

УДК 681.3.01

**Й. Й. Білинський, д. т. н., проф.; М. Й. Юкиш, к. т. н.; О. А. Павлюк****ДАКТИЛОСКОПІЧНІ СКАНЕРИ**

*У статті проаналізовано основні методи дактилоскопічного сканування й наведено конструкції основних існуючих типів сканерів, вказано їхні переваги й недоліки. Визначено основну проблему та способи її вирішення.*

**Ключові слова:** дактилоскопічний сканер, відбиток, біометрія.

**Вступ**

Для ідентифікації людини широко використовуються біометричні технології, такі як: ідентифікація за голосом, обличчям, сітківкою ока, відбитком пальців чи долонь, ДНК та інші. Біометричні технології широко використовуються в системах керування доступом, обліку робочого часу й реєстрації відвідувачів, у системах голосування, проведення електронних платежів. Саме вони найбільше розвивають біометричний ринок [1 – 3].

Найбільший розвиток біометричних технологій розпочався після подій 11 вересня 2001 року у США. Тоді розробкою біометричного обладнання зайнялися багато відомих компаній, таких як: LG, Sanyo, Polaroid, NEC, Panasonic, які раніше не займалися цим.

Пристрої для перетворення папіярного візерунку пальця в цифрове зображення або в цифровий образ називаються дактилоскопічними сканерами. Ще в 19 столітті було встановлено, що папіярний візерунок пальців є неповторним у кожній людині (вони різні навіть у близнят), а за понад, ніж столітню історію використання відбитків пальців у криміналістиці та інших галузях не було виявлено двох людей з однаковими відбитками [1, 2, 4, 5]. Зараз дактилоскопічні сканери можна зустріти в банках, на митницях, у громадських закладах, ноутбуках, мобільних телефонах та інших місцях і пристроях. Їхнє використання, за прогнозами аналітичного агентства Frost & Sullivan [5], буде щорічно збільшуватися на 25%, завдяки тому, що почалося масове створення біометричних паспортів у США і Євросоюзі. Індія розпочала програму Unique Identification Authority, метою якої є видати кожному з 1,2 мільярдів жителів біометричну ідентифікаційну карту [5].

**Постановка завдання**

Підвищення надійності роботи сканерів, захист від шахрайства досягається переважно спеціальним програмним забезпеченням, але сама їхня технологія залишає деяку невизначеність і ймовірність неправильного прийняття рішення внаслідок можливого некоректного втручання. Наприклад, у Німеччині хакери роздобули відбитки пальців голови німецького МВС (Міністерства внутрішніх справ) Вольфганта Шойбле, наклеїли його відбитки на свої і пройшли ідентифікацію на оптичному сканері [6]. Тому важливо розвивати інші, більш захищені технології, оскільки в багатьох країнах Європи можна розраховуватись у супермаркеті не кредиткою, а відбитком пальця.

Надалі використання відбитків в інших сферах життєдіяльності людей буде тільки збільшуватися. Слабке місце сканерів, як було сказано вище, демонструє випадок, коли штучна копія пальця, яка повністю відповідає його параметрам, ідентифікується як справжня. Саме тому слід використовувати властивості живого пальця людини. Він має певну температуру, по ньому проходять електричні імпульси від скорочення серця, у ньому відбуваються зміни тиску крові (пульс), сама кров, рухаючись, заряджає шар мертвих клітин на поверхні пальця певним зарядом [7]. Якщо під час сканування відбитку перевіряти одну чи декілька вищенаведених властивостей, то некоректно втрутитись у роботу сканера буде надзвичайно складно.

Тому основною метою роботи є огляд сучасних автоматизованих методів сканування дактилоскопічних відбитків, які забезпечують високий рівень захищеності сканерів від

різних видів шахрайств.

### Основна частина

На сьогодні відомо багато видів дактилоскопічних сканерів, які за принципом роботи можна поділити на 3 основні категорії: оптичні, ультразвукові та напівпровідникові. (рис. 1) [8].

