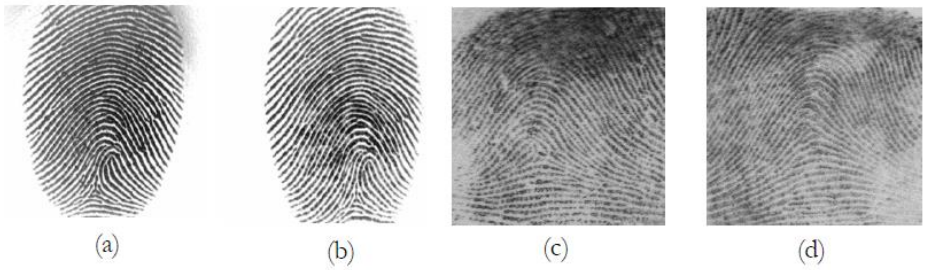

Рисунок 1.2 Варіації відбитків пальців.

(a) і (b) два відбитки пальців одного пальця з низькою варіацією, (c) і (d) два відбитки пальців від різних користувачів із високою варіацією

Рисунок 1.2 ілюструє ці два типи варіацій модальності відбитків пальців. У разі великої відмінності всередині класу система не може ідентифікувати «справжніх» осіб і вважає їх «самозванцями», але у випадку невеликих відмінностей між класами система не може виключити «самозванця» і вважає його «самозванцем». справжній". Це основні помилки, які може зробити

система розпізнавання на етапі зіставлення. Співвідношення помилково розпізнаних користувачів до загальної кількості користувачів у кожному класі може бути основним показником ефективності базової системи.

Частота хибних відхилень і хибних помилок прийняття. Нехай *s(T, Q)* буде показником подібності, який кількісно визначає, наскільки «вхідні» функції запиту *Q* подібні до «збережених» шаблонних функцій *T*. Отже, результат відповідності не є простим “ так/ні», але натомість це значення в діапазоні від 0 до 1. Що ближче оцінка до 1, то точнішою є відповідність між шаблоном і запитом. Щоб прийняти рішення про відповідність, система визначає порогове значення *h*, щоб:

$$\begin{cases} score(T,Q) \geq \eta & \Rightarrow \quad \text{T and Q match (T = Q)} \\ score(T,Q) < \eta & \Rightarrow \quad \text{T and Q don't match (T} \neq \text{Q)} \end{cases} \tag{1.1}$$

Помилки, які біометрична система може зробити на етапі зіставлення, по суті, дві: 1- помилкова помилка відхилення: це відповідає справжній особі, яку розпізнають як самозваного користувача. Очікувана ймовірність того, що два зразки *T* і *Q*, отримані від одного суб’єкта, будуть оголошені як «невідповідні» визначає коефіцієнт помилкових відхилень (FRR).

$$FRR = p(\text{s(T, Q)} < \eta / \text{ T = Q}) = \int_0^{\eta} p(s(T,Q)/T = Q)ds \tag{1.2}$$

де *p(s(T,Q)/T=Q)* — справжній розподіл балів.

Помилка фальшивого прийняття: яка відповідає особі-самозванцю, яку розпізнають як справжнього користувача. Очікувана ймовірність того, що два зразки з однаковими біометричними характеристиками, отримані від різних користувачів, будуть неправильно оголошені як «збіг», визначає коефіцієнт помилкового прийняття (FAR).

$$FAR = p(\mathrm{s(T,Q)} \geq \eta / \mathrm{T} \neq \mathrm{Q}) = \int_{\eta}^{1} p(s(T,Q)/T \neq Q)ds \quad (1.3)$$

де $p(s(T,Q)/T \neq Q)$ — розподіл результатів самозванця

Коефіцієнт помилкових збігів (FMR) і коефіцієнт помилкових невідповідностей (FNMR). використання відповідно FAR і FRR. FMR і FNMR зазвичай використовуються в системах ідентифікації, де біометричні дані запиту порівнюються з набором збережених шаблонів. Рисунок 1.4-(a) ілюструє приклад справжнього та фальшивого розподілу балів і пов'язаних FAR і FRR для заданого порогового значення η. Зверніть увагу, що як FRR, так і FAR є функціями, що залежать від змінного порогового значення η. Зменшення значення цього порогу, щоб зробити систему толерантною до обробки деяких справжніх внутрішніх варіацій і шумів, а отже, для зменшення FRR, призводить до збільшення FAR. З іншого боку, якщо η збільшується, щоб виключити деякі невеликі варіації між користувачами, а отже, для більшої безпеки системи з низьким FAR, тоді FRR зростає. Зменшити обидва значення неможливо. На практиці потрібно знайти компроміс між цими двома показниками, щоб параметри були оптимізовані на основі цільової програми. Однак як розробник системи може описати продуктивність розпізнавання незалежно від порогу η?

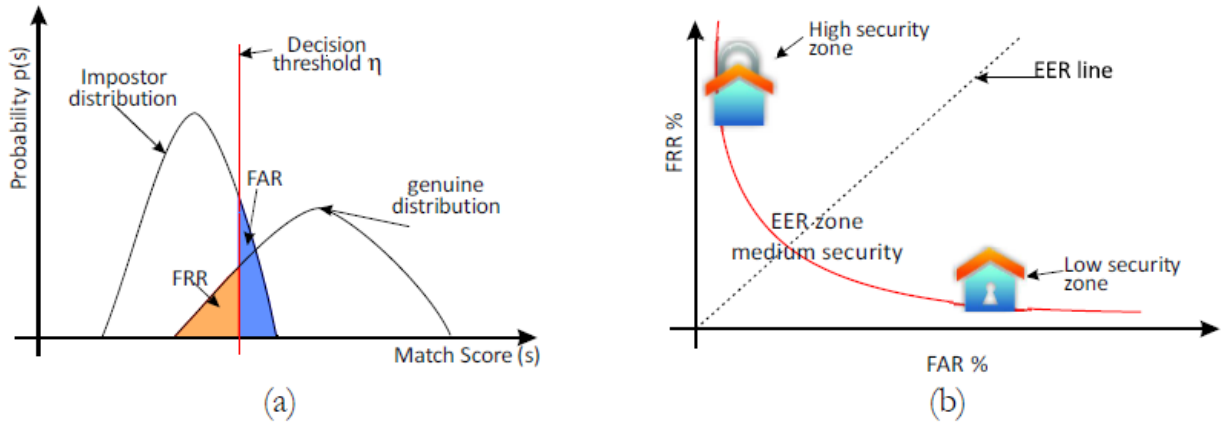

Рисунок 1.4. (a) Справжні та фальшиві розподіли, що визначають ставки FAR і FRR. (b) Крива ROC, що ілюструє три різні зони безпеки.

Крива ROC Крива. ROC є графічною ілюстрацією зміни FRR проти FAR для всіх можливих робочих порогів. Це дозволяє описати продуктивність системи розпізнавання незалежно від порогу η. На рис. 1.4-(b) показано приклад кривої ROC. Згідно з цим малюнком ми можемо виділити три зони безпеки: 1- Зона високого рівня безпеки: вона визначається високими значеннями FRR (що відповідають низьким значенням FAR), так що система вважає більшість користувачів самозванцями (навіть деякі справжні). Це підходить для критично важливих програм, які потребують високого рівня безпеки, таких як військова оборона та банківські рахунки. 2- Зона низького рівня безпеки: визначається високими значеннями FAR (що відповідають низьким значенням FRR), щоб система надала авторизацію більшості користувачів. Це підходить для систем контролю доступу з низьким рівнем безпеки, таких як університети чи ресторани, де «бажаний стабільний і швидкий доступ для справжніх людей і безпека бажана, але це не критична проблема». Це також стосується судово-медичних додатків, де ми не хочемо пропустити жодного підозрюваного. 3- Середня зона безпеки: визначається значеннями FAR і FRR ближче одне до одного. Ця зона визначає компроміс з точки зору безпеки, де потрібен середній рівень, наприклад, у звичайних цивільних біометричних програмах. Точка перетину між першою лінією, що розділяє навпіл, і кривою ROC називається рівною частотою помилок, яка визначає поріг η, для якого FAR і FRR є рівними з одночасним найнижчим значенням, яке може бути. Залежно від цільової програми, де буде розгорнуто систему біометричного розпізнавання, можна налаштувати поріг η у функції бажаного рівня безпеки (низький, середній або високий).

Рівна частота помилок. Рівна частота помилок (EER) є найважливішим показником для оцінки ефективності системи розпізнавання. Це гарантує однакові помилки помилкового прийняття та помилкового відхилення. У біометричній літературі прийнято порівнювати ефективність запропонованих алгоритмів зіставлення за цим показником. Ефективність алгоритму тим

краща, чим нижчий EER. Однак EER, як єдиний критерій, не підсумовує всі характеристики системи. Конкурс FVC (Maio, Maltoni, Cappelli, Wayman, & Jain, 2002; Maio et al., 2004) використовував, окрім EER, інші критерії ефективності, такі як: ZeroFNMR: визначається як найнижчий FAR, при якому хибне відхилення дорівнює нулю, ZeroFMR: визначається як найнижчий FRR, при якому хибне прийняття дорівнює нулю, середній час відповідності та середній час реєстрації, максимальний розмір пам'яті (RAM), виділений для реєстрації та для відповідності, середній і максимальний розмір шаблону. Варто зазначити, що всі помилки, згадані вище, пов’язані з модулем відповідника, інші типи помилок, пов’язані з кожним модулем біометричної системи, можна визначити. Наприклад, помилка невдалої реєстрації (FER) пов’язана з модулем реєстрації, щоб вказати, що він не зміг отримати індивідуальні біометричні характеристики з будь-якої причини.

1.4. Переваги та обмеження біометрії схеми автентифікації

Як зазначалося раніше, класичні схеми автентифікації базуються на тому, що користувач знає, наприклад секретну інформацію (пароль) або/або те, що є в його розпорядженні як ідентифікатори (токени). Вони були та досі використовуються в більшості програм безпеки, навіть у найбільш критичних, таких як банківська справа. Перевага цих систем полягає в тому, що їх легко впроваджувати та інтегрувати в поточні робочі системи з низькою вартістю. Крім того, їх можна поновити в будь-який час (скасувати). Біометрія може надавати розширені послуги, які недоступні або слабші в класичних схемах. Як це робить біометрія?

Переваги біометрії. Підвищена безпека: служба захисту від крадіжки особистих даних безпека, яку забезпечують класичні системи, обмежена, оскільки паролі можна легко вгадати, скопіювати або забути, тоді як маркери можна зламати або вкрасти. (Harrell & Langton, 2015) повідомили, що понад

17,6 мільйонів людей у США стали жертвами одного або кількох випадків викрадення особистих даних у 2019 році. Серед жертв найбільш поширеними були існуючі банківські (38%) або рахунки кредитної картки (42%). типи неправомірної інформації. З іншого боку, випадки крадіжки особистих даних у біометричних системах дуже обмежені (John, 2003). Біометричні дані, як внутрішні характеристики, неможливо вгадати, скопіювати, забути чи вкрасти. Вони не можуть бути відокремлені від людини, тому його присутність необхідна під час аутентифікації, і ніхто не зможе зробити це замість нього.

Підвищена зручність. У класичних системах користувачі повинні пам'ятати або записувати на папері свої паролі або носити з собою свої маркери. Їм не можна надати доступ до послуг, якщо вони забудуть або втратять свої облікові дані. На відміну від класичних систем, біометрію не потрібно запам'ятовувати або щось носити з собою. Доступ до доступних послуг доступний у будь-який час.

Підвищення підзвітності: проблеми з можливістю передачі даних «Біометрія є чудовою технологією, коли питання можливості передачі є проблемою» (V. M. Lee, 2015). Користувачів можна за бажанням замінити іншими в системах відвідування на основі маркерів шляхом передачі їхніх ідентифікаторів. Відповідальність за присутність людей базується на володінні жетоном, а не на тому, хто представляє жетон. Біометрія може вирішити цю проблему в програмах підзвітності, таких як запис біометричних ідентифікацій осіб, які сідають на борт літака, підписується на частину обладнання тощо.

Негативне розпізнавання. У класичних системах розпізнавання один користувач може зареєструвати себе двічі або більше. з двома різними ідентифікаторами, щоб незаконно отримати додаткову перевагу функцій, пропонованих системою. Наприклад, користувач може подати дві або більше заяв на отримання візи, на соціальне забезпечення тощо. Користувачі можуть

легко відмовити в одній зареєстрованій особистості після того, як скористалися послугою. Очевидно, що класичні системи не можуть виявити ці шахрайські дії. Проблему можна сформулювати так: «як система розпізнавання може підтвердити, що певна особа зареєстрована в системі, хоча вона може це заперечувати?» це відоме як проблема негативного розпізнавання. Біометрія готова відповісти на це питання.

Послуга невідмовності. Послуга невідмовності стосується здатності системи пов'язувати дію з користувачем, який виконав її таким чином, щоб ця особа не могла заперечити свою відповідальність за цю дію. Системи на основі токенів і паролів не можуть надати таку послугу, оскільки вони не можуть підтвердити, що один користувач несе відповідальність за перевірену системою дію як виконану ним. Користувач може заперечувати дію та стверджувати, що це зробила інша особа, використовуючи його облікові дані. Наприклад, особа отримує доступ до певних ресурсів комп'ютера, а потім заперечує свою відповідальність. Для консолідації системних звітів керівники використовували б звичайні альтернативи відеоспостереження, які не створюють комфорту для співробітників. Оскільки біометричні характеристики важко обдурити, «будь-яка вчинена дія, яка може бути пов'язана з цією біометрією, ймовірно, була здійснена законним власником даної біометрії. Через це важко повірити виправданням, згідно з якими правопорушення нібито було скоєно іншою особою, яка шахрайським шляхом отримала чиїсь біометричні дані» (V. M. Lee, 2015).

Обмеження біометрії. Фундаментальна перевага паролів і маркерів над біометрією, окрім простоти та можливостей інтеграції, полягає в їх можливості скасування. Насправді ця характеристика є суттєвим «недоліком» біометрії. На відміну від паролів і токенів, які можна скасувати та оновити в будь-який час (хоча настійно рекомендується робити це, навіть якщо вони не скомпрометовані); біометричні характеристики не можна переоформити, оскільки вони не можуть бути відокремлені від власника та замінені іншими

ознаками. Отже, після зламу біометричні характеристики стають марними та втрачаються назавжди. На щастя, нещодавні досягнення в скасованій біометрії, яка фактично є активною областю досліджень, запропонували деякі видатні рішення для подолання цієї проблеми (Campisi, 2013; Patel, Ratha, & Chellappa, 2015).

1.5 Ринок біометрії та ПЗ. Безпека та конфіденційність у біометрії

Компанія Biometrics успішно переконала широкий спектр додатків прийняти не лише як фундаментальний компонент архітектури безпеки, але й як економічний інструмент, який може призвести прямо чи опосередковано до економії витрат і зменшення фінансових ризиків (Nanavati, Thieme, Raj, & Nanavati, 2002). За два десятиліття він швидко і значно просунувся вперед. Останні дослідження підтверджують, що ринок біометрії зросте з 8,7 мільярдів доларів у 2013 році до майже 27,5 мільярдів доларів у 2019 році, зареєструвавши щорічне зростання на 19,8% між 2014 та 2019 роками (Miller, 2015). Модальність відбитків пальців все ще домінуватиме на ринку. Це прискорення виправдовується поширенням електронних послуг, які вимагають ідентифікації, а також зростанням шахрайства та крадіжок особистих даних, з якими необхідно боротися. На додаток до цього, прийняття електронних документів, особливо біометричних паспортів та національних ідентифікаційних карток, великими урядами сприятиме значному розширенню їх використання.

Біометрія зараз використовується, але не обмежується: Державні програми: біометричне національне посвідчення особи, біометричний паспорт, прикордонний контроль, соціальне забезпечення, електронне голосування … Контроль доступу: він може бути фізичним, наприклад системи обліку робочого часу та безпеки дверей або логічний, наприклад доступ до ресурсів віддаленого комп’ютера та інформаційних систем.

Мобільні програми: новітні мобільні телефони оснащені технологіями біометрії, які дозволяють ідентифікувати власника, розблокувати пристрій, здійснювати комерційні операції тощо. Наприклад, Apple і Samsung та інші А-бренду поставляються з вбудованим сканером відбитків пальців разом з інтелектуальне програмне забезпечення, призначене для розпізнавання. Комерційні програми: більшість продуктів інтегрують біометричні дані для покращення досвіду користувача. Доступ до комп'ютерів, інтернет-додатків, електронної комерції, банківських транзакцій тощо. Криміналістичні програми: судово-медичні лабораторії зазвичай використовують біометричні дані у своїх кримінальних розслідуваннях та визначенні батьківства, а також для ідентифікації трупів.

Нові дослідження підтвердили можливість визначення походження предків людини за відбитком пальця. Військові програми: сюди входять системи ідентифікації для використання в польових умовах, програми контролю доступу та моніторингу в чутливих областях, а також розгортання великих баз даних.

З інтенсивним розгортанням біометричних систем виникає кілька проблем безпеки щодо вразливості шаблону. Систему можна атакувати на кожному етапі процесу розпізнавання (Maltoni et al., 2009). Якщо біометричні дані захоплені або викрадені зловмисником, вони можуть бути відтворені, використані не за призначенням і, крім того, використані для реконструкції оригінального біометричного об'єкта. Наприклад, (Cappelli, Lumini, Maio, & Maltoni, 2007) описали успішний підхід до реконструкції зображення відбитка пальця за стандартним шаблоном ISO (ISO/IEC19794-2:2005, 2005). Цей міжнародний стандарт визначає формати шаблонів для систем відбитків пальців на основі дрібниць. Він рекомендує використовувати просту фундаментальну інформацію щодо контрольних точок, таку як двовимірні координати, тип контрольних точок, напрямок і деяку додаткову інформацію про хребти та сингулярні точки. Реконструйований відбиток пальця може бути

використаний для обходу системи ідентифікації та відстеження користувача від однієї програми до іншої шляхом перехресного зіставлення біометричних даних. Зламаний шаблон «може виявити конфіденційну інформацію про особу, яку можна зберігати, обробляти та поширювати без її дозволу. Ця інформація може бути використана для дискримінації людей, наприклад, шляхом відмови у страхуванні людям із прихованими проблемами зі здоров'ям» (Campisi, 2013). Таким чином, необхідно покращити аспекти конфіденційності та безпеки «звичайних» біометричних систем шляхом прийняття суворих стратегій при проектуванні таких систем (Belguechi, Cherrier, Rosenberger, & Ait-Aoudia, 2013)

1.6 Висновки до розділу 1

Біометрія спрямована на імітацію процесу розпізнавання ментальних образів таким чином, щоб ідентифікувати людей. Це більш безпечна та надійна альтернатива класичним схемам автентифікації, заснованим на секретах і маркерах. Технології біометрії використовують фізіологічні та поведінкові характеристики людини для розпізнавання людей у автоматизованому процесі. Ці характеристики мають відповідати деяким вимогам, зокрема універсальності, продуктивності та застосовності. Процес розпізнавання базується на двох етапах: перший, етап реєстрації, має на меті дозволити системі дізнатися особу особи. Він починається з вилучення деяких дискримінантних атрибутів із отриманих даних, які будуть ущільнені для створення шаблону, який зберігатиметься в базі даних. Шаблон — це дуже репрезентативна структура, яка ефективно узагальнює індивідуальні біометричні характеристики. Другий крок, крок зіставлення, викликає вже збережений шаблон для порівняння з нововилученими атрибутами. За результатами порівняння система приймає рішення, чи справді особа є зареєстрованою ідентичністю, на яку вона претендує, чи ні з певним ступенем

достовірності в діапазоні від 0 до 1. Через великі міжкласові та невеликі внутрішньокласові варіації деяких біометричних зразків, рішення системи може бути помилковим. Продуктивність системи розпізнавання традиційно характеризується двома статистиками помилок: FRR і FAR. Перший виникає, коли система відхиляє справжню особу, а другий виникає, коли особу самозванця приймається неправильно. Компроміс між цими двома помилками називається рівною частотою помилок (ERR), де FAR і FRR мають однакові значення. Вважається, що жодна біометрична ознака не може бути точною на 100%; поєднання кількох біометричних характеристик для роботи в єдиній системі розпізнавання може значною мірою консолідувати рішення про розпізнавання та, таким чином, підвищити точність. Ринок і індустрія біометрії знають високе прискорення, виправдане зростанням неконтрольованих електронних послуг, які потребують точної індивідуальної автентифікації, разом із одночасним зростанням шахрайства в усьому світі. Відбиток пальця є найбільш домінуючим способом на ринку; це являє собою компроміс з точки зору точності, безпеки та вартості серед інших модальностей.

2. ЗАСОБИ ОЦІНКИ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ ІНДИВІДУАЛЬНИХ ОСОБЛИВОСТЕЙ ВІЗЕРУНКА ПАЛЬЦІВ

2.1 Індивідуальні особливості візерунка пальців

Відбиток пальця — це найдавніший біометричний спосіб, який використовувався людьми для вирішення проблем ідентифікації, пов'язаних із торгівлею, батьківством дітей, підписанням контрактів тощо в стародавньому Вавилоні, єгипетській та китайській цивілізаціях, що сягають до третього століття до нашої ери (Maltoni, Maio, Jain, & Prabhakar 2009). Це все ще найдомінантніший спосіб у сучасному світі завдяки його прийнятності для широкого кола користувачів і зрілій технології, а також його відносно недорогій вартості. Найпрекрасніше, що стало результатом досвіду людства в розпізнаванні відбитків пальців, це автоматизація процесу ідентифікації. Зараз автоматизовані системи ідентифікації відбитків пальців (AFIS) розгортаються як важлива частина більшості програм, де безпека є головною проблемою. AFIS поєднує передові технології зондування зі складним програмним забезпеченням розпізнавання для створення інтелектуальних програм ідентифікації. Більше того, нещодавні досягнення у дослідженні відбитків пальців показали, що відбитки пальців можуть виявити не лише особу людини, вони можуть визначити стать людини та навіть походження її предків (Fournier & Ross, 2015). У цьому розділі ми описуємо процес розпізнавання відбитків пальців, зосереджуючись, зокрема, на автоматизованих системах на основі дрібниць. Спочатку ми визначаємо, що ми маємо на увазі під відбитком пальця, що робить його придатним для розпізнавання, щоб потім обговорити його індивідуальність. Далі крок за кроком описано процес автоматичного розпізнавання. Подано короткий огляд методів, які зазвичай пропонуються в літературі для досягнення кожного кроку. Хоча в літературі розрізняють

автентифікацію, ідентифікацію та розпізнавання, ми використовуємо ці терміни як синоніми в решті цього документа.

У науці про біометрику відбиток пальця — це візерунок текстури, утворений перемежовуваними виступами та западинами на кінчиках пальців (Maltoni та ін., 2009). У криміналістиці це «відбиток, видимий чи ні, який залишається, коли палець (пальці) людини стикаються з поверхнею, що знаходиться за характерним візерунком з виступів, канавок, завитків, арок та інших елементів, за допомогою яких відбиток може ідентифікувати». (Newton, 2008). Гребні - це сегменти верхнього шару шкіри пальця, які торкаються поверхні, а западини - це нижні сегменти. Після отримання лінії хребтів представляють темні ділянки на зображенні відбитків пальців, тоді як долини розглядаються як міжгребневі простори, що утворюють світлі області (див. рис. 2.1). Хоча гребні тертя здаються добре організованими з однаковою шириною та висотою, вони надзвичайно різноманітні. Їхня ширина варіюється від 100 мкм для дуже тонких виступів до 300 мкм для товстих виступів. Загалом період циклу хребта/долини становить приблизно 500 мкм (Maltoni та ін., 2009).

Рис. 2.1 Зображення відбитка пальця з позначеним: гребінь (хребет) і долиною

Крім того, відбитки пальців чоловіків і жінок деталі відрізняються. У чоловічих відбитках пальців виступи, як правило, товщі та змінені, тоді як у жіночих відбитків пальців виступи більш структуровані та менш товсті з високою щільністю. Ці варіації не так легко вловити неозброєним оком. Порізи та опіки пальців не можуть змінити структуру гребня, вона буде відтворена такою ж оригінальною, якою була, коли шкіра відростає. Утворення відбитків пальців є результатом взаємодії між генами та середовищем, у якому розвивається плід. ДНК дає інструкції щодо того, як має розвиватися шкіра, а навколишнє середовище (утроба матері та потік навколоплідних вод) впливає на її форму. Тому два пальці однієї людини або двох близнюків не можуть мати однаковий відбиток, оскільки останній залежить від випадковості факторів навколишнього середовища (Anil K Jain, Flynn, & Ross, 2007). Остаточна форма відбитка пальця повністю встановлюється на сьомому місяці життя плода і залишається незмінною протягом усього життя особини. Це одна з найпривабливіших характеристик, на основі якої базуються системи ідентифікації за відбитками пальців.

Хоча останні дослідження підтверджують, що стародавні люди усвідомлювали індивідуальність відбитків пальців, систематичні дослідження структури відбитків пальців були розпочаті наприкінці сімнадцятого століття. Історія починається в 1684 році анатомія Nehemiah Grew, який був першим, хто науково дослідив хребти тертя. Пізніше Marcello Malpighi вважається першим, хто використав мікроскоп для вивчення шкіри. Він відзначив наявність виступів, спіралей і петель у відбитках пальців. З тих пір гребінь тертя вивчався протягом багатьох років. У 1788 році German J. C. A. Mayer оголосив про унікальність структури хребта, тоді як Hermann Welcker зазначив, що відбиток його пальця не змінився між першим відбитком і другим, зробленим через 40 років, він вважається першим, хто стверджував, постійність фрикційних хребтів. У 1880 році Henry Faulds опублікував у журналі значення фрикційної шкіри для індивідуалізації, особливо її

використання як докази злочинів. Його вважають першим, хто використав чорнило для зняття відбитків пальців. Трохи пізніше Francis Galton написав книгу про відбитки пальців, ввівши поняття «дрібниць» як постійної та унікальної характеристики. На початку 20 століття розпізнавання злочинців за відбитками пальців стало стандартною практикою. «Здавалося б, що нічого особливого не відбулося щодо ширшої сфери біометрії до 1960-х років, коли поява електроніки та інтегральних схем стала обіцянкою автоматизації» (Krishan, Kanchan, & Bumbrah, 2012). Це дуже допомогло на початку 1970-х років написати алгоритми та використовувати датчики для ідентифікації людей. Коротка історія розпізнавання відбитків пальців наведена на рисунку 2.2. Додаткову інформацію про історію відбитків пальців можна знайти в (Krishan та ін., 2012).

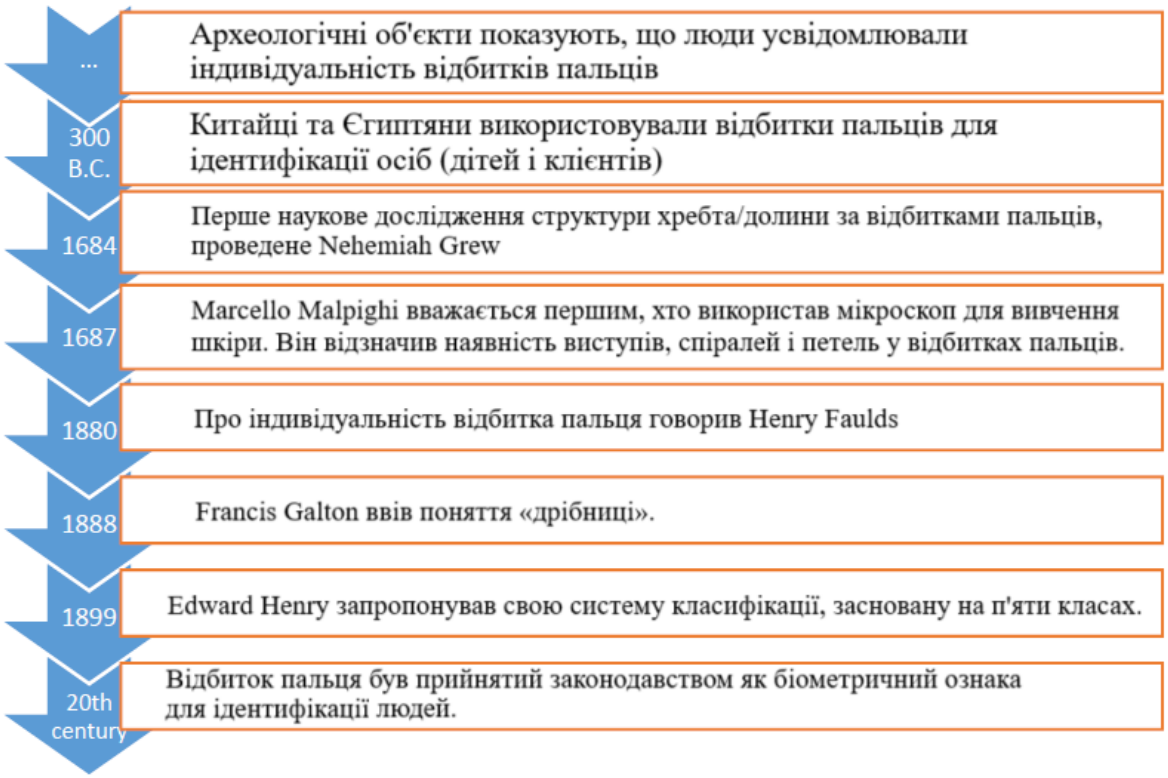

Рис. 2.2 Історія розпізнавання відбитків пальців

Завдяки цим зусиллям технології автоматизованого розпізнавання відбитків пальців зараз швидко розширилися та використовуються не лише в судово-медичних програмах, які першими застосували розпізнавання відбитків пальців, а й у широкому спектрі програм, таких як контроль доступу, вхід на комп'ютер, електронні комерція тощо. Це пояснюється його високою точністю та прийнятністю, а також його недорогою технологією.

