



Унікальність та неповторюваність папілярних узорів у вік штучного інтелекту

Вероніка Венчагова

старший судовий експерт сектору дактилоскопічних досліджень
відділу криміналістичних видів досліджень, Одеський науково-дослідний
експертно-криміналістичний центр Міністерства внутрішніх справ України, м. Одеса,
Україна, ORCID: <https://orcid.org/0000-0002-4262-4028>, e-mail: nicavench@gmail.com

Тези присвячено дослідженню можливості підроблення слідів папілярних узорів за допомогою штучного інтелекту, неповторюваності цих узорів та надійності їх використання з метою захисту персональних даних.

Ключові слова: дактилоскопія; судова експертиза; відбитки пальців; штучний інтелект.

Uniqueness and Unrepeatability of Papillary Patterns in the Age of Artificial Intelligence

Veronika Venchahova

The article is devoted to the study of the possibility of falsifying traces of papillary patterns with the help of artificial intelligence, the uniqueness and reliability of such a means of protecting personal data.

Keywords: fingerprinting; forensic examination; fingerprints; artificial intelligence.

Як відомо з курсу криміналістики, основними властивостями папілярних узорів є їхня індивідуальність, стійкість та відновлюваність. *Індивідуальність* папілярних узорів полягає в тому, що в кожній людині свої малюнки папілярних ліній, а будова їхніх ліній має таку сукупність ознак, яка дає змогу відрізнити один візерунок від іншого. Цікавий (і поки ще єдиний) випадок зафіксовано в мешканців Швеції Андреаса Даніельсона та його доньки Марі, у яких зовсім відсутні папілярні лінії на пальцях рук. Та навіть відсутність папілярних ліній — це яскрава індивідуальність відбитків пальців рук людини, яка дає змогу її ідентифікувати.

Стійкість папілярних узорів виявляється в тому, що протягом усього життя людини їх будова не змінюєть-

ся. На нігтьових фалангах вони виникають на 3—4-му місяці розвитку плода людини, а остаточне формування їх відбувається на шостому місяці. Розвиток організму людини пов'язаний зі збільшенням ширини, висоти та довжини папілярних ліній, але малюнок, його окремі деталі, кількість папілярних ліній залишаються незмінними. В експертній практиці мали місце випадки виявлення пересадки злочинцям, які перебували на дактилоскопічному обліку, ділянок шкіри папілярного узора. Однак і в цих випадках є певні ознаки, що дають змогу встановити факт пересадки шкіри та ідентифікувати особу. Про *відновлюваність* папілярних ліній свідчать такі дані: пошкоджений епідерміс через певний час відновлюється в початковому вигляді,



а пошкодження дерми призводить до порушення папілярних ліній та утворення шрамів або рубців [1].

Завдяки властивості неповторюваності папілярних узорів учені розробили можливість їх використання задля забезпечення персональних даних, входів до приміщень тощо за допомогою біометричних замків. Біометрія — це система розпізнавання людини за допомогою фізичних або поведінкових характеристик. Зараз усе більшої популярності набувають біометричні замки, у яких ідентифікатором є відбиток пальця.

Перевагами використання біометричних замків є, наприклад, їхня компактність — в одному пристрої (або навіть кнопці) перебувають як сам замок, так і зчитувач відбитка пальця, зручність їх використання через те, що такий замок може містити інформацію про щонайменше 1000 відбитків пальців, дає користувачу змогу легко та швидко надавати доступ та видаляти з бази даних відбитки пальців; також однією з переваг є простота монтажу — вони вбудовуються в мобільні пристрої, планшети, ноутбуки, двері без необхідності зламу дверної коробки, також ці замки містять вбудований акумулятор.

Дослідимо можливість виготовлення штучних відбитків пальців рук для використання їх для зламу біометричних замків. По-перше, необхідно отримати якісний зразок папілярного узору пальців людини, найкраще з гладкого скла чи пластику. Потім необхідно законтрастувати цей відбиток. Далі треба відсканувати або сфотографувати відбиток пальця у ви-

сокій якості, у фоторедакторі видалити зайві дрібні деталі, пил, бруд, віддзеркалити зображення.

Наступний крок: необхідно роздрукувати відбиток пальця на плівці та присипати його графітовим порошком, далі покрити шаром рідкого латексу для повторення рельєфу папілярного узору. Далі можна приклеїти отриманий відбиток на свій палець.

Але навіть такий складний і витратний за часом спосіб не зможе розкодувати біометричний замок. Справа в тому, що сенсор сучасних замків зчитує не лише зображення, а й температуру та вологість пальця. Тому обдурити сучасний біометричний замок — завдання нелегке.