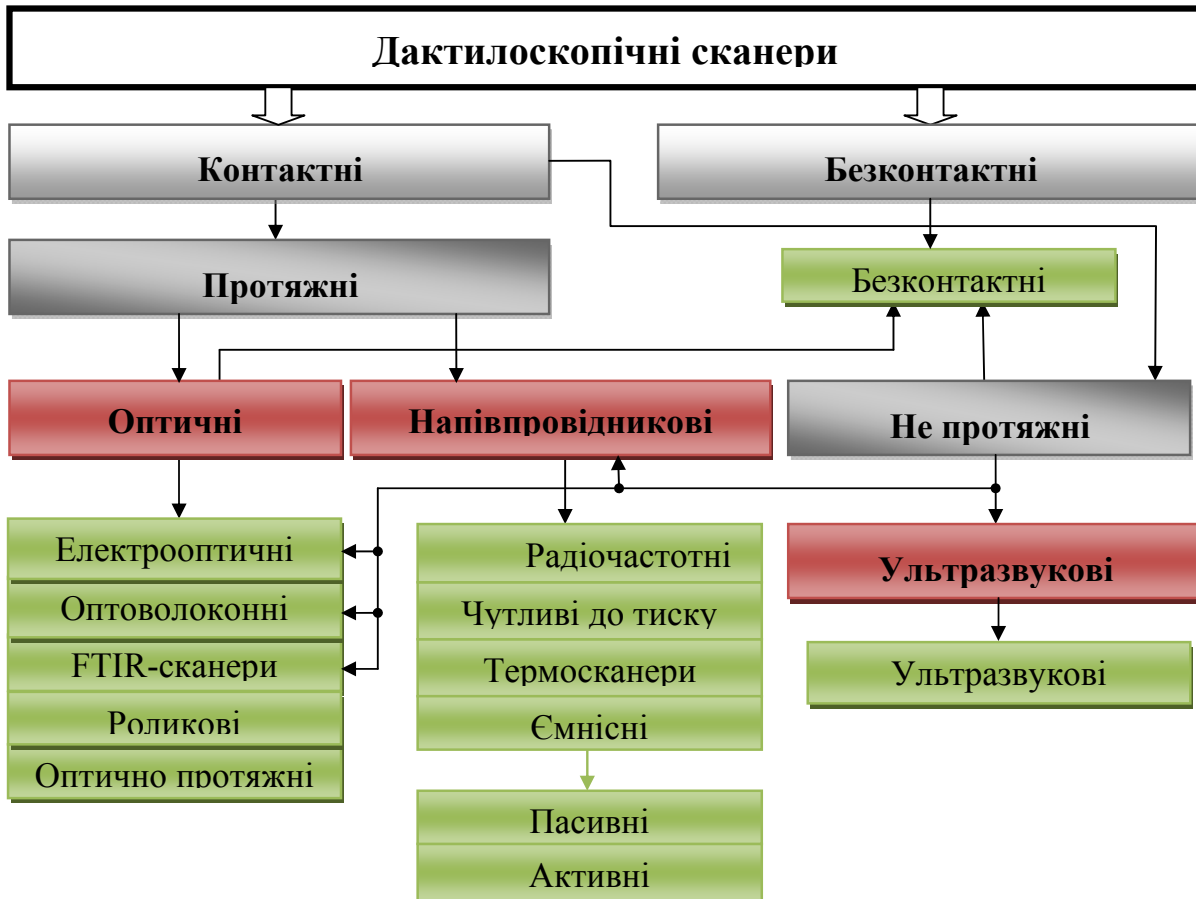


Рис. 1. Класифікація дактилоскопічних сканерів за фізичним принципом їх роботи і способом реалізації

До основних характеристик сканерів можна віднести роздільну здатність, швидкість зчитування, зносостійкість та інші параметри. На основі аналізу джерел вітчизняних і зарубіжних авторів у таблиці 1 наведено основні характеристики сканерів [9 – 17].

Основні характеристики дактилоскопічних сканерів

| Характеристика                          | Тип сканерів |               |                   |
|---|--------------|---------------|-------------------|
|   | Оптичні      | Ультразвукові | Напівпровідникові |
| Роздільна здатність (dpi)               | 500-3000     | 500           | 508               |
| Швидкість зчитування (кадр/с)           | 50-2130      | -             | 20-30             |
| Зносостійкість (млн. дотиків)           | 1-4          | -             | 1-10              |
| Розміри (мм)                            | 45 * 63 * 26 | 87*150*82     | 27*20,4* 3,5      |
| Ціна, \$                                | 130-200      |               | 20-50             |
| Імовірність допуску чужого              | $10^{-9}$    | -             | $10^{-9}$         |
| Чутливість до забруднень поверхні шкіри | висока       | низька        | низька            |

Основними виробниками оптичних сканерів є BioLink, Digital Persona, Identix; напівпровідникових – Infineon, ST-Microelectronics, Veridicom, IDEX, Atmel; ультразвукових – Ultra-Scan Corporation.

Оптичні сканери засновані на використанні оптичних методів одержання зображення. Ці сканери найбільш широко використовуються. Сьогодні існують такі технології реалізації оптичних сканерів: FTIR-сканери, оптоволоконні сканери, електрооптичні сканери, оптично протяжні сканери, роликові сканери, безконтактні сканери [8, 18 – 20].

FTIR-сканери (Frustrated Total Internal Reflection – “порушене повне внутрішнє відбиття”) працюють завдяки ефекту повного внутрішнього відбиття. Палець прикладається до скла, під яким з одного боку знаходиться джерело світла, а з іншого – камера. Світло від скла, відбиваючись, потрапляє на камеру, у тому місці, де скла торкнувся гребінь відбитка, повного внутрішнього відбиття не відбувається, і з тієї області надходить менший потік світла. Так на камеру потрапляє темний візерунок гребнів, який потім оцифровується [8, 20].