Є кілька важливих факторів, таких як шум, спотворення, умови отримання та взаємодію користувача, які роблять два послідовних відбитка одного пальця не зовсім схожими. Отже, відбитки пальців неможливо зіставити безпосередньо, використовуючи просту відстань між їхніми грубими даними у шкалі сірого; натомість розпізнавання відбитків пальців, незалежно від того, чи виконується експертом-людиною вручну, чи автоматично, в основному є процесом, заснованим на функціях. Це означає, що окремий палець, після отримання його відбитка, представляється як набір функцій, витягнутих із зображення, які пізніше будуть ущільнені та збережені в шаблоні, який буде використано на етапі зіставлення. Відбиток можна переглядати на трьох різних рівнях: глобальному, локальному та більш тонкому. На кожному рівні можна витягти деякі відповідні характеристики, що описують відбиток пальця. Рівні деталізації у відбитку — це прості описи різних типів інформації у відбитку.

Функції 1-го рівня охоплюють відбиток у глобальній перспективі, до якого додаються всі глобальні характеристики, пов'язані з орієнтованим текстурним візерунком, представленим структурою хребта/долини. До них відносяться поле орієнтації, частота хребта та сингулярності. Хоча ці функції не несуть жодної інформації про індивідуальність відбитка пальця, їх можна використовувати як ексклюзивні інструменти для зменшення простору пошуку на етапі зіставлення, забезпечуючи класифікацію відбитків пальців, а також для розрізнення шаблонів відбитка пальця та долоні .

Поле орієнтації Відбитки пальців демонструють всюди чітку локальну орієнтацію хребта. З кожним місцем розташування пікселя *p(x, y)* може бути пов'язане значення в діапазоні від *0* до π, що вказує нахил дотичної лінії до хребта в точці p. Усі орієнтації пікселів після обчислення складають поле орієнтації (OF) зображення. На рис. 2.3 (a і b) показано відбиток пальця та пов'язану з ним оцінку OF.

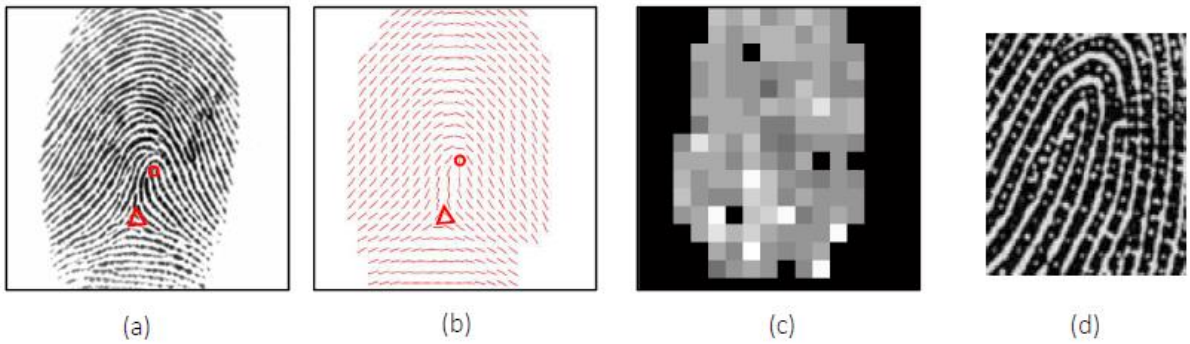

Рис. 2.3 Особливості різних рівнів у відбитку пальця. (a) Оригінальне зображення, що показує гребні тертя з позначеними особливими точками, (b) поле орієнтації, (c) частотне зображення та (d) частковий відбиток пальця з порами.

Частота гребня Подібним чином відбиток пальця демонструє відстань гребня в кожному місці пікселя. Локальна частота хребта в точці p(x, y) — це кількість хребтів на одиницю довжини вздовж сегмента з центром у точці p і ортогонального орієнтації локального хребта (Maltoni, 2009). Це ще одна властивість, яка характеризує відбиток пальця. На рис. 2.3 (c) показано приклад частоти зображення відбитків пальців.

Сингулярні області, сингулярні точки та візерунки відбитків пальців Структура хребта в будь-якому відбитку пальця має тенденцію приймати глобальну конфігурацію зі спеціальною формою. Він розмежовує дві відмінні області: 1) звичайні області: де хребти розташовані плавними паралельними лініями, що мають переважний напрямок, і 2) окремі області: де візерунок

хребта демонструє високу кривизну без домінуючого напрямку. Сингулярні області визначають деякі спеціальні точки, які називаються особливими точками, визначені місцями, де OF швидко змінюється з максимальною кривизною хребта. Edward Hennery в (E. R. Henry, 1990) визначив дві основні сингулярні точки: перша є центральною точкою і визначається як «сама верхня точка самого внутрішнього вигнутого хребта». Друга точка — це дельта-точка, і вона знаходиться в «центрі трикутної області, де зустрічаються три різні хребтові потоки». Кількість і розташування особливих точок безпосередньо впливає на «форму» поля орієнтації, яке можна систематично класифікувати на п’ять класів відповідно до класифікаційної системи Henry (E. R. Henry, 1990): обертання, ліва петля, права петля, арка та шатрова арка (див. рис. 2.4). Три перші класи становлять понад 95% населення (Maltoni та ін., 2009). Більше про сингулярні точки можна знайти в наступному розділі. Головною перевагою функцій рівня 1 є їх здатність знімати навіть із низькою роздільною здатністю зображення.

Рис. 2.4 П’ять основних класів відбитків пальців із позначеними серцевиною (у вигляді кіл) і дельтами (у вигляді трикутників). Зверніть увагу, що звичайна арка не має, за визначенням, жодної особливої точки.

Функції рівня 2. Об’єкти рівня 2 стосуються всіх локальних деталей, пов’язаних зі шляхами хребтів. До них належать початкова позиція хребта

(відносно рамки зображення), шлях, який пройшов хребет (у термінах суміжних пікселів), його розмір (кількість пікселів) і кінцева позиція, де гребінь зупиняється. Зауважте, що всі ці деталі вимірюються в один піксель у ширину, пов’язаний зі скелетним (або розрідженим) зображенням вхідного відбитка. Найпомітнішими характеристиками рівня 2 є локальні розриви, що демонструються хребтами. Насправді хребти часто проходять безперервними кривими і раптово закінчуються в певних точках, які називаються закінченнями хребтів. Інші розщеплюються в деяких точках, які називаються біфуркаціями, утворюючи інші хребти. І закінчення хребта, і точки біфуркацій називаються точками (або елементами Гальтона). Інші форми розривів уже існують у відбитках пальців, такі як вилки, шпори, містки, крапки, перехрестя та трифуркації. Ці особливості набувають форми кількох локальних складених дрібниць, які можна виразити в термінах біфуркації та/або кінцевих дрібниць (Daluz, 2014). Повідомлялося, що майже 50 % дрібниць складаються з кінцевих точок, 25 % — це біфуркації, 15 % — точки. Кількість, напрямки розташування та типи, а також просторові співвідношення між ними є джерелами індивідуальності, тому їх можна використовувати для ідентифікації.

Функції рівня 3. Відбитки пальців, отримані з високою роздільною здатністю, як правило, 1000 точок на дюйм, демонструють деяку корисну інформацію, яку не видно неозброєним людським оком у стандартній роздільній здатності, яку надають основні датчики на ринку, які зазвичай працюють із роздільною здатністю 500 точок на дюйм. Ця інформація додається до пор і форми хребтів. Пори відносяться до отворів уздовж траєкторії хребтів (Рис. 2.3-d). Розташування по вздовж виступів відбитків пальців гарантує індивідуальність пальця за умови використання надійного екстрактора. На практиці пори використовуються разом із деталями або гребнями (A K Jain, Chen, & Demirkus, 2007) у мультибіометричному сенсі,

щоб підвищити точність розпізнавання, особливо коли подаються часткові відбитки пальців без достатньої кількості деталей.

Автоматизована система ідентифікації за відбитками пальців. Запровадження розпізнавання відбитків пальців багатьма агентствами, особливо в судово-медичних і правоохоронних додатках, призвело до появи великих баз даних, які містять мільйони відбитків пальців на основі тисяч запитів, які потрібно щоденно аналізувати. Ручна система пошуку та перевірки відбитків пальців вимагала все більше людських ресурсів, а також тривалого часу для відповіді на один запит. Тим не менш, він наближався до того, що не міг справлятися зі щоденним навантаженням (Krishan, 2012). Автоматизація процесу розпізнавання була абсолютною і терміновою необхідністю для прискорення обробки запитів. При розробці такої автоматизованої системи виникли три основні проблеми: 1) як отримати відбиток пальця, чи записаний він на предметі, чи з живого пальця? 2) як обробити отримане зображення, щоб виділити характерні риси? і 3) як досягти порівняння двох наборів ознак? У результаті в 1972 році було встановлено перший прототип автоматизованої системи ідентифікації за відбитками пальців, який повністю запрацював у 1983 році. З того часу в систему було внесено багато вдосконалень як на апаратному, так і на програмному рівнях.

Автоматизована система ідентифікації відбитків пальців (AFIS) – це комп’ютеризована технологія, яка дозволяє збирати, обробляти та зберігати характеристики відбитків пальців людини для прийняття рішення щодо її особи. Система складається з апаратної та програмної підсистем. Апаратні компоненти в основному складаються із пристрою для зчитування відбитків пальців, центрального процесора (або декількох), інфраструктури зберігання та зв’язку, тоді як підсистема програмного забезпечення складається з ефективних алгоритмів для обробки відбитків пальців.

2.2 Аналіз проблеми зі збігом даних

Методи на основі локальних дескрипторів принесли багато бажаних покращень, зокрема, допуск до локальної деформації, високу здатність розрізняти дрібниці та значні характеристики відповідності. Однак існує низка складних проблем, які необхідно вирішити, щоб підвищити продуктивність, зокрема: статичність дескриптора, наявність фальшивих деталей і відсутність справжніх, окрім високої обчислювальної складності, що становить складні проблеми, які літературі приділяється, на жаль, мало уваги. У наступних підрозділах більш детально обговорюється вплив цих проблем на продуктивність локального дескриптора та розглядаються деякі запропоновані рішення.

Проблема нестабільного статичного дескриптора. Більшість методів зіставлення на основі деталей використовують нестатичний дескриптор. Дескриптор дрібниць вважається статичним, якщо його елементи ознаки попередньо встановлені на основі локальної структури сусідства перед кроком зіставлення, а їхні значення залишаються незмінними протягом усього часу процесу зіставлення. Крім того, той самий дескриптор із однаковими значеннями використовується як посилання на будь-який виданий дескриптор дрібниць, наданий для зіставлення. Однак; локальна структура, на якій базується дескриптор, не є стабільною, якщо деякі дрібниці пропускаються з одного відбитка на інший, навіть якщо вони з того самого пальця. Дійсно, через багато причин, особливо шум і умови отримання відбитків пальців; алгоритм вилучення дрібниць може видати помилкові дрібниці. Тобто він може додавати фіктивні дрібниці, яких спочатку не існує в еталонному відбитку, або, навпаки, пропускати справжні дрібниці, які спочатку існують у еталонному відбитку. Крім того, між двома відбитками може бути лише невелика ділянка, що перекривається, так що в обох випадках буде пропущено декілька деталей.

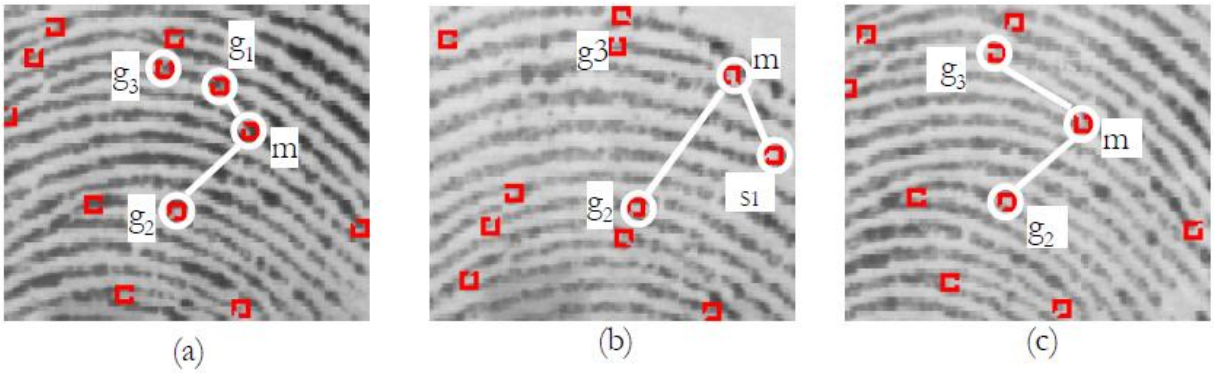

Рис.2.5 Вплив доданих/пропущених дрібниць на структуру дескриптора дрібниць на основі двох сусідів. (a), (b) і (c) є частковими відбитками того самого пальця з бази даних FVC2002 із позначеними деталями. (a) Еталонний дескриптор контрольних точок m, що складається з g1 і g2; (b) дескриптор «m» змінився, він складається з g2 і s1. Помилка пов’язана з помилковою точкою s1, яка замінила g1; (c) Контрольна точка g1 пропущена, дескриптор було змінено, щоб охопити цей час g2 і g3.

Рисунок 2.5 ілюструє вплив проблеми доданих/пропущених контрольних деталей на стабільність дескриптора контрольних деталей уздовж трьох часткових відбитків одного пальця. Наприклад, будь-які помилкові контрольні точки «s», додані поблизу центральної контрольної точки «m», можуть виключити справжню контрольну точку «g» із локальної структури завдяки відношенню «найближчий сусід» (Рис. 2.5-b). З іншого боку, будь-які пропущені справжні дрібниці поблизу m будуть замінені іншими дрібницями, які насправді не належать до структури «m» (Рис. 2.5-c). Таким чином, встановлений дескриптор, в обох випадках, базується на локальній структурі, відмінній від структури еталонного дескриптора, і його ненадійно зіставляти. Ця несумісність призводить до заохочення випадків хибного збігу та може призвести до деяких непослідовних пар деталей.

Проблема розміру простору пошуку. Більшість методів зіставлення дескрипторів, заснованих на локальних дрібницях, представляють високу складність зіставлення, що пов’язано головним чином з двох причин: і) задано

два шаблони друку T і запит Q, обидва з N дрібниць у середньому (зазвичай N становить від 30 до 60). Етап локального зіставлення має виконати вичерпну перевірку, щоб охопити всі дескриптори контрольних деталей, установлених у Q для кожної контрольної точки в T (тобто N2 порівнянь), щоб визначити набір найкращих відповідних пар контрольних деталей P, ii) через вплив помилкових контрольних деталей , етап локального зіставлення може доставляти хибно зіставлені пари або генерувати пари, які мають спільні деталі. Як наслідок, необхідний додатковий етап консолідації для уточнення локальних результатів і поширення їх на глобальний рівень. Цього можна досягти шляхом вирівнювання двох відбитків відповідно до кожної пари дрібниць у P. Нарешті, пара дрібниць, яка максимізує загальну оцінку, зберігається для створення остаточного списку парних дрібниць. Цей крок передбачає витрати часу, еквівалентні принаймні O(kN2), де k — розмір P.

Запропоновані рішення. Щоб вирішити ці проблеми, деякі автори розробляють свій дескриптор таким чином, щоб він був незалежним щодо будь-яких дрібниць, виявлених у відбитку пальця, використовуючи інформацію, що не є дрібницями. (Tico & Kuosmanen, 2003) використовували локальну інформацію про орієнтацію поля, отриману в наборі точок відбору проб навколо центральної точки, щоб побудувати свій дескриптор. Подібний підхід був запропонований (Feng, 2008; Qi & Wang, 2005) у поєднанні з дескриптором деталей. Оскільки вони не можуть нехтувати проблемою помилкових дрібниць, використовується жадібний алгоритм зіставлення з подальшим легким кроком консолідації. Остаточне глобальне вирівнювання досягається шляхом вирівнювання двох списків дрібниць відповідно до пари дрібниць, що максимізує функцію подібності під час локального етапу зіставлення. На жаль, це не завжди надійна пара деталей, яку можна вибрати. Інші роботи використовували обчислювальну геометрію для моделювання відбитків пальців як глобальних структур на основі дрібниць, які більш стійкі до проблеми помилкових дрібниць. (Deng & Huo, 2005) використовували

структуру тріангуляції Делоне для з’єднання деталей. Таким чином, будь-які додані/пропущені контрольні точки матимуть лише локальний обмежений вплив на околиці контрольних точок, які обмежені трикутниками Делоне. Маючи лише O(N) трикутників, N є кількістю деталей, простір пошуку надзвичайно скорочується. Також використовуються інші подібні геометричні структури, такі як вкладені опуклі багатокутники (Khazaei & Mohades, 2007). Цікавий метод був запропонований (Das, Karthik, & Chandra Garai, 2012), який здатний виявляти будь-які додані/пропущені дрібниці. Він спирається на структуру графіка мінімальної відстані (MDG), що походить від основної точки. Двофазний підхід досягається для пошуку збігу між парою MDG: спочатку три послідовні збігаються ребра повинні бути знайдені лише на основі їхніх відстаней. По-друге, решта обох графіків поділяються на два підграфи, які знову зіставляються разом. Автори повідомили про хороші результати. Проте цей метод має й недоліки: структура MDG менш стабільна для відповідності; будь-які помилкові дрібниці можуть мати глобальний вплив на графік, оскільки вони можуть відхилити його частковий або повний шлях (див. рис. 2.6).

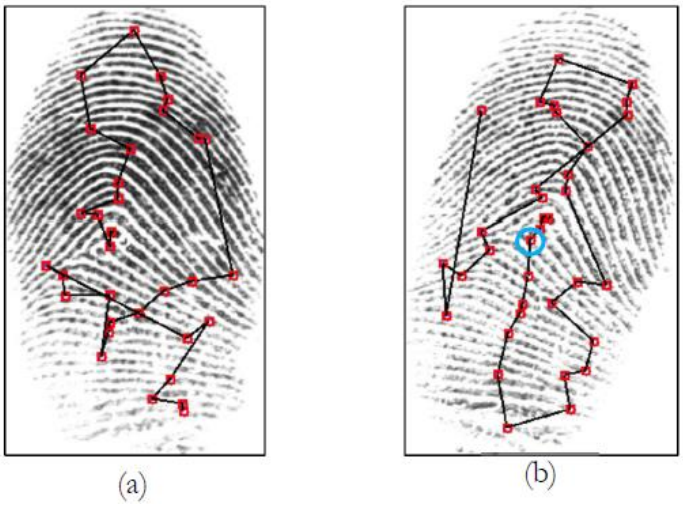

Рис. 2.6 Два відбитки одного пальця з відповідними MDGs. Поява дрібниць, обведених колом у (b), повністю змінила MDGb відповідно до MDGa. Дві MDGs помилково не збігаються

Усі попередні методи не атакують безпосередньо проблему помилкових дрібниць; вони скоріше намагаються зменшити його ефект, створюючи більш складні дескриптори та/або споживаючи більше часу.

Твердо переконані, що проблема полягає не в появі помилкових деталей, оскільки ми не можемо уникнути відсутності справжніх деталей і наявності фальшивих деталей, навіть якщо ми використовуємо ефективний алгоритм вилучення деталей, це скоріше полягає в класичному зіставленні схема, яку використовують більшість алгоритмів зіставлення на основі деталей. Ця схема базується на статичному дескрипторі дрібниць, який не допускає додавання або пропущення дрібниць. У цій роботі ми пропонуємо модифікувати класичну схему відповідності, яка базується на статичному дескрипторі, щоб мати справу з динамічним дрібницею-дескриптором, який може змінювати свої характеристики в міру просування процесу відповідності. Такий дескриптор більш гнучкий щодо доданих або пропущених деталей. Запропонований алгоритм зіставлення моделює просторовий розподіл дрібниць в обох відбитках пальців у вигляді форми, що називається формою полісегментів на основі дрібниць (MPS), що походить від основної точки. На основі нестатичного дескриптора схема відповідності досягається за допомогою свого роду алгоритму зіставлення шаблону форми між двома MPS. Він починається з припущення, що два MPS схожі, і намагається адаптивно синхронізувати одну форму відповідно до другої. Кожного разу, коли в MPS виявляється пропущена контрольна точка, запропонований алгоритм відповідності вводить нову віртуальну контрольну точку в другу, щоб реконструювати сумісні структури в обох відбитках і, таким чином, дозволити поширенню синхронізації. Наприкінці алгоритму обидва відбитки мають однакову просторову форму, що дозволяє нам обчислити оцінку відповідності. Запропонований підхід має дві переваги: він вводить поняття динамічного дескриптора та віртуальних дрібниць, а також представляє алгоритм зіставлення зі зниженим часом складності, який дорівнює O(n*logn).

Запропонований метод складається з трьох основних етапів: 1) виділення ознак дрібниць і виявлення основної точки, 2) побудова полісегментної структури дрібниць і 3) етап зіставлення, що дає оцінку відповідності. Подальші розділи надають більш детальну інформацію про цей процес.

2.3 Аналіз складності ідентифікації даних

Алгоритм зіставлення проходить два основних етапи. Перший етап — це етап побудови MPS, який включає алгоритм швидкого сортування, який виконується в O(N log(N)) для обох відбитків. Другий етап — це схема відповідності на основі MPS, яка порівнює кожен вузол у шаблоні MPS з відповідним вузлом, який має той самий індекс у запиті MPS. Однак це порівняння може включати процес вставки віртуальних дрібниць. У гіршому випадку, тобто у випадку пари відбитків самозванця, усі вузли шаблону MPS можуть бути вставлені в запит MPS і навпаки. Отже, кількість перевірених вузлів становить N+M. Таким чином, друга стадія проходить гірше за O(2N). Отже, складність, пов'язана з нашим алгоритмом відповідності, становить ~ O(N log(N)).

Таблиця 2.1 Складність запропонованого алгоритму з деякими відомими алгоритмами відповідності

Algorithm	Total complexity
(Tico & Kuosmanen, 2003)	$O(kN^2)$
(Das et al., 2012)	$O(N^2)$
(Jain, Hong, & Bolle, 1997)	$O(N^3)$
(Feng, 2008)	$O(N^2)$
Our algorithm	O(N log(N))

Запропонований алгоритм є дуже швидким порівняно з деякими відомими алгоритмами відповідності (див. Таблицю 2.1)

Таблиця 2.2 Показники ефективності запропонованого алгоритму

EER(%)	FMR100(%)	FMR1000(%)	ZeroFmr(%)
22,420	60,000	78,571	86,905

Для оцінки нашого алгоритму ми використали базу даних FVC2004 DB2-A (Maio, Maltoni, Cappelli, Wayman, & Jain, 2004), яка складається зі 100 пальців із 8 відбитками кожного, тобто загалом 800 відбитків. Зазначені в цьому конкурсі показники ефективності нашого алгоритму зведені в таблицю 2.2. Параметри, які використовуються для «th», дорівнюють (12, 12, π/6, π/6, π/8). Еволюція FMR і FNMR у функції порогового значення Thg проілюстрована на рисунку 2.7. Алгоритм добре працює у випадку хороших відбитків пальців, де основна точка добре розташована. Однак, якщо один відбиток пальця має погану якість або взагалі не містить основної точки, продуктивність значно знизиться.

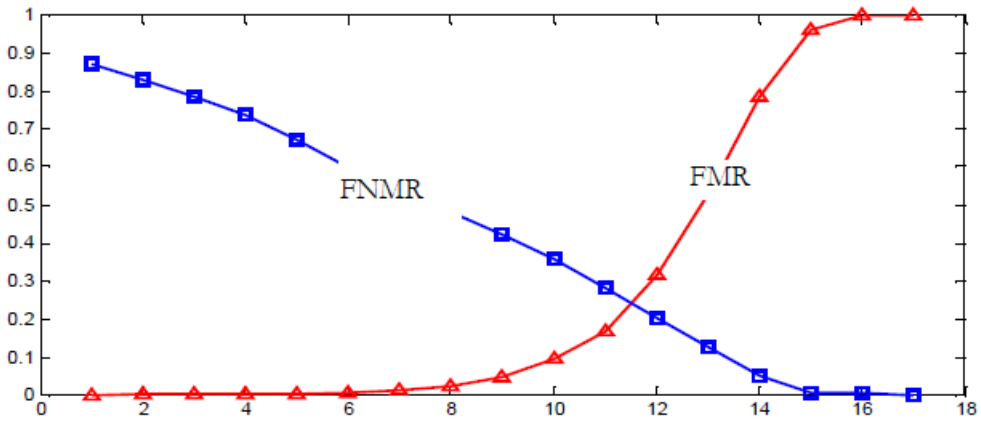

Рис. 2.7 Еволюція FMR і FNMR

2.4 Висновки до розділу 2

Біометричне розпізнавання за візерунком пальців є ефективним інструментом для ідентифікації особи за її унікальними фізичними характеристиками. Засоби оцінки цього виду технології грають важливу роль у забезпеченні точності та безпеки систем біометричного розпізнавання. Ось деякі висновки з оцінки біометричного розпізнавання відбитків пальців:

1. Точність ідентифікації: - Засоби біометричного розпізнавання відбитків пальців демонструють високу точність ідентифікації особи. - Великий обсяг унікальних патернів на пальцях робить цей метод надзвичайно ефективним.

2. Надійність: - Надійність біометричного розпізнавання відбитків пальців залежить від якості обладнання та алгоритмів обробки зображення. - Важливо враховувати фактори, такі як стан шкіри пальців (сухість, вологість), щоб забезпечити стабільність роботи системи в різних умовах.

3. Швидкість розпізнавання: - Досягнення високої швидкості обробки та порівняння великої кількості відбитків пальців є важливим аспектом ефективності системи.

4. Захист від обману: - Системи біометричного розпізнавання повинні бути стійкими до спроб обману, таких як використання фальшивих відбитків чи інших методів підробки.

5. Конфіденційність та захист даних: - Засоби оцінки повинні гарантувати конфіденційність особистої інформації та забезпечувати високий рівень захисту даних від несанкціонованого доступу.

6. Інтеграція та сумісність: - Важливо, щоб системи біометричного розпізнавання відбитків пальців були легко інтегровані з існуючими системами безпеки та іншими технологічними рішеннями.

Загалом, біометричне розпізнавання відбитків пальців є потужним інструментом для забезпечення безпеки та ідентифікації особи. Однак

ефективність цієї технології залежить від правильної імплементації, вдосконалення алгоритмів та постійного вдосконалення систем на основі засобів оцінки та відгуку користувачів.

3. АВТЕНТИФІКАЦІЯ НА ОСНОВІ ВІДБИТКІВ ПАЛЬЦІВ І СЛУЖБИ ДЛЯ МОБІЛЬНИХ СИСТЕМ НАВЧАННЯ

3.1 Мобільне навчання

Останні досягнення в мобільних технологіях збагатили мобільні пристрої все більшими можливостями. Сучасні смартфони характеризуються великими екранами, потужними графічними картами, процесорами високої обчислювальної потужності та різноманітними датчиками (Малюнок 3.1). З цього випливає, що відповідне використання мобільних пристроїв не обмежується голосовим спілкуванням та іграми; він поширюється на великий набір програм загального призначення, таких як геолокалізація, інтернет-магазини, доповнена реальність та освіта.

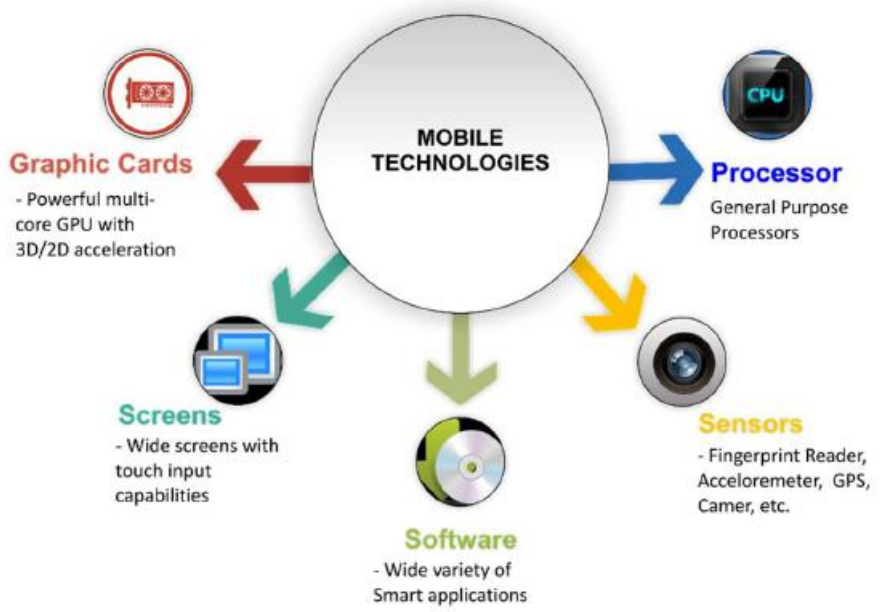

Рис. 3.1 Останні можливості мобільних технологій

Визначення Мобільне навчання – це адаптація освітніх ресурсів і послуг до контексту «поточних учнів» за допомогою «технологій навколишнього середовища». Насправді, докладається багато зусиль, щоб задовольнити

освітні цілі поточних користувачів, які, як відомо, дуже мобільні та зазвичай підключені до Інтернету через свої мобільні пристрої, у яких недостатньо або недостатньо часу, щоб допомогти в презентаційному класі, але мотивовані навчатися. Ця ситуація вимагає розробки нових стратегій для розробки та представлення курсів і супутніх матеріалів, які забезпечують кращі умови для навчання в будь-якому місці та в будь-який час.

Поточні проблеми безпеки. Фактичний прогрес у сфері мобільного навчання приділяє мало уваги деяким проблемам безпеки, які загрожують конфіденційності як учня, так і системи. (Kambourakis, 2013) чудово визначив вісім проблем, пов’язаних із безпекою та конфіденційністю систем мобільного навчання, серед яких ми наводимо найбільш критичні:

(1) безпека та конфіденційність системи та даних,

(2) конфіденційність учня,

(3) проблеми, пов’язані з мобільними пристроями та

(4) фільтрація вмісту.

Насправді учні повинні отримувати доступ до послуг і споживати навчальні ресурси за допомогою своїх мобільних пристроїв. Деякі з них можна зберігати на мобільному телефоні або ділитися з іншими. З точки зору системи, доступ до ресурсів має надаватися в будь-який час лише справжнім користувачам, які мають бути ефективно автентифікованими та контрольованими. З боку учня отриманий вміст не повинен бути шкідливим для учня. Серйозне занепокоєння викликало неправильне використання мобільних пристроїв у разі їх втрати або маніпуляцій з боку інших людей, крім власника. Тому навчальні заклади, педагоги та окремі учні можуть бути глибоко стурбовані зростаючими загрозами безпеці та конфіденційності даних (Kambourakis, 2013). Ще одне важливе питання, яке слід враховувати в таких системах, пов’язане з невідмовністю. Останнє вказує на те, наскільки учень і система впевнені у своїй ідентичності, один щодо одного, коли вони

передають інформацію, один як справжній передавач, а інший як справжній приймач.

Пов'язані роботи. Сучасні технології мобільного навчання, пов'язані з безпекою та конфіденційністю як навчальної системи, так і учня, значною мірою успадковані від контекстів електронного навчання та мережевого зв'язку (Kambourakis, 2013). Загалом він базується на класичних секретних методах (паролі, токени або PKI) (de Medeiros Gualberto & Zorzo, 2010; El-Khatib, Korba, Xu, & Yee, 2003; Ugray, 2009), які не дуже підходять.

Загальновідомо, що проблеми, які виникають у системах мобільного навчання, суттєво відрізняються від тих, які відомі в мобільному навчанні, оскільки застосування мобільних пристроїв може розкривати більше приватних даних і потребує набагато більше проблем (Udell & Woodill, 2014). Деякі інші, але, на жаль, небагато цікавих методів використовують той факт, що останні мобільні телефони мають охоплення кількома датчиками, які можна використовувати для безпечної ідентифікації користувачів за допомогою їхніх біометричних характеристик. У (Kambourakis & Damopoulos, 2013) автори вводять динамічну схему на основі підпису для забезпечення пост-автентифікації та неспростування в системах мобільного навчання. Автори повідомляють, що запропонована схема може правильно класифікувати підписи користувачів у кількості 95%. Робота (Адібі, 2010) обговорює збагачену мультимедіа інтерактивну систему невідмовності, залучену до середовища мобільного навчання для відстеження користувачів, які отримують доступ до навчальних матеріалів, і контролю особи відвідувачів іспиту. У (Kambourakis, Damopoulos, Papamartzivanos, & Pavlidakis, 2014) автори розкрили схему натискання клавіш на сенсорному екрані для ідентифікації користувачів. Повідомлений рівний коефіцієнт помилок (EER) у 12% свідчить про низьку точність ідентифікації. Той самий метод досліджувався в (Flior & Kowalski, 2010) для постійної ідентифікації користувачів під час онлайн-обстеження. (Alotaibi, 2010) запропонував схему

на основі відбитків пальців, щоб гарантувати, що жодна неавторизована особа не обманює здачу електронного іспиту. Інші комерційні рішення, такі як Apple TouchID і Samsung Galaxy, пропонують вбудований зчитувач відбитків пальців для реалізації безпечного мобільного розблокування на основі відбитків пальців. У поєднанні з операційною системою SDK це рішення також дозволяє ідентифікувати власника мобільного телефону в інтернет-магазинах і, таким чином, у мобільному навчанні. Біометричні рішення для безпеки та збереження конфіденційності в мобільному навчанні здаються більш перспективними. Однак біометричні дані вразливі. Як тільки біометрична система скомпрометована, біометричні ознаки остаточно втрачаються і не можуть бути відновлені. Як наслідок, користувача можна відстежувати всюди. У цій роботі ми пропонуємо використати останні досягнення в системі ідентифікації за відбитками пальців, щоб запропонувати стратегію безпечного спілкування в мобільних системах навчання. Запропонована схема пропонує як безпечну автентифікацію, так і послуги невідмовності. У наступному розділі представлені деякі біометричні поняття, які можна скасувати, зосереджуючись на відбитку пальця, після чого ми детально представляємо запропоновану нами схему.

3.2 Скасована біометрія

Біометрична автентифікація заснована на порівнянні вхідних біометричних даних із збереженим шаблоном функцій. Якщо останнє скомпрометовано, це може допомогти реконструювати підроблені біометричні дані для незаконного використання. Після зламу біометричні дані суб’єкта остаточно втрачаються та не можуть бути відновлені. Успіх системи автентифікації значною мірою залежить від безпеки збереженого шаблону.

Скасована біометрія означає методи, спрямовані на застосування деяких навмисних спотворень до оригінальних біометричних даних для захисту

збереженого шаблону (Maltoni, Maio, Jain, & Prabhakar, 2009). Після цього трансформований шаблон зберігається замість оригінальних. Формальніше кажучи, нехай *B* буде вихідним шаблоном, *F* — функцією перетворення, а *P* — вектором параметрів, що використовується для генерації трансформованого шаблону B_p.

$$B_p = F(B, P) \tag{3.1}$$

Функція перетворення F повинна відповідати трьом вимогам:

1- вона повинна зберігати прийнятну точність ідентифікації в трансформованому домені,

2- вона повинна бути необоротною, щоб гарантувати, що вихідний шаблон не можна відновити, тому F-1 не існує або він є обчислювально складно повернути його, і

3- він дозволяє повторно генерувати нові шаблони, якщо трансформований скомпрометовано. Цей новий згенерований шаблон не повинен збігатися ні з скомпрометованим, ні з вихідним шаблоном, щоб запобігти відстеженню користувачів.

Наприклад, зміна вектора параметрів P дозволяє системі відбитків пальців, яку можна скасувати, генерувати безліч несумісних трансформованих ознак відбитків пальців на основі одного оригінального відбитка пальця. Отже, користувачі можуть надавати різні функції відбитків пальців, просто змінюючи значення вектора параметрів, для кожної прикладної системи, яка їх стосується, щоб забезпечити незалежність безпеки між програмами. Було запропоновано багато алгоритмів для захисту шаблону відбитків пальців. (Ratha, Connell, & Bolle, 2001) були першими, хто ввів поняття скасованої біометрії. Вони окреслили основні слабкі ланки в автоматизованих біометричних системах і запропонували деякі рішення, які були розглянуті та

розроблені в (Ratha, Chikkerur, Connell, & Bolle, 2007). Там автори запропонували розладнати дрібниці у 2D-просторі, змінюючи їх позиції щодо розташування особливих точок, використовуючи три необоротні функції: декартову, полярну та функціональну складку поверхні. Автори підтвердили, що третя функція дає кращі результати, ніж інші. (Lee, Choi, Toh, Lee, & Kim, 2007) запропонували скасовувані шаблони відбитків пальців без вирівнювання на основі інформації про інваріантну орієнтацію дрібниць, отриману з їх орієнтації та локальних сусідніх областей. Отримана інваріантна інформація злегка переміщується за відстанню та орієнтацією за допомогою двох змінних функцій як ключа для перекладу та обертання для формування захищеного шаблону. (Ahmad, Hu, & Wang, 2011) модифікували версію полярної трансформації (Ratha et al., 2007), щоб вона не залежала від реєстрації на основі глобальних ознак (ядро-точка). Замість цього створюється полярна система координат на основі контрольних точок, на основі якої генерується локальний шаблон для кожної контрольної точки відносно інших. Потім шаблон обертається, перекладається та масштабується з використанням деяких параметрів як ключа для накладення перетворення «багато до одного». (Das, Karthik, & Chandra Garai, 2012) описав алгоритм хешування відбитків пальців без вирівнювання на основі графіків мінімальної відстані (MDG). Алгоритм захисту — це трансформація на основі дрібниць, принцип якої полягає в тому, щоб приховати розташування дрібниць і показати відстань між двома найближчими дрібницями. Хеш-граф генерується шляхом з'єднання кожної дрібниці з найближчою, починаючи з основної точки. Щоб зробити шаблон скасовуваним, вони застосували схему зміщення (Lee et al., 2007). (Belguechi, Cherrier, Rosenberger, & Ait-Aoudia, 2013a, 2013b) запропонували застосувати метод BioHashing, запропонований (Jin, Ling, & Goh, 2004), до добре відомого пальцевого коду в (Jain, Prabhakar, Hong, & Pankanti) , 2000) у поєднанні з локальним дескриптором деталей для створення захищеного шаблону. Ці алгоритми є вдосконаленими версіями запропонованих авторами

(Belguechi, Rosenberger Christopher, & Samy Ait-Aoudia, 2010). Автори повідомили про хорошу безпеку та відповідну точність. Щоб забезпечити більший захист у разі витоку ключа, отриманий захищений шаблон вбудовано в смарт-карту. Пропонується скасована система Match on Card (MoC). Примітною річчю в цій роботі є сувора система оцінювання, яку вони використовували для перевірки своєї схеми безпеки. (Moujahdi, Bebis, Ghouzali, & Rziza, 2014) запропонували структуру представлення на основі дрібниць, яка називається оболонкою відбитків пальців, для створення їх захищеного шаблону. По-перше, контрольні точки впорядковуються відповідно до їх відстані до кожної окремої точки. Випадкове значення додається до списку відстаней для формування спеціального ключа користувача. Відстані використовуються для побудови кількох суміжних прямокутних трикутників. (Prasad & Santhosh Kumar, 2014) створили захищений шаблон шляхом побудови M прямокутників з різними орієнтаціями навколо кожної дрібниці та обчислення інваріантних локальних зв’язків. Потім генерується бітовий рядок фіксованої довжини, який перетворюється на комплексний вектор шляхом застосування DFT. Щоб зробити шаблон скасовуваним, отриманий вектор перетворюється за допомогою ключа конкретного користувача.

3.3 Схема автентифікації на основі відбитків пальців для мобільного навчання

Оскільки сучасні смартфони оснащені вбудованим зчитувачем відбитків пальців, запропонований метод використовує модальність відбитків пальців для безпечного спілкування під час мобільного навчання. Інші модальності, такі як голос або обличчя, також можна використовувати в цьому методі. Ми пропонуємо надати системі навчання орган автентифікації (AA), який відповідає за автентифікацію учнів на основі їх відбитків пальців, коли вони

запитують доступ до системи. Оскільки користувачі не обов'язково довіряють AA, їхні ідентифікаційні дані не можна використовувати в простій формі як дані автентифікації. AA реалізує алгоритм відбитків пальців, який можна скасувати, описаний (Ratha та ін., 2007), щоб захистити шаблон на основі дрібниць. Він пропонує змінити положення деталей за допомогою матриці перетворення один до багатьох, щоб отримати новий трансформований шаблон. Усі трансформовані ідентифікаційні дані учнів на основі відбитків пальців зберігаються в базі даних. Таким чином, навіть якщо база даних скомпрометована, оригінальний шаблон відбитка пальця не може бути розкритий. Запропонована схема проходить через усі етапи процесу навчання: (i) підписка (ii) доступ до ресурсів і (iii) процес оцінювання (Рисунок 3.2).

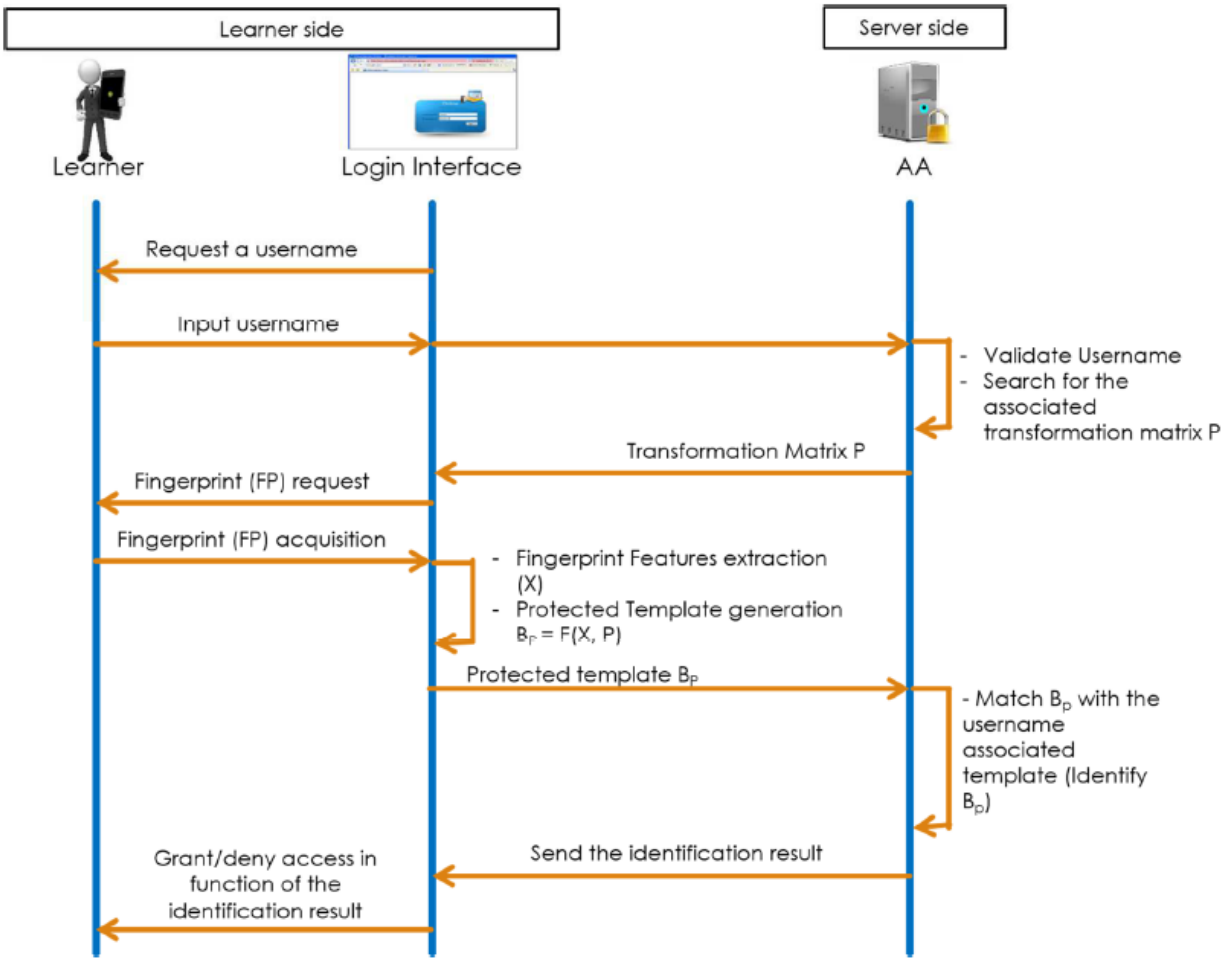

Рис. 3.2 Процес підписки

Підписка. Учень зобов'язаний підписатися, щоб отримати авторизацію для доступу до ресурсів. Етап підписки дозволяє АА дізнатися особу учня. Інтерфейс підписки (SI) просить користувача ввести ім’я користувача, яке буде надіслано в АА для перевірки. АА генерує випадковим чином матрицю перетворення P, пов’язану з отриманим іменем користувача, і надсилає її назад до SI. SI просить користувача ввести свій відбиток пальця. Цей останній отримується та обробляється локально, після чого перетворюється за допомогою отриманої матриці P. Отриманий трансформований шаблон Bp надсилається до АА за допомогою безпечного алгоритму шифрування, такого як RSA або алгоритм Blowfish. АА при отриманні шаблону Bp пов’язує його з обліковим записом користувача та підтверджує отримання шаблону.

Варто зазначити, що цю операцію потрібно виконувати на стороні клієнта, щоб забезпечити безпеку отриманого відбитка пальця. Крім того, весь зв’язок має бути захищений за допомогою надійного алгоритму шифрування. Така ж схема дотримується, коли користувач хоче створити новий шаблон ідентифікатора Hp1. Це означає, що інтерфейс підписки дозволяє користувачеві повторно створити новий захищений шаблон за умови, що він уже автентифікований за допомогою старого шаблону Bp, як зазначено в наступному підрозділі. Процес підписки показано на рисунку 3.2.

Доступ до ресурсів. На цьому кроці учень має отримати доступ до навчальних ресурсів. Учень має бути автентифікований як справжній користувач. Інтерфейс входу (LiI) просить користувача ввести своє ім’я користувача, яке буде надіслано до АА. Це останнє підтверджує існування отриманого імені користувача та витягує пов’язану матрицю перетворення P, яка буде надіслана LiI. Останній запитує користувача ввести свій відбиток пальця, який буде перетворено в захищений трансформований шаблон за допомогою того самого алгоритму, що й на кроці підписки, застосованому до отриманого параметра P.

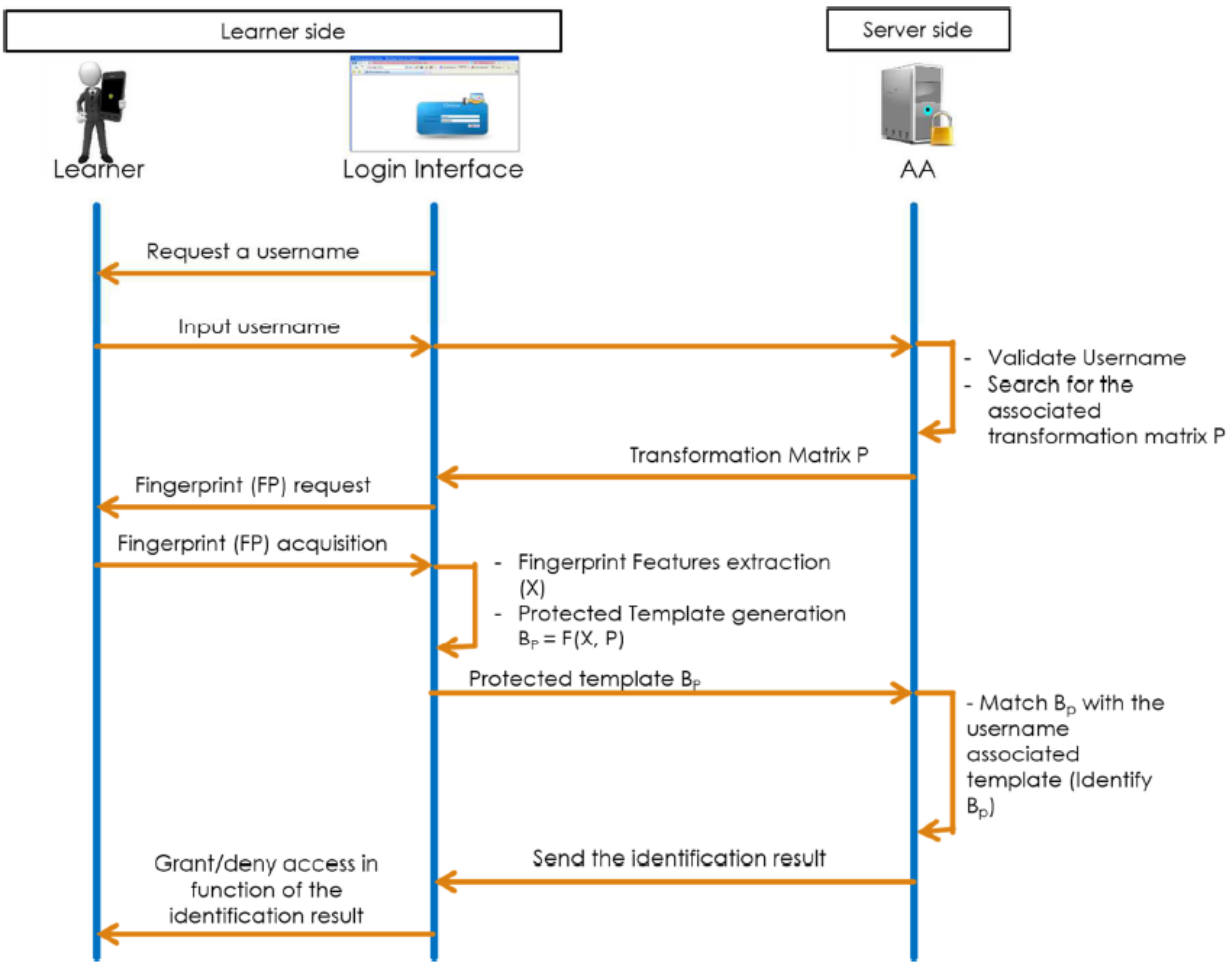

Рис. 3.3 Процес автентифікації

Отриманий шаблон Bp буде надіслано до AA. При отриманні AA ідентифікує користувача в базі даних шляхом запуску процесу відповідності між Bp як шаблоном запиту та збереженим шаблоном, пов’язаним з користувачем. Користувачеві надається доступ за результатами ідентифікації. Процес доступу до ресурсів показано на рисунку 3.3.

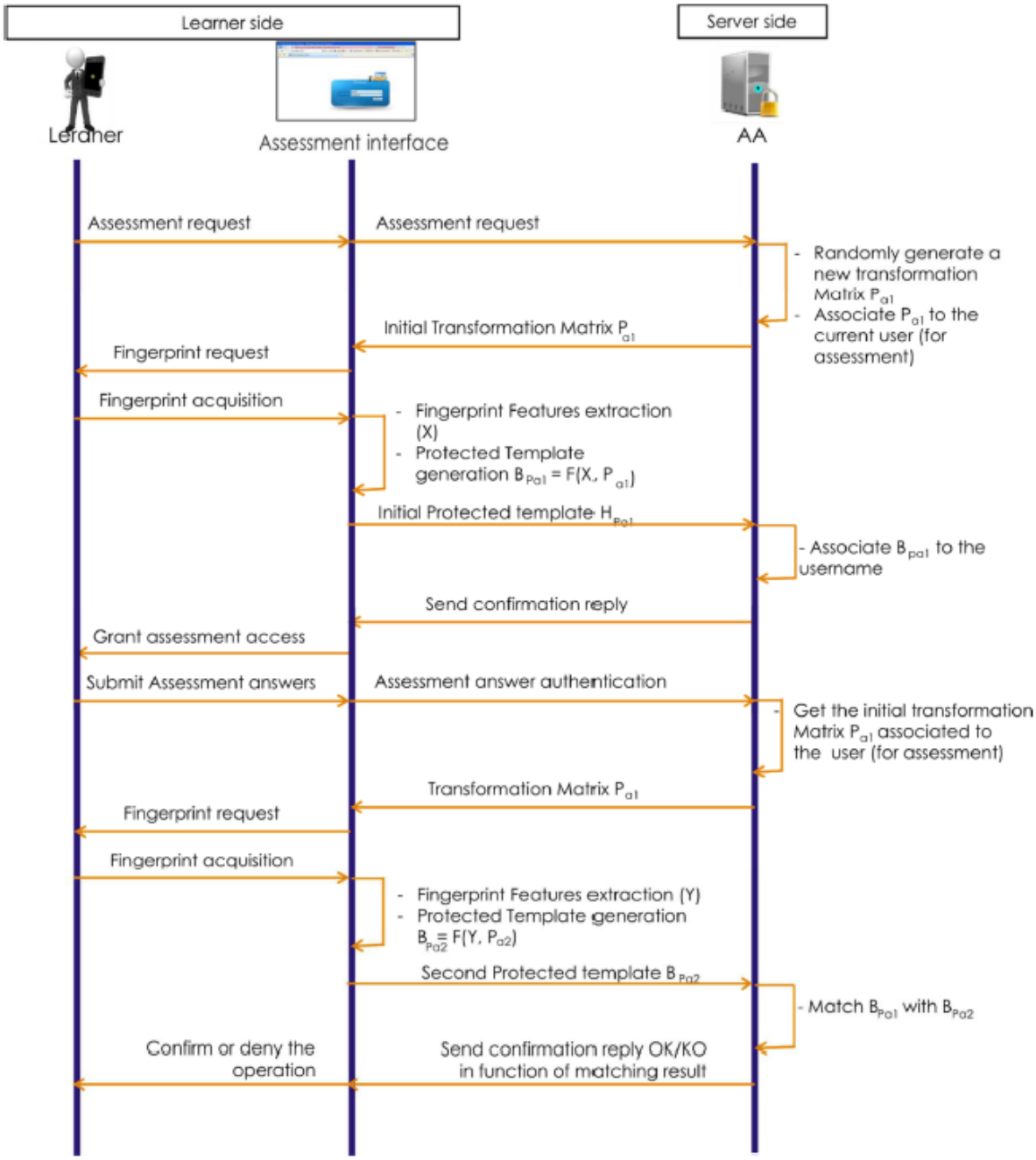

Рис. 3.4 Процес оцінювання

Процес оцінювання потребує послуги неспростування, яка гарантує, що відповіді на оцінювання є тим самим учнем, який уже пройшов автентифікацію для виконання процесу оцінювання. Крім того, система навчання не може відмовити користувачеві в поданні своїх оціночних відповідей. Процес неспростування показано на рисунку 3.4. Коли ви запитуєте оцінювання, учень повинен спочатку увійти в систему, як описано в

попередньому підрозділі. Після входу в систему учень запитує вправу, інтерфейс оцінювання (AI) надсилає ім’я користувача до AA. Останній випадковим чином генерує нову тимчасову матрицю перетворення Pa1, пов’язує її з іменем користувача та надсилає назад до ШІ. AI просить користувача про повторну автентифікацію та генерує новий захищений шаблон Bpa1, використовуючи той самий алгоритм скасування відбитків пальців, застосований до матриці Pa1, який буде надіслано до AA. Цей останній зберігає Bpa1, пов’язаний з його іменем користувача. Надсилаючи відповіді для оцінювання, учень, який увійшов у систему, має надати трансформований шаблон, який відповідає Bpa1, щоб завершити процес подання. Це гарантує, що особа, яка спочатку запитала оцінку, є тією самою особою, яка подає відповіді. При отриманні оціночних відповідей система відповідає повідомленням підтвердження. Вищеописаний процес можна повторити для кожної вправи, що становить оцінку.

3.4 Висновок до розділу 3

Обґрунтували схему на основі відбитків пальців, щоб забезпечити вирішення деяких проблем безпеки та конфіденційності в системах мобільного навчання, використовуючи останні досягнення в системах відбитків пальців, які можна скасувати. Запропонована схема забезпечує безпеку всього навчального процесу, зокрема під час підписки, доступу до ресурсів та процесу оцінювання. Пропонуються безпечні послуги автентифікації та невідновності. Система може бути вдосконалена для застосування в реальному мобільному навчанні на основі онлайн-лабораторій. Однією з основних переваг запропонованої схеми є те, що її можна розглядати як загальну структуру для захисту віддалених ресурсів.

З урахуванням цих переваг, важливо також врахувати можливі виклики, такі як технічні обмеження, можливість фальшивого визначення та

конфіденційність даних. Додаткові вивчення та тестування будуть необхідні для впровадження цієї схеми в реальних умовах мобільного навчання.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИУАЦІЯХ

4.1 Облаштування і безпека серверних приміщень

Використання хмарних веб-сервісів на сьогоднішній день несе в собі як позитивні, так і негативні моменти. З одного боку, використання хмарних сервісів здатне надати неабияку кількість обчислювальних ресурсів для компанії, а з іншого змушує облаштувати серверне приміщення. Для продуктивної і безпечної роботи серверних приміщень існує ряд вимог, також, це стосується і операторів які працюють на цьому робочому місці.

Приміщення, де розміщені робочі місця операторів, потрібно оснастити вогнегасниками. Виняток становлять ті, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер). Приміщення, де розміщені робочі місця операторів сервера загального призначення, варто обладнати системою автоматичної пожежної сигналізації та засобами пожежогасіння (пп. 1.15, 1.16 п. 1 розд. III Правил № 65).

Щоб запобігти витоку інформації у серверних приміщеннях через побічні випромінювання і наводи, а також порушенню її цілісності через вплив зовнішніх електромагнітних полів, слід використовувати екрановані шафи, сейфи (клас опору до злому не нижче II), кабіни. Можна використовувати екрановані шафи (сейфи) для розміщення серверів баз даних, прикладних задач тощо. Екрановані шафи (сейфи) повинні мати сертифікат відповідності, виданий Державною службою спеціального зв’язку та захисту інформації України.

Серверні приміщення рекомендовано обладнати у приміщеннях без вікон. Це не поширюється на старі приміщення, які реконструюють, та на неекрановані приміщення, у яких установлені екрановані шафи (сейфи). Щоб запобігти несанкціонованому доступу до серверних приміщень, обладнайте їх

двері автоматизованою системою доступу або кодовим замком. А також не менше ніж двома рубежами охоронної сигналізації, кожний із яких підключений окремими кодами до приймально-контрольних приладів, установлених на посту охорони банку та/або охорони банку.

Серверні приміщення слід обладнати системою оповіщення під час пожежі та автоматичною системою газового пожежогасіння. Внутрішні поверхні цих приміщень облицюйте пожежобезпечними матеріалами, що відповідають санітарно-гігієнічним вимогам. Через повітропроводи системи вентиляції та канали для введення кабелів і комунікацій до серверних приміщень можуть проникнути сторонні речовини, щоб цього не допустити, обладнайте їх вогнетривкими пробками чи вогнетривкими аварійними заслінками. Також обладнайте централізованою або окремими системами припливно-витяжної вентиляції та автоматичного кондиціювання повітря з очищенням від пилу. Вони мають забезпечувати у приміщенні температуру повітря 18-24 ºС і відносну вологість не більше ніж 60% у будь-яку пору року.