Учені із Нью-Йоркського університету застосували нейронну мережу, аби підробити відбитки людських пальців, і їм це вдалося. Результатами своєї роботи вони поділилися на конференції з безпеки в Лос-Анджелесі.

Великий недолік сучасних біометричних систем автентифікації за відбитками — це те, що вони «не бачать» відсканований цілий відбиток пальця. Для їх розблокування потрібен лише невеличкий фрагмент, який вони порівнюють із тим фрагментом, що вже є в базі. Тобто відбиток має відповідати одному параметру замість багатьох, які використовуються для визначення збігів слідів під час проведення дактилоскопічної експертизи.

Також варто зауважити, що деякі елементи візерунка мають меншу ідентифікаційну вагомість, тобто більш поширені за інші (наприклад, початки та закінчення, розгалуження та злиття папілярних ліній трапля-

ються значно частіше, ніж фрагменти, крапки, гачки тощо), та й узагалі петльові та дугові типи папілярних узорів більш поширені за завиткові. Можна дійти висновку: вірогідність, що фальшивий відбиток, який складається з таких поширених фрагментів, швидше підійде, значно вища.

Зважаючи на викладене вище, учені «навчили» програмне забезпечення штучно створювати відбитки

пальців. Але, як здається, деякі з них мали гострі кути, були прямокутними та «кутуватими» (див. *рис.*). І дійсно, навіть без досвіду проведення дактилоскопічних експертиз людина на око може визначити, де підробка, а де — справжні відбитки. Але сканер відбитків пальців та біометричні замки із таким сканером, як уже йшлося вище, мають іншу систему зчитування даних та їх оцінювання.

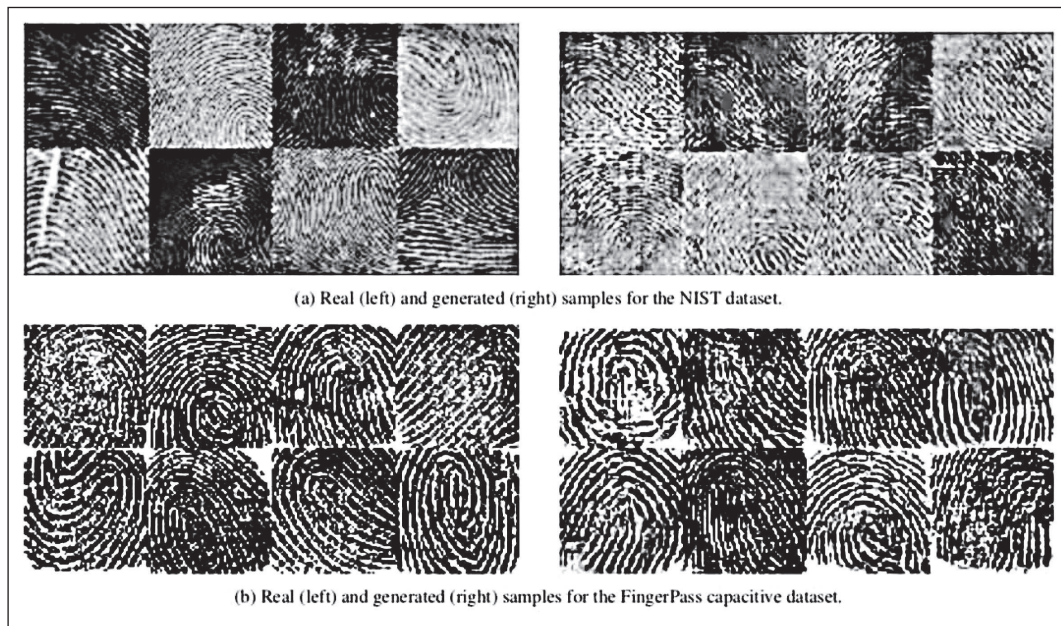


Рис. У лівій частині рисунка розміщено справжні відбитки пальців рук людини, а у правій — згенеровані за допомогою нейронної мережі

У результаті цих дій за допомогою «штучних» відбитків науковцям вдалося обійти біометричну автентифікацію в одному випадку із п'яти.

За словами програмістів, такий метод схожий на «словникову атаку»: щоб зламати систему, хакер завантажує попередньо згенерований перелік найпоширеніших паролів.

Перелік джерел посилання

1. Шепітько В. Ю., Журавель В. А., Коновалова В. О. та ін. Криміналістика: підручник. У 2 т. Т. 1; за ред. В. Ю. Шепітька. Харків, 2019. 328 с. URL: https://profbook.com.ua/index.php?route=product/product/download&product_id=5111&download_id=1150&srsId=AfmBOoqa-CayurA3798fWJ-plw9NbRutqAnDSdjlJ-d0UhDBwES5asKo6r (дата звернення: 14.09.2025).