УДК 004.056.53 **DOI:10.30837/rt.2025.4.223.08**

І.В. ОЛЕШКО, канд. техн. наук, В.І.ЛУЦЕНКО, О.Є. ПЕТРЕНКО, канд. техн. наук, О.А. МЕЛЬНИКОВА, канд. техн. наук

ОЦІНКА ЕФЕКТИВНОСТІ АТАК З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ НА СИСТЕМИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ

Вступ

У сучасному цифровому середовищі, де обсяг онлайн-транзакцій, мобільних сервісів та віддалених комунікацій невпинно зростає, питання надійної автентифікації користувачів набуває особливої ваги. Традиційні методи захисту, зокрема паролі та PIN-коди, дедалі частіше демонструють свою вразливість перед кіберзагрозами, що стимулює пошук більш стійких та зручних рішень. На цьому тлі біометрична автентифікація стає одним із ключових напрямів підвищення безпеки інформаційних систем. Її популярність зумовлена високою точністю, складністю підроблення та простотою використання. Одним з найпоширеніших методів біометричної автентиифікації є автентифікація за відбитками пальців.

Зі стрімким розвитком технологій штучного інтелекту виникають принципово нові кібератаки для біометричних систем автентифікації. Завдяки можливостям ШІ, зокрема машинному навчанню, зловмисники мають змогу моделювати та відтворювати біометричні дані з метою обходу систем біометричної автентифікації.

Метою статті є оцінка ефективності розповсюджених атак з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців. Наші дослідження можуть бути корисними при розробці та тестуванні нових та існуючих біометричних систем автентифікації, для впровадження захисту критичної інфраструктури та фізичного доступу, а також для аудиту і стандартизації безпеки.

Огляд літературних джерел

Системи біометричної автентифікації на основі відбитків пальців є однією з найпоширеніших технологій в комерційних і мобільних додатках, що підтверджується зростанням ринку та широкою інтеграцією в доступні рішення [1]. Одночасно в літературі фіксується, що найбільш розповсюдженим видом загроз для цих систем залишаються спуфінг-атаки, коли зловмисник намагається видати цифрову копію відбитка за істинне зображення для обхода сенсорів [2].

Сучасні дослідження показують, що розвиток генеративних моделей і методів глибокого навчання створюють нові загрози для систем біометричної автентифікації, зокрема шляхом генерації синтетичних образів, які можуть сприйматися системами біометричної автентифікації, як істинні [3]. Генеративні змагальні мережі або ж GAN є класом методів машинного навчання, який складається з двох нейронних мереж, генератора і дискримінатора. Ці мережі змагаються між собою в рамках теорії ігор [4]. Метою GAN є створення моделі, яка здатна синтезувати зразки, схожі на реальні дані з навчального набору. Згенерована інформація оцінюється і переглядається дискримінатором, який намагається відрізнити синтетичні дані від реальних. Генератор постійно покращує якість своїх вихідних даних так, щоб дискримінатор не міг їх відрізнити від справжніх [5]. Дослідження показують, що атаки на основі штучного інтелекту часто комбінують різні стратегії та підходи, що підвищує їхню стійкість у реальних сценаріях [6].

Таким чином, оцінка ефективності атак на основі штучного інтелекту є ключовою передумовою безпечного функціонування сучасних біометричних систем та їх подальшого розвитку.

1. Система біометричної автентифікації за відбитками пальців

Відбитки пальців являють собою унікальні генетичні риси, притаманні людині від народження. Зазвичай вони різняться між собою завдяки особливостям візерунків, що складаються з гребенів і западин. Саме ці деталі відіграють вирішальну роль у процесі ідентифікації відбитків. Для розпізнавання переважно використовуються точки роздвоєння гребенів та

кінцеві точки [7]. Зазвичай алгоритми розпізнавання базуються на збігу дрібниць, аналізу ключових точок, напрямів гребенів та загальної геометрії візерунку, перетворюючи ці характеристики у числові вектори. Дрібниці відбитків пальців мають особливості, зображені на рис. 1.

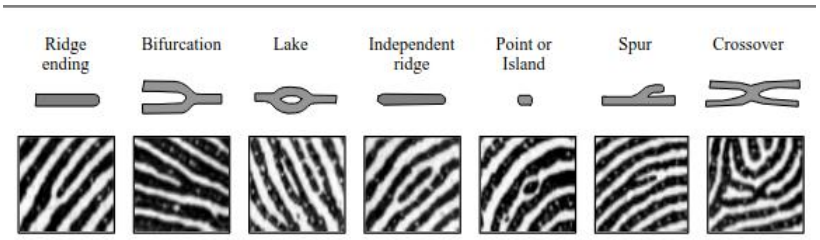

Рис. 1. Дрібниці відбитків пальців

Коефіцієнт подібності сам по собі не обов'язково вказує на те, чи належать два зображення відбитків пальців одній і тій самій людині. Натомість він показує, наскільки складно зіставити два відбитки. Хоча шаблони з високими показниками подібності найімовірніше належать одному й тому ж пальцю, це не завжди так. У системах розпізнавання за відбитками пальців можна обчислити три типи оцінок подібності на основі дрібниць [7]: локальна попарна оцінка, що вимірює відмінності для кожної пари дрібниць; глобальна оцінка, що аналізує співвідношення кількості співпавших дрібниць до їх загальної кількості; та гібридні оцінки, які поєднують інформацію на локальному і глобальному рівні.

Кожна дрібниця може бути описана кількома атрибутами, включаючи її розташування на зображенні, орієнтацію та тип. Найпоширеніші алгоритми зіставлення розглядають кожну дрібницю як триплет m = {x, y, θ}, що вказує координати розташування мінуції {x, y} та кут мінуції θ:

$$T = \{m_1, m_2, \dots m_m\}, m_i = \{x_i, y_i, \theta_i\}, \qquad i = 1 \dots m$$
$$I = \{m'_1, m'_2, \dots m_n\}, m'_j = \{x_j, y_j, \theta_j\}, \qquad j = 1 \dots m$$

Дрібниця у зображенні I та дрібниця у шаблоні T вважаються відповідними, якщо просторова відстань між ними менша за задану допустиму величину (формула (1), а різниця напрямків між ними менша за кутову допустиму величину (формула (2). Згідно з цими формулами при обчисленні різниці кутів враховується їхня циклічність. Допустимі межі необхідні для компенсації неминучих помилок, що виникають під час виділення ознак, а також для врахування можливих деформацій пальця:

$$sd(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \le r_0 \tag{1}$$

$$dd(m'_j, m_i) = \min\left(\left|(\theta'_j - \theta_i)\right|, 360^o - \left|(\theta'_j - \theta_i)\right|\right) \le \theta_0 \tag{2}$$

Вирівнювання двох відбитків пальців є обов'язковим етапом [7], спрямованим на максимізацію кількості співставлених дрібниць. Коректне вирівнювання потребує визначення параметрів зміщення (по осях x та y) та обертання (кут θ). Для опису процедури вирівнювання вводять функції, зокрема map(), яка відображає дрібницю з відбитка I у нову позицію, та індикаторну функцію mm(), що повертає 1, коли мінуції відповідають критеріям зіставлення (1) та (2), і 0 в іншому випадку.

З урахуванням введених функцій, задачу зіставлення можна сформулювати наступним чином:

$$\max_{\Delta x, \Delta y, \theta, P} \sum_{i=1}^{m} mm(map_{\Delta x, \Delta y, \theta}(m'_{P(i)}, m_i) \tag{3}$$

де P(i) – невідома функція, яка визначає пару між I та T мініатюрами.

Формалізована задача вирівнювання полягає у визначенні параметрів геометричного перетворення, що максимізують кількість відповідностей між дрібницями порівнюваних відбитків.

Схожість між двома шаблонами дрібниць розраховується по формулі [8]

$$r_0 = \frac{N_M^2}{N_Q * N_R} \tag{4}$$

2. Атаки з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців

Спуфінг відбитків пальців є однією з найпоширеніших атак на біометричні системи. Із появою генеративних моделей, зокрема GAN, ця проблема стала ще гострішою, оскільки з'явилася можливість створювати високоякісні синтетичні відбитки пальців, не маючи доступу до оригіналів. Однією з таких моделей є SpoofGAN, запропонована у 2022 р. [9]. Процес генерації зображення в ній складається з трьох етапів: спочатку відбувається синтез базового відбитка (бінарного зображення структури гребенів) з використанням латентного вектора $z_{id} \in R^{256}$; далі йде створення різних відбитків шляхом застосування реалістичних трансформацій до базового зображення; на завершальному етапі відбувається накладання текстур за допомогою другої нейронної мережі для імітації реалістичної шкіри. На рис. 2 зображено структуру GAN моделі SpoofGAN з трьома основними етапами.

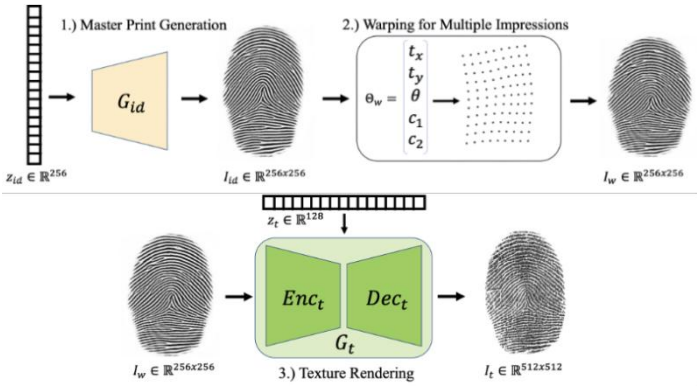

Рис. 2. Архітектура GAN моделі SpoofGAN

Більш новітній підхід, FingerFaker, запропонований у 2023 р., використовує концепцію псевдонабору дрібниць. Це дозволяє генерувати синтетичні відбитки без доступу до даних користувача [10]. Атака починається з випадкової ініціалізації популяції псевдодрібниць, яка обробляється генетичними операторами. Попередньо навчений генератор створює фальшиві відбитки, які надсилаються в систему розпізнавання. Якщо атака не вдається, FingerFaker використовує показники якості та результати порівняння для вибору наступного покоління псевдонаборів і повторює процес.

Алгоритм Фенга і Джейн реалізовано шляхом розбиття цільового простору на квадратні блоки 8x8 пікселів. Для кожного блоку прогнозується локальна орієнтація гребенів на основі напрямків найближчих дрібниць (використовується до восьми дрібниць, по одній з кожного з восьми секторів навколо блоку) [11]. Щоб врахувати періодичність, кути напрямків дрібниць a_k подвоюються. Потім орієнтація обчислюється через зважене агрегування тригонометричних компонентів, де w_k є ваговою функцією, що визначає вплив дрібниці k:

$$u = \sum_{k=1}^{K} \cos(2a_k) w_k \tag{7}$$

$$u = \sum_{k=1}^{K} \cos(2a_k) w_k \tag{8}$$

Фінальна орієнтація блоку $O(m, n)$ обчислюється як:

$$O(m, n) = \frac{1}{2}\arctan\left(\frac{v}{u}\right) \quad (9)$$

Блок-схема алгоритму реконструкції відбитків пальців Фенга і Джейн зображена на рис. 3.

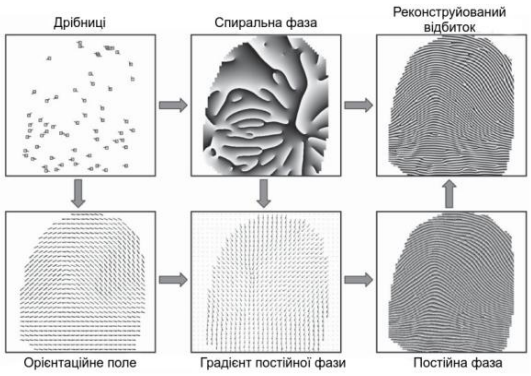

Рис. 3. Блок-схема алгоритму реконструкції відбитків пальців Фенга і Джейн

Методу відновлення відбитку пальця також представили Бузагло та Келлер у 2022 р. Було запропоновано використовувати енкодер дрібниці до вектора, де $x \in \mathbb{R}^{h*w*3}$ – зразок відбитку пальця, а $S_x = \{\theta_{ij}, T_{ij}\}$ – набір дрібниць отриманих з x в точці $\{i, j\}$, θ_{ij} є напрямом і T_{ij} є класом дрібниці. Модель відновлення має на меті реконструювати x зображення за заданим набором S_x. Основною задачею на початку є перетворення набору дрібниць у мапу дрібниць $M_x \in \mathbb{R}^{h*w*3}$. Після цього мапа дрібниць кодується у латентний вектор $w \in \mathbb{R}^{512}$ та подається до генератора GAN моделі, яка реконструює відбиток пальця [12].

У табл. 1 наведено порівняння розглянутих методів атак з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців.

Таблиця 1

Назва методу	**Тип атаки**	**Переваги**	**Недоліки та обмеження**	**Можливість цільового спрямування**
SpoofGAN	Синтетична генерація	Висока точність генерації, не потребує фізичного доступу до оригіналу	Вимагає значних обчислювальних ресурсів, генерує випадкові особистості	Відсутня
FingerFaker	Синтетична генерація	Не потребує доступу до даних жертви	Висока ресурсомісткість навчання, складність налаштування	Відсутня
Метод Фенга і Джейна	Реконструкція з шаблону	Використовує лише стандартні дані дрібниць із шаблонів	Обмежена реалістичність без додаткових даних про текстуру	Наявна
Метод Бузагло та Келлер	Реконструкція з шаблону	Висока точність реконструкції завдяки використанню GAN	Залежність результату від якості класифікації вхідних дрібниць	Наявна

На основі порівняння визначено, що хоча методи синтетичної генерації демонструють високу точність у створенні загальних біометричних образів, вони не становлять прямої загрози для конкретних облікових записів без додаткових механізмів підбору. Найбільшу небезпеку для персоналізованої безпеки становлять методи реконструкції, які дозволяють зловмиснику відновити унікальний папілярний візерунок конкретної особи з компрометованого шаблону.

3. Експериментальне дослідження атаки методом реконструкції відбитку пальця

3.1. Налаштування експерименту

Для проведення експериментального дослідження необхідна система з наступними характеристиками:

- операційна система Ubuntu 20.04 і вище;
- процесор Intel Core i5 або AMD Ryzen 5 з тактовою частотою від 2.5 ГГц;
- оперативна пам'ять обсягом не менше 8 ГБ;
- відеокарта з підтримкою CUDA та обсягом пам'яті не менше 4 ГБ з рекомендацією використання NVIDIA RTX серії;
- вільне місце на жорсткому диску обсягом не менше 30 ГБ для зберігання моделей та проміжних результатів;
- клавіатура та миша для взаємодії з інтерфейсом програми.

Центральним елементом архітектури є генератор відбитків пальців, побудований на основі StyleGAN2, який попередньо натренований на наборі даних NIST SD14.

Практична реалізація виконана мовою Python 3.8. Для нормального функціонування програми необхідно встановити PyTorch версії 1.8 або вище для роботи з нейронними мережами, OpenCV – для обробки зображень, NumPy – для роботи з багатовимірними масивами, SciPy – для математичних операцій.

Детектор дрібниць MINDTCT, розроблений NIST, необхідний для отримання характеристик дрібниць з оригінальних зображень відбитків 512x512 у форматах PNG або JPG.

Архітектура з використанням CUDA потрібна для ефективної паралельної обробки на GPU.

3.2. Проведення експерименту

Обраний для дослідження метод реконструкції відбитків базується на праці Бузагло та Келлера. Загальна архітектура є конвеєром, що складається з чотирьох основних компонентів: модуль обробки дрібниць, блок алгоритмічного перетворення, енкодер на основі ResNet50 та генератор StyleGAN2. Загальна схема обраного методу зображена на рис. 4.

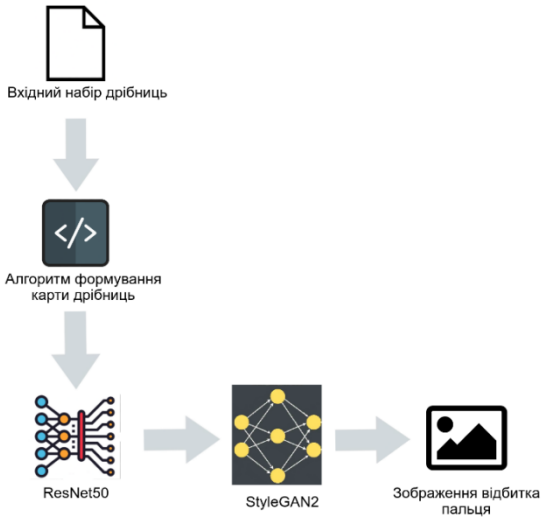

Рис. 4. Загальна архітектура обраного методу реконструкції

Процес реконструкції починається з обробки дрібниць: на початковому етапі дискретний набір мінуцій перетворюється у структуроване просторове представлення. Спеціалізований алгоритмічний блок перетворює цей набір у тривимірний тензор розміром $h * w * 3$, де h та w відповідають висоті та ширині цільового зображення відповідно.

Отримана карта дрібниць M_x піддається операції згортки з Гауссовим ядром $G(\sigma)$ для стабілізації характеристик та зменшення шуму. Цей крок є критично важливим для забезпечення стабільності навчання нейронних мереж на наступних етапах обробки.

Модуль енкодера виконує перетворення оброблених просторових даних у компактне латентне представлення. В якості архітектурної основи енкодера використовується згорткова нейронна мережа ResNet50. Енкодер E приймає на вхід згладжену карту дрібниць розмірністю $h * w * 3$ та формує латентний вектор w фіксованої розмірності 512.

Завершальний етап реалізується генератором StyleGAN2 (G). Ця модель перетворює латентний код w у послідовність стильових векторів, які модулюють процес синтезу на різних рівнях деталізації, що дозволяє досягти високої якості реконструйованих зображень.

Результатом роботи генератора є зображення відбитка пальця I у градаціях сірого $I \in \mathbb{R}^{h*w}$, де I представляє реконструйоване зображення відбитка пальця з роздільною здатністю $h * w$. Структура реалізованого методу реконструкції відбитку пальця зображена на рис. 5.

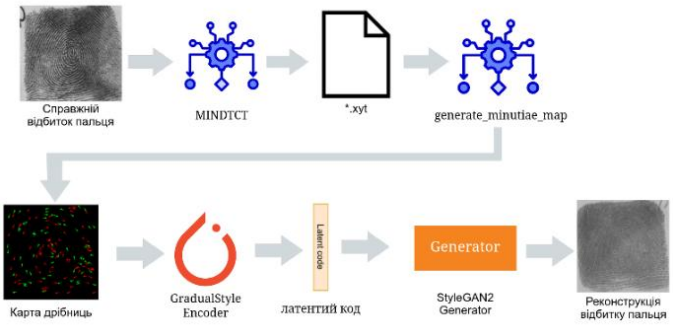

Рис. 5. Структура реалізованого методу реконструкції відбитку пальця

3.3. Оцінка ефективності

Для оцінки ефективності реалізованого методу було створено програмну реалізацію для аналізу атак. Цей сценарій передбачає, що зловмисник реконструює відбитки з викрадених шаблонів і використовує їх проти тієї ж системи, з якої вони були вкрадені.

Для порівняння відбитків було інтегровано алгоритм BOZORTH3, розроблений NIST [13]. Цей алгоритм порівнює локальні структури дрібниць і працює з файлами формату .xyt.

Для проведення експериментального дослідження було використано 466 genuine відбитків пальця та зроблено 99235 impostor порівнянь. Genuine відбитки представляли справжні зразки користувачів системи, тоді як impostor порівняння включали спроби несанкціонованого доступу з використанням реконструйованих відбитків.

В основі оцінки ефективності використовується значення порогу, що є числовим значенням схожості, яке система використовує для прийняття рішення про надання доступу. Для визначення порогового значення було побудовано гістограму згідно з рис. 6. На ній зображено розподіл оцінок відповідностей для легітимних користувачів та зловмисників. По горизонтальній осі відкладено числові значення оцінок схожості, а вертикальна вісь відображає частоту появи таких значень під час експерименту. Червоним кольором позначено розподіл для спроб несанкціонованого доступу. Основна маса цих значень зосереджена в області низьких показників, що свідчить про ефективне відсіювання системою більшості атак. Зеленим кольором виділено розподіл для легітимних користувачів з реконструйованих зображень, що зміщений у бік високих показників. У місці перетину цих двох графіків знаходиться порогове значення. Високий відсоток успішності атаки підтверджує, що реконструйовані відбитки долають цей бар'єр і зміщуються в зону довіри, через що система помилково ідентифікує їх як легитимні.

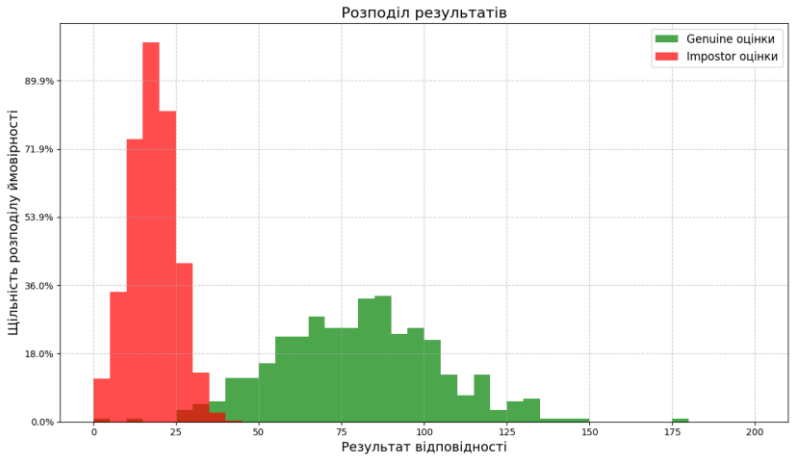

Рис. 6. Розподіл результатів відповідності відбитків пальців

Для визначення оптимального порогу обчислюється коефіцієнт хибного прийняття в діапазоні від 0 до 300 з кроком 5 $\mathrm{FAR(t)} = \frac{\mathrm{impostor} \geq \mathrm{t}}{\mathrm{total\_impostor}}$, де $\mathrm{impostor} \geq \mathrm{t}$ є кількістю оцінок для зловмисних відбитків, які перевищують або дорівнюють порогу t, total_impostor показує загальну кількість порівнянь зловмисних відбитків. Для заданого цільового значення знаходиться оптимальний поріг за критерієм $\mathrm{Оптимальний\ поріг} = \mathrm{argmin}|\mathrm{FAR(t)} - \mathrm{FAR\_target}|$, де FAR_target заздалегідь задані цільові рівні безпеки системи (1 %, 0.1 %, 0.01 %).

Точність верифікації показує відсоток успішних атак як частку реконструйованих відбитків, які змогли подолати відповідний поріг системи $\mathrm{Точність} = \left(\frac{\text{кількість genuine оцінок} \geq \text{Поріг}}{\text{Загальна кількість спроб атаки}}\right) * 100.$

Результати оцінки ефективності атаки наведені в табл. 2.

Таблиця 2

FAR, %	**Поріг**	**Точність,** %
1	33	98.52
0.1	39	97.66
0.01	43	96.68

Аналіз результатів демонструє, що при зниженні допустимого рівня хибних прийняттів з 1 до 0.01 %, поріг прийняття рішень зростає з 33 до 43 балів, що призводить до зменшення точності верифікації з 98.52 до 96.68 %.

В роботі проведено порівняльний аналіз успішності атаки реалізованим методом та інших розповсюджених атак на основі штучного інтелекту на системи біометричної автентифікації за відбитками пальців. Результати такого аналізу наведені у табл. 3.

Таблиця 3

Метод	**Тип атаки**	**Успішність атаки,** %	**FAR,** %
SpoofGAN	Синтетична генерація	99.87	FAR = 0.01
FingerFaker	Синтетична генерація	94.22	FAR = 0.01
Feng & Jain	Реконструкція	93.62	FAR = 0.01
Реалізований метод	Реконструкція	96.68	FAR = 0.01

З табл. 3 можна зробити висновок, що метод, заснований на праці Бузагло та Келлера дозволяє досягти точності розпізнавання за підробленим зразком 96.68 %. Це перевищує

показники методу реконструкції Фенга та методу синтетичної генерації. І, хоча метод SpoofGAN демонструє найвищу точність розпізнавання, реалізований підхід підтверджує критичну небезпеку, оскільки забезпечує високу ймовірність злому конкретного облікового запису.

Висновки

Проаналізовано існуючі біометричні системи автентифікації та встановлено, що автентифікація за відбитком пальця є однією з найпоширеніших технологій. Атаки на основі штучного інтелекту створюють нові виклики та необхідність впровадження додаткових механізмів захисту для біометричних систем.

Розглянуто систему біометричної автентифікації за відбитками пальців та надані основні формули для знаходження подібності двох зображень.

Зроблено порівняльний аналіз методів атак із використанням GAN, зокрема порівняно синтетичну генерацію SpoofGAN, FingerFaker та методи реконструкції відбитків з шаблонів дрібниць на основі алгоритмів Фенга і Джейна, а також Бузагло і Келлера. Встановлено, що підхід Бузагло і Келлер є одним з найперспективніших.

Проведено експериментальне дослідження атаки методом реконструкції відбитку пальця. Результати експерименту підтвердили вразливість біометричних систем автентифікації до атак реконструкції. Навіть при налаштуваннях системи безпеки, де FAR = 0.01 %, реконструйовані відбитки продемонстрували високу ефективність обходу біометричної системи автентифікації, досягнувши точності роспізнавання у 96.68 %.

Проведено порівняння оцінок ефективності розповсюджених методів атак на основі штучного інтелекту на біометричні системи автентифікації за відбитками пальців. Встановлено, що метод Бузагло і Келлера демонструє одну з найвищих ефективнстостей серед розглянутих підходів. Точність верифікації за цим методом варіює з 98.52 до 96.68 % в залежності від налаштувань системи.

Вважаємо, що актуальними та необхідними є подальші дослідження у сфері проведення атак на основі штучного інтелекту на системи біометричної автентифікації. Це дозволить створювати ефективні методи протидії таким атакам та підвищити рівень надійності біометричних систем автентифікації загалом.

Список літератури:

1. Методи і технології біометричної ідентифікації за результатами літературних джерел / Л. Г. Коваль та ін. // Вчені записки ТНУ ім. В.І. Вернадського. Серія: технічні науки. 2019. Т. 30 (69) Ч. 1 № 2. С. 104–111.

2. Security vulnerabilities against fingerprint biometric systems: book chapter / Sushanta Kumar Das and other // Recent Advances in Computational Intelligence Applications for Biometrics and Biomedical Devices. 2025. Chapter 4. P. 35–43.

3. Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution / P. Bontrager, et al. // Conference: 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS) IEEE BTAS. 2018. P. 1–9. DOI:10.1109/BTAS.2018.8698539.

4. Goodfellow I, Pouge.t-Abadie J, Mirza M, Xu B, Warde-FarleyD, Ozair S, Courville A, Bengio Y. Generative adversaria lnetworks. Commun // ACM, 2020. vol. 63, no. 11. P.139–144.

5. Ateniese G. Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers / G.Ateniese,G.Felici,L.V.Mancini 1 et al. // International Journal of Security and Networks. 2010. Vol.10,Issue 3. P.137–150.

6. Combined Adversarial Attacks for Breaking Fingerprint Presentation Attack Detectors / S. Zedda // EUSIPCO 2025: conference paper, Thu, 11 Sep. 2025, Italy, Bellini. P. 1352–1356.

7. Yu Y, Niu Q, Li X, Xue J, Liu W, Lin D. A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications. Micromachines (Basel). 2023 Jun 14;14(6):1253. doi: 10.3390/mi14061253. PMID: 37374839; PMCID: PMC10305017..

8. Maltoni D., Maio D., Jain A.K., Prabhakar S. Handbook of Fingerprint Recognition. 2nd ed. London : Springer-Verlag London Limited, 2009. 475 p.

9. S. A. Grosz, A. K. Jain. SpoofGAN: Synthetic Fingerprint Spoof Images // IEEE Transactions on Information Forensics and Security. 2023. vol. 18. P. 730–743. doi: 10.1109/TIFS.2022.3227762.

10. Shen Y., Ma Z., Lin F., Yan H., Ba Z., Lu L., Xu W., Ren K. FingerFaker: Spoofing Attack on COTS Fingerprint Recognition Without Victim's Knowledge // Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems (SenSys '23). New York : Association for Computing Machinery, 2024. P. 167–180.

11. K. Cao, A. K. Jain. Learning fingerprint reconstruction: From minutiae to image // IEEE Trans. on Information Forensics and Security. 2015. Vol. 10, no. 1. P. 104–117.

12. Bouzaglo R., & Keller Y. Synthesis and reconstruction of fingerprints using generative adversarial networks. arXiv preprint arXiv:2201.06164, 2022.

13. NIST Biometric Image Software (NBIS). nist.gov. URL: https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis/.

Надійшла до редколегії 20.10.2025

Відомості про авторів:

Олешко Інна Вікторівна – канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: inna.oleshko@nure.ua; ORCID: https://orcid.org/0000-0002-8021-0467

Луценко Владислав Ігорович – Харківський національний університет радіоелектроніки, бакалавр; Україна; e-mail: vladyslav.lutsenko1@nure.ua; ORCID: https://orcid.org/0009-0007-0102-461X

Петренко Ольга Євгенівна, канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: olha.petrnko@nure.ua; ORCID: https://orcid.org/0000-0002-7862-5399

Мельникова Оксана Анатоліївна – канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; email: oksana.melnykova@nure.ua; ORCID: https://orcid.org/0000-0001-8843-9648