Серверні приміщення та приміщення електронних архівів розміщуйте у віддалених один від одного кінцях будівлі. Якщо є змога, ці приміщення розміщуйте у внутрішній частині будівлі або з боку внутрішнього двору.

У кожному серверному приміщенні забезпечте ведення журналу на паперових носіях. У ньому зазначають:

- дату та час відчинення і зачинення кімнати;
- прізвища працівників, які відвідували кімнату;
- опис проведених робіт.

Фахівці, що забезпечують технічне обслуговування електротехнічних пристроїв серверного приміщення, є електротехнічним персоналом. Вони повинні мати ІІІ кваліфікаційну групу з електробезпеки. Присвоювати кваліфікаційну групу з електробезпеки особам, які працюють тільки з програмним забезпеченням, немає потреби. Адже ці особи є звичайними користувачами комп’ютерної техніки.

На підприємстві, де експлуатують електронно-обчислювальну техніку, мають розробляти інструкцію з охорони праці (відповідно до Положення про розробку інструкцій з охорони праці, затвердженого наказом Держнаглядохоронпраці від 29.01.1998 № 9; НПАОП 0.00-4.15-98; п. 1.8 розд. І Правил № 65). Постає запитання: чи мають розробляти на підприємстві інструкцію з охорони праці для оператора (користувача) комп'ютерної техніки?

Відповісти однозначно не можна. Є відомчі інструкції, пов'язані з використанням ЕОМ на виробництві: наприклад, була Інструкція щодо користування персональним комп'ютером (затверджена наказом Державної судової адміністрації України від 10.01.2004 № 1/04) та чинна Примірна інструкція з охорони праці під час експлуатації електронно-обчислювальних машин (затверджена наказом Міністерства доходів і зборів України від 05.09.2013 № 443).

ДСТУ не передбачають наявність для користувача комп'ютера інструкції з охорони праці під час роботи з ЕОМ. Вони передбачають інструкцію з експлуатування (користування) цією технікою.

Користувачі ЕОМ мають використовувати інструкцію з експлуатування, а для апаратури з під'єднанням з'єднувачем та призначеної для встановлення користувачем – інструкцію із встановлення (монтажу; п. 1.7.2 ДСТУ 4467-1:2005). Інструкція з охорони праці під час роботи з комп'ютером (комп'ютерною технікою) може бути як однією з інструкцій за видом робіт, якої має дотримуватися обслуговуючий персонал (обслуга) (прим. 3 до п. 1.7.2 ДСТУ 4467-1:2005).

Отже, інструкція з охорони праці для комп'ютерної техніки недоцільна з таких міркувань:

1. Сучасна ЕОМ є електротехнічним пристроєм загального призначення. Під час експлуатації ЕОМ найважливішим є питання електробезпеки. Тому інструкцією з охорони праці (поряд із інструкцією з пожежної безпеки та

інструкцією з надання домедичної допомоги) має бути інструкція з електробезпеки. До неї варто включити вимоги електробезпеки під час експлуатації ЕОМ.

2. Робота на ЕОМ загального призначення не є роботою з підвищеною небезпекою. Програмне забезпечення не стосується теми охорони праці. Немає потреби визначати в інструкції з охорони праці вимоги щодо улаштування робочого місця користувача ЕОМ. Адже організувати робоче місце користувача ЕОМ зобов'язаний роботодавець. Він має інформувати працівника про умови праці, небезпечні і шкідливі виробничі фактори на його робочому місці, які ще не усунуто, можливі наслідки їх впливу на здоров'я та про права працівника на пільги і компенсації за роботу в таких умовах. Також роботодавець має провести відповідний інструктаж та навчання з питань охорони праці.

4.2 Пожежна безпека в навчальних закладах

Відповідно до Правил пожежної безпеки України, затверджених постановою Міністерства освіти і науки від 15.08, та правил пожежної безпеки навчальних закладів України забезпечується пожежна безпека організацій і підприємств системи освіти України. 2016 № 974, зареєстрований в Міністерстві юстиції України 8 вересня 2016 року за номером 1229/29359.

Забезпечення пожежної безпеки в організаціях, на підприємствах системи освіти України здійснюється згідно з Відповідно з Правилами пожежної безпеки в Україні та Правилами пожежної безпеки для навчальних закладів та установ системи освіти України, затверджених наказом Міністерства освіти і науки України 15.08.2016 № 974, зареєстрованих в Міністерстві юстиції України 08.09.2016 за № 1229/29359, відбувається забезпечення пожежної безпеки в організаціях.

Основним завданням пожежної безпеки в навчальних закладах є захист і порятунок персоналу (дітей) від небезпечних пожежних факторів, які супроводжуються неконтрольованим горінням. При виникненні пожежі дії працівників, залучених до гасіння пожежі, повинні бути спрямовані на забезпечення безпеки особового складу, особливо дітей, а також їх евакуацію та рятування.

Усі заклади та установи перед початком навчального року мають бути затверджені відповідною комісією, у тому числі представниками органів державного нагляду у сфері пожежної безпеки.

Діти у будинках дитячих дошкільних закладів повинні розміщуватися з таким розрахунком, щоб молодші розташовувалися на нижчих поверхах.

У багатоповерхових навчальних корпусах та школах-інтернатах класи повинні розміщуватися на нижніх поверхах. У кімнатах з дітьми підлога повинна бути прикріплена до кріплення (за винятком дитячих садків), мати помірну здатність до димоутворення. У дитячих закладах, які працюють цілодобово, літні дитячі дачі повинні бути оснащені чергуванням персоналу нічної служби. Зал очікування повинен забезпечувати телефонний зв’язок. Черговий повинен забезпечити: особовий склад на пожежі засобами індивідуального захисту органів дихання, комплектом ключів від евакуаційних дверей, переносним ліхтарем, а також знати кількість дітей, які ночують, їх місцезнаходження та зателефонувати до найближчого пожежно-рятувальної частини для передачі інформації.

У загальноосвітніх навчальних закладах (крім закладів для дітей з розумовими і фізичними вадами) можуть створюватися дружини молодих пожежників-рятувальників. У закладах та установах, де учні/першокласники проживають цілодобово, необхідно встановити обов’язки персоналу нічної служби, яка не має права спати під час зміни. Зал очікування повинен забезпечуватися телефонним зв’язком. Черговий персонал повинен окремо оснастити фільтруючими пристроями усіх дітей та обслуговуючий персонал

на випадок пожежі, комплектом ключів від евакуаційних виходів і воріт, а також автомобільних під'їздів і установ для в'їзду на територію установи. Не допускається в будівлях установ і в місцях:

- розміщувати людей на горищі та на поверсі (будівлі), не передбачаючи двох евакуаційних виходів;
- перепланувати ділянку без урахування будівельних норм і правил;
- установлювати ґрати та пристрої на вікнах приміщень де перебувають учасники навчально-виховного процесу, а саме: сходових клітках, у коридорах, холах та вестибюлях Якщо ґрати все таки встановлені (кабінет інформатики, інші приміщення з обладнанням, що має матеріальну цінність), вони повинні розсуватися, зніматися або розкриватися, під час перебування в цих приміщеннях вони мають бути відчиненими;
- знімати дверні полотна в отворах, що з'єднують коридори зі сходовими клітками, та двері евакуаційних виходів;
- використовувати для опалення нестандартні (саморобні) нагрівальні пристрої;
- користування прилади для приготування їжі, крім спеціально обладнаних приміщень;
- захаращувати шляхи евакуації;
- встановлення дзеркал та встановлення фальш-дверей на шлях евакуації;
- встановлювати перешкоди на шляху евакуації; пороги, виступи, поворотні двері, розсувні двері, підйомні двері та інші пристрої для евакуації;
- при наявності людей у будівлі проводити електрозварювання та інші види пожежонебезпечних робіт;
- використовувати для освітлення свічки та гасові лампи та ліхтарі;
- використовувати відкритий вогонь для нагрівання труб систем опалення, водопостачання, каналізації тощо (для цього використовується гаряча вода, пару або гарячий пісок);

- зберігати використані обтиральні матеріали на робочому місці, в шафах, зберігати їх у кишенях робочого одягу;
- підключати до джерела живлення електроприлади без нагляду.

При належному виконанні всіх вимог ризик пожежі набагато зменшується. Навіть в випадку виникнення пожежі виконання вимог дозволяє набагато легше проводити евакуацію та мінімізувати наслідки пожежі.

ВИСНОВКИ

У розділі 1: Дослідження та аналіз проблематики біометричної ідентифікації даних. Ми систематично вивчили та розглянули проблеми, пов'язані з біометричною ідентифікацією даних. Визначено, що точність, швидкість та надійність є ключовими аспектами вдосконалення біометричних систем. Наш аналіз також охопив етичні та конфіденційнісні питання, пов'язані зі збором та обробкою біометричних даних.

У Розділі 2: Засоби оцінки біометричного розпізнавання індивідуальних особливостей візерунка пальців. Були досліджені та розглянуті різні методи та засоби для оцінки біометричного розпізнавання відбитків пальців. Особливу увагу приділено технічним аспектам, таким як алгоритми обробки зображення та моделі порівняння. Висвітлено важливі параметри, що впливають на надійність та ефективність систем.

У Розділі 3: Автентифікація на основі відбитків пальців і служби для мобільних систем навчання. Ми досліджували можливості використання автентифікації на основі відбитків пальців у мобільних системах навчання. Показано, що це може покращити безпеку під час навчання, забезпечуючи доступ лише автентифікованим користувачам. Розглянуті служби для обробки та отримання нових інформативних ознак для поліпшення біометричної ідентифікації.

Дипломна робота висвітлює ключові аспекти біометричної ідентифікації в мобільних системах навчання. За допомогою досліджень та аналізу проблематики, ми визначили, як важливо поліпшити точність та надійність систем біометричного розпізнавання. Засоби оцінки та методи автентифікації на основі відбитків пальців є ефективними засобами для досягнення цієї мети, забезпечуючи високий рівень безпеки та конфіденційності у сфері мобільного навчання. Пропонується подальше розширення та вдосконалення цих підходів для максимальної ефективності та зручності використання в реальних умовах.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Adibi, S. A remote interactive non-repudiation multimedia-based m-learning system. Telematics and Informatics, 27(4), (2010), 377–393.

2. Ahmad, T., Hu, J., & Wang, S. Pair-polar coordinate-based cancelable fingerprint templates. Pattern Recognition, 44(10-11), (2011), 2555–2564. http://doi.org/10.1016/j.patcog.2011.03.015

3. Alonso-Fernandez, F., Fierrez, J., & Ortega-Garcia, J. An enhanced gabor filter-based segmentation algorithm for fingerprint recognition systems. In Proc. IEEE Intl. Symposium on Image and Signal Processing and Analysis, ISPA, Spec. Sess on. Signal Image Processing for Biometrics, IEEE Press, Zagreb (Croatia), September 2005 (pp. 239–244).

4. Alotaibi, S. Using biometrics authentication via fingerprint recognition in e-exams in e-learning environment. The 4th Saudi International Conference,. Baruch, O. (1988). Line thinning by line following. Pattern Recognition Letters, 8(4), (2010), 271–276.

5. Bazen, A. M., & Gerez, S. H. Segmentation of fingerprint images. In Proc. Workshop on Circuits Systems and Signal Processing (ProRISC 2001) (Vol. 276280).

6. Bazen, A. M., & Gerez, S. H. Systematic methods for the computation of the directional fields and singular points of fingerprints. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 24(7), (2002), 905–919.

7. Belguechi, R., Cherrier, E., Rosenberger, C., & Ait-Aoudia, S. An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates. Computers and Security, 39(PART B), (2013), 325–339. http://doi.org/10.1016/j.cose.2013.08.009

8. Belguechi, R., Cherrier, E., Rosenberger, C., & Ait-Aoudia, S. (2013). Operational bio-hash to preserve privacy of fingerprint minutiae templates. IET Biometrics, 2(2), (2013), 76–84.

9. Belguechi, R., Rosenberger Christopher, & Samy Ait-Aoudia. Biohashing for Securing Minutiae Template. In Pattern Recognition (ICPR), 2010 20th International Conference on (2010), (pp. 1168–1171). http://doi.org/10.1109/ICPR.2010.292

10. Belhadj, F., Ait-Aoudia, S., & Akrouf, S. Secure Fingerprint-based authentication and non-repudiation services for mobile learning systems. In Interactive Mobile Communication Technologies and Learning (IMCL), 2015 International Conference on (pp. 200–204). http://doi.org/10.1109/IMCTL.2015.7359586

11. Belhadj, F., Akrouf, S., Harous, S., & Ait-Aoudia, S. (2015). Efficient fingerprint singular points detection algorithm using orientation-deviation features. Journal of Electronic Imaging, 24(3), (2015), 033016. http://doi.org/10.1117/1.JEI.24.3.033016

12. Bengueddoudj, A., Akrouf, S., Belhadj, F., & Nada, D. Improving fingerprint minutiae matching using local and global structures. In 8th International Workshop on Systems, Signal Processing and Their Applications, WoSSPA 2013 (pp. 279–282). http://doi.org/10.1109/WoSSPA.2013.6602376

13. Bolle, R. M., Senior, A. W., Ratha, N. K., & Pankanti, S.. Fingerprint minutiae: A constructive definition. In Biometric Authentication (2002), (pp. 58–66). Springer.

14. Cappelli, R., Ferrara, M., Franco, A., & Maltoni, D.. Fingerprint verification competition 2006. Biometric Technology Today, 15(7), (2007), 7–9.

15. Cappelli, R., Ferrara, M., & Maltoni, D. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 32(12), (2010), 2128–2141.

16. Cappelli, R., Lumini, A., Maio, D., & Maltoni, D. Fingerprint classification by directional image partitioning. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 21(5), (1999), 402–421.

17. Cappelli, R., Lumini, A., Maio, D., & Maltoni, D. Fingerprint Image Reconstruction from Standard Templates. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(9), (2007), 1489–1503. http://doi.org/10.1109/TPAMI.2007.1087

18. Cavusouglu, A., & Görgünouglu, S. A fast fingerprint image enhancement algorithm using a parabolic mask. Computers & Electrical Engineering, 34(3), (2008), 250–256.

19. Chen, J., & Moon, Y.-S. A minutiae-based fingerprint individuality model. In Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on (pp. 1–7).

20. Chen, J., & Moon, Y.-S. The statistical modelling of fingerprint minutiae distribution with implications for fingerprint individuality studies. In Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on (pp. 1–7). http://doi.org/10.1109/CVPR.2008.4587399

21. Chen, Y., & Jain, A. Beyond Minutiae: A Fingerprint Individuality Model with Pattern, Ridge and Pore Features. In M. Tistarelli & M. Nixon (Eds.), Advances in Biometrics SE – 54, (2009), (Vol. 5558, pp. 523–533). Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-01793-3_54

22. Chikkerur, S., Cartwright, A. N., & Govindaraju, V. Fingerprint enhancement using STFT analysis. Pattern Recognition, 40(1), (2007), 198–211.

23. Chikkerur, S., Govindaraju, V., Pankanti, S., Bolle, R., & Ratha, N. Novel approaches for minutiae verification in fingerprint images. In Application of Computer Vision, 2005. WACV/MOTIONS'05 Volume 1. Seventh IEEE Workshops on (Vol. 1, pp. 111–116).

24. Chikkerur, S., & Ratha, N. Impact of singular point detection on fingerprint matching performance. In Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on (pp. 207–212).

25. Chua, S. C., Wong, E. K., & Tan, A. W. C. Fingerprint Ridge Distance Estimation: A Mathematical Modeling. International Journal of Computer Applications, 2015, 126(15).

26. Das, D., & Mukhopadhyay, S. A Pixel Based Segmentation Scheme for Fingerprint Images. In Information Systems Design and Intelligent Applications, 2015, (pp. 439–448).

27. Springer. Das, P., Karthik, K., & Chandra Garai, B. A Robust Alignment-free Fingerprint Hashing Algorithm Based on Minimum Distance Graphs. Pattern Recogn., 45(9), (2012), 3373–3388. http://doi.org/10.1016/j.patcog.2012.02.022

28. Dass, S. Individuality of Fingerprints: A Review. In S. Z. Li & A. K. Jain (Eds.), Encyclopedia of Biometrics SE - 58-2, 2014, (pp. 741–751). Springer US. http://doi.org/10.1007/978-3-642-27733-7_58-2

29. Dass, S. C. Markov random field models for directional field and singularity extraction in fingerprint images. Image Processing, IEEE Transactions on, 13(10), 2004, 1358–1367.

30. de Medeiros Gualberto, T., & Zorzo, S. D. Service for secure and protected applications in Collaborative Learning Environments. In Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on, (pp. 2419–2426).

31. Deng, H., & Huo, Q. Minutiae matching based fingerprint verification using delaunay triangulation and aligned-edge-guided triangle matching. In Audio- and Video-Based Biometric Person Authentication, 2005, (pp. 270–278).

32. Ferreira, P. M., Sequeira, A. F., & Rebelo, A. A Fuzzy C-Means Algorithm for Fingerprint Segmentation. In Pattern Recognition and Image Analysis, (2015), (pp. 245–252). Springer.

33. FitzGerald, E., Ferguson, R., Adams, A., Gaved, M., Mor, Y., & Thomas, R. Augmented reality and mobile learning: the state of the art. International Journal of Mobile and Blended Learning, 5(4), (2013), 43–58.

34. Flior, E., & Kowalski, K. Continuous biometric user authentication in online examinations. In Information Technology: New Generations (ITNG), 2010 Seventh International Conference on (pp. 488–492).

35. Golabi, S., Saadat, S., Helfroush, M. S., & Tashk, A. A novel thinning algorithm with fingerprint minutiae extraction capability. International Journal of Computer Theory and Engineering, 4(4), (2012), 514–517.

36. Gonzalez, R. C. Digital image processing. Pearson Education India. Gottschlich, C. (2012). Curved-region-based ridge frequency estimation and curved Gabor filters for fingerprint image enhancement. Image Processing, IEEE Transactions on, 21(4), 2220–2227.

37. Gottschlich, C., & Schoonlieb, C.-B. Oriented diffusion filtering for enhancing low-quality fingerprint images. Biometrics, IET, 1(2), (2012), 105–113. http://doi.org/10.1049/iet-bmt.2012.0003

38. Nykytyuk V., Dozorskyi V., Dozorska O. Detection of biomedical signals disruption using a sliding window. Scientific jornal of the Ternopil National Technical University. 2018. № 3 (91). P. 125–133.

39. Vasyl Dozosky, Oksana Dozorska, Vyacheslav Nykytyuk, EvheniaYavorska, Leonid Dediv. The Method of Selection and Pre-processing of ElectromyographicSignals for Bio-controlled Prosthetic of Hand. 2020 IEEE 15th International Scientific and Technical Conference onComputer Sciences and Information Technologies (CSIT). Volume 1, Lviv-Zbarazh, Ukraine 23-26 September 2020. P. 188-191) Electronic ISBN:978-1-7281-7443-3, USB ISBN:978-1-7281-7442-6, Print on Demand (PoD) ISBN:978-1-7281-7444-0. Print ISSN: 2766-3655, Online ISSN: 2766-3639. DOI: 10.1109/CSIT49958. 2020.9321935.

40. Vyacheslav Nykytyuk, Vasyl Dozorskyy, Nataliia Kunanets, Volodymyr Pasichnyk, Oleksandr Matsiuk, Ihor Bodnarchuk: Electrical Probe-Signal Processing and Criterion for the Determination of Time Parameters of the Teeth Filling Material Polymerization Process in Dentistry. 4th IDDM 2021: Valencia, Spain. P. 54-63

41. Oleksii Duda, Nataliia Kunanets, Serhii Martsenko, Vyacheslav Nykytyuk, Volodymyr Pasichnyk. Information technology platform for the selection and analytical processing of information on COVID-19. 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT). Volume 2, Lviv, Ukraine 22-25 Sept. 2021. P. 231-328. Electronic ISBN:978-1-6654-4257-2, Print on Demand(PoD) ISBN:978-1-6654-4258-9, Electronic ISSN: 2766-3639, Print on Demand(PoD) ISSN: 2766-3655. DOI: 10.1109/CSIT52700.2021.9648839.

42. Oleksii Duda, Nataliia Kunanets, Serhii Martsenko, Vyacheslav Nykytyuk, Volodymyr Pasichnyk. Covid-19 data collections and analytical processing. 2021 ieee 16th international conference on computer sciences and information technologies (CSIT). Volume 2, Lviv, Ukraine 22-25 Sept. 2021. p. 252-257. electronic isbn:978-1-6654-4257-2, print on demand (pod) isbn:978-1-6654-4258-9, electronic issn: 2766-3639, print on demand (pod) issn: 2766-3655. doi: 10.1109/csit52700.2021.9648839.

43. Vyacheslav Nykytyuk, Vasil Dozorskyi, Oksana Dozorska, Andrii Karnaukhov and Liubomyr Matiichuk. The Method of User Identification by Speech Signal. The 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP-2022) Ternopil, Ukraine, November 22-24, 2022. Vol-3309 urn:nbn:de:0074-3309-1. P.225-232. ISSN 1613-0073 DOI: 10.1425/jsdtl.

44. Ihor Bodnarchuk, Yuriy Skorenkyy, Taras Kramar, Oleksii Duda and Vyacheslav Nykytyuk. Use of Analytical Hierarchy Process in Scenarios Design for a Digital Museum with XR components. The 2nd International Workshop on

Information Technologies: Theoretical and Applied Problems (ITTAP-2022) Ternopil, Ukraine, November 22-24, 2022. Vol-3309 urn:nbn:de:0074-3309-1. P. 414-425. ISSN 1613-0073 DOI: 10.1425/jsdtl.

45. Kryazhych O., Itskovych V., Iushchenko K., Hrytsyshyna V., Bruvier D., Nykytyuk V., Bodnarchuk I. (2023) The use of abstract moore automaton to control the sensors of a service-oriented alarm and emergency notification network. Scientific Journal of TNTU (Tern.), vol 109, no 1, pp. 111–120. ISSN 2522-4433

46. Dediv, L., Dozorska, O., Kukuruza, V., Nykytyuk, V., Kovalyk, S. Computer Simulation Modeling of Voice Signals in the Matlab Environment for the Task of Computerized Diagnostic Systems Testing. The 1st International Workshop on “Computer information technologies in Industry 4.0” (CITI-2023) will be held in Ternopil, Ukraine, from June 14 to 16, 2023. The Workshop is organized by the Faculty of Applied Information Technologies and Electrical Engineering of Ternopil Ivan Puluj National Technical University. 2023, 3468, pp. 257–262. Vol-3468 urn:nbn:de:0074-3468-8, ISSN 1613-0073.

47. Dozorskyi, V., Dediv, I., Sverstiuk, S., Nykytyuk, V., Karnaukhov, A. The Method of Commands Identification to Voice Control of the Electric Wheelchair. The Workshop is organized by the Faculty of Applied Information Technologies and Electrical Engineering of Ternopil Ivan Puluj National Technical University. The 1st International Workshop on “Computer information technologies in Industry 4.0” (CITI-2023) will be held in Ternopil, Ukraine, from June 14 to 16, 2023. The Workshop is organized by the Faculty of Applied Information Technologies and Electrical Engineering of Ternopil Ivan Puluj National Technical University. 2023, 3468, pp. 233–240. Vol-3468 urn:nbn:de:0074-3468-8, ISSN 1613-0073.

48. О.О. Кузьо, В.К. Крилов, Н.Л. Мацюк. Використання технологій OSINT для формування портету користувача. Міжнародної науково-практичної конференції молодих учених та студентів 7-8 грудня 2022 року. Україна, Тернопіль. Ст. 140.

ДОДАТКИ

Матеріали XI Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 7-8 грудня 2022 року

УДК 004.9

О.О. Кузьо, В.К. Крилов, Н.Л. Мацюк
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ OSINT ДЛЯ ФОРМУВАННЯ ПОРТРЕТУ КОРИСТУВАЧА

Kuzo O.O., Krylov V.K., Matsuk N.L.

USING OSINT TECHNOLOGY TO FORM USER PORTRAIT

Сьогодні, враховуючи стрімкий розвиток інформаційних технологій і соціальних процесів, проблема ефективного виконання управлінських завдань і прийняття рішень постає гостро при роботі з великими масивами неструктурованих різнорідних даних на основі індивідуальних користувацьких профілів.

Для моделювання та дослідження таких систем нині широко використовується OSINT (англ. – Open Source Intelligence) – концепції, методи та прийоми легального отримання та використання інформації з відкритих джерел.

Основною ідеєю OSINT є цілеспрямований збір інформації про об'єкти інтересу (Harvesting) для подальшої обробки та багатовекторного контент-аналізу отриманих даних.

OSINT зручний тим, що: - набагато менше ризику: ніхто не порушує приватність і закони; - ця методика дешевша - не потрібно додаткового обладнання та дорогого програмного забезпечення; - така інформація є легкодоступною (онлайн) і зазвичай завжди актуальна.

Є два основні методи збору інформації:

1. Пасивний. У цьому випадку шукачу інформації неможливо розкрити себе і те, що він шукає. Пошук обмежується вмістом веб-сайту суб'єкта, архівною або кешованою інформацією, незахищеними файлами.

2. Активний. Цей підхід рідко використовується в Інтернет-розвідці. Для отримання інформації було досліджено IT-інфраструктуру компанії та активно взаємодіяли з комп'ютерами та машинами. Передові методи використовуються для отримання доступу до відкритих портів, сканування вразливостей і серверних веб-додатків. У цьому контексті інформаційний інтелект легко ідентифікувати. Соціальна інженерія також застосовується тут.

Вибір методу збору інформації залежить від зібраної інформації та необхідних даних. Важливо розуміти, що те, що легко отримати, не завжди є законним.

Процес розробки OSINT виглядає наступним чином: 1. Оволодіння базовими технологіями, такими як Google Dorks. 2. Пошук цікавих способів використання інструментів і методів і написання невеликих звітів з візуальними результатами. 3. Максимальна анонімність. Під час дослідження OSINT багато часу йде на те, щоб забезпечити вашу безпеку під час пошуку. Це необхідно для того, щоб компанії або окремі особи не могли визначити, що певна інформація збирається.

Література

1.Буслов П.В., Зоренко Д.С., Рябуха Ю.М Використання технологій OSINT для отримання пошукової інформації : практичний порадник. Х. : ІПІОК для СБ України, 2021. 28 с

2. Mozhaiev M, Buslov P. Development of an Information Model for the Personality's Social Portrait Formation Using OSINT Technology // Proceedings of the Technical University – Sofia, Volume 70, Issue 4, 2020, P 37-48.

3. White T. Hadoop: The Definitive Guide, 4th Edition. O'Reilly Media, Inc., 2015, 235p.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.9
В.В. Никитюк, канд. тех. наук, доц., А.К. Карнаухов, Н.Л. Мацюк
Тернопільський національний технічний університет імені Івана Пулюя

ЗАСОБИ ОПТИМАЛЬНОЇ ОЦІНКИ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ ІНДИВІДУАЛЬНИХ ОСОБЛИВОСТЕЙ ВІЗЕРУНКА ПАЛЬЦІВ

V.V. Nykytyuk, Ph.D., Assoc. Prof., A.K. Karnaukhov, N.L. Matsuk

MEANS OF OPTIMAL ASSESSMENT OF BIOMETRIC RECOGNITION OF INDIVIDUAL FEATURES OF THE PATTERN OF FINGERS

Ключові слова: Біометрична система, розпізнавання образів, ідентифікація, автентифікація, шифрування, база даних

Key words: Biometric system, pattern recognition, identification, authentication, encryption, database

Технологія біометрії має на меті імітувати процес розпізнавання образів людини для ідентифікації людей. Він пропонує більш безпечну та надійну альтернативу традиційним методам автентифікації на основі паролів і маркерів. Біометричні системи використовують фізіологічні та поведінкові характеристики, унікальні для окремих людей, для автоматичного розпізнавання. Ці характеристики повинні відповідати певним вимогам, включаючи універсальність (присутність у всіх індивідуумів), продуктивність і застосовність.

Процес розпізнавання в біометрії включає два основні етапи: реєстрацію та підбір. Під час реєстрації система фіксує та витягує дискримінантні атрибути з біометричних даних особи. Потім ці атрибути стискаються та зберігаються як шаблон у базі даних. Шаблон служить репрезентативною структурою, що підсумовує біометричні характеристики особи.

На кроці зіставлення система отримує збережений шаблон і порівнює його з нещодавно отриманими атрибутами особи, яка автентифікується. На основі результатів порівняння система приймає рішення, чи є особа зареєстрованою особою, якою вона себе представляє, з певним рівнем достовірності в діапазоні від 0 до 1. Однак через варіації біометричних зразків як всередині, так і між особами, система може приймати помилкові рішення.

Ефективність системи біометричного розпізнавання зазвичай характеризується двома статистичними даними про помилки: частотою помилкових відхилень (FRR) і частотою помилкових прийомів (FAR). FRR виникає, коли система відхиляє справжню особу, тоді як FAR буває, коли особу самозванця приймається неправильно. Рівна частота помилок (ERR) представляє компроміс між цими двома помилками, де FAR і FRR мають однакові значення. Загальновідомо, що жодна біометрична характеристика не може досягти 100% точності. Поєднання кількох біометричних характеристик в одній системі розпізнавання може посилити рішення щодо розпізнавання та підвищити точність.

Ринок і індустрія біометрії переживають стрімке зростання через зростання попиту на безпечну автентифікацію в електронних послугах і зростання випадків шахрайства в усьому світі. Серед різних біометричних модальностей розпізнавання відбитків пальців є найбільш домінуючим на ринку. Він пропонує компроміс між точністю, безпекою та вартістю порівняно з іншими методами. У наступному розділі ми детально розглянемо відбитки пальців як біометричну характеристику та автоматизований процес розпізнавання на основі цієї модальності.