Оптоволоконні сканери складаються з оптоволокон, які, у свою чергу, складають матрицю, до якої прикладають палець. Над пальцем знаходиться сильне джерело світла, котре просвічує палець. Кожне оптоволокно закінчується фотоелементом. Якщо оптоволокна торкається гребінь, то фотоелемент сприймає світло, що проходить через палець, якщо гребеня немає, то немає і світла. Дані з фотоелементів дозволяють створити цифрове зображення [8, 18].

Електрооптичні сканери. В основі цієї технології лежить використання спеціального електрооптичного полімеру, до складу якого входить світловипромінюючий шар. Коли прикладають палець до сканера, неоднорідність електричного поля на його поверхні (різниця потенціалів між гребенями й западинами) зумовлює світіння цього шару так, що він висвічує відбиток пальця. Потім масив фотодіодів сканера перетворює це світіння в цифровий вид.

Оптично протяжні сканери в цілому аналогічні з FTIR-пристроями. Їхня особливість у тому, що палець потрібно не просто прикладати до сканера, а проводити ним по вузькій смужці-читачу. Під час руху пальця по поверхні сканера робиться серія миттєвих знімків (кадрів). При цьому сусідні кадри знімаються з деяким накладенням, тобто перекривають один одного для того, щоб точно скласти ціле зображення з кадрів. Така конструкція дозволяє значно зменшити розміри використовуваної призми й самого сканера.

Роликові сканери складаються з прозорого циліндричного ролика, усередині якого статичне джерело світла, лінза й мініатюрна камера. Сканування пальця відбувається при прокатуванні пальцем ролика. Під час руху пальця по поверхні ролика робиться серія миттєвих знімків (кадрів) фрагмента папілярного візерунка, що торкається поверхні. Після повного «прокручування» пальця, «збирається картинка» його відбитка [8].

Безконтактні сканери не потребують безпосереднього контакту пальця з поверхнею скануючого пристрою. Палець прикладається до отвору в сканері, кілька джерел світла підсвічують його знизу з різних сторін, у центрі сканера знаходиться лінза, через яку зібрана інформація проектується на КМОН-камеру, що перетворює отримані дані в зображення відбитка пальця [8, 19, 20].

Ще одним різновидом дійсно безконтактного сканера є сканер, що використовує поляризацію світла. Він працює так: руку разом з відбитками освітлюють поляризованим світлом і знімають зображення, попередньо пропустивши відбите світло через поляризаційний фільтр. Після першої зйомки фільтр повертається на  $90^0$  електродвигуном, і знову проводиться зйомка. Завдяки порівнянню двох зображень, вдається суттєво покращити контраст папілярних ліній і отримати малюнок підшкірної тканини. Перевагою цього сканера є: відсутність забруднення поверхні датчика, біологічна безпека (з погляду гігієни), можливість захисту сканера броньованим склом. Недоліком сканера є складність конструкції й досить висока ціна [21].

Перевагами оптичних сканерів відносно низька ціна; компактність. Недоліки: вони потребують постійного догляду (пил, бруд, подряпини можуть суттєво погіршити якість цифрового відбитка). Ще одним недоліком є чутливість до стану шкіри на самому пальці: жирна, суха чи потріскана шкіра можуть бути причиною розмитого зображення.

Найбільший недолік цих сканерів – слабка захищеність від муляжів та інших способів обману [8, 18 – 20].

Ультразвукове сканування — це сканування поверхні пальця ультразвуковими хвилями й вимір відстані між джерелом хвиль і западинами й гребенями на поверхні пальця за відбитою від них луною.

Перевагами цих сканерів є: зображення, отримане ними, у 10 разів краще, ніж в оптичних; такий спосіб сканування практично повністю захищений від муляжів; таке сканування, дозволяє, крім відбитка, одержувати й деякі додаткові характеристики (наприклад, пульс усередині пальця). Недоліками є висока ціна й великі розміри в порівнянні з іншими типами сканерів [8].

Напівпровідникові сканери. У їхній основі лежить використання для одержання зображення поверхні пальця властивостей напівпровідників, які змінюються в місцях контакту гребенів папілярного візерунка з поверхнею сканера. Сьогодні існує кілька технологій реалізації напівпровідникових сканерів: термосканери, сканери чутливі до тиску, емнісні і радіочастотні сканери [8, 18 – 20].

У термосканерах використовуються сенсори, які складаються з піроелектричних елементів, що дозволяють фіксувати різницю температури й перетворювати її в напругу. Під час прикладання пальця до сенсора по температурі гребенів, що торкаються піроелектричних елементів, папілярного візерунка й температури повітря, що перебуває в западинах, будується температурна карта поверхні пальця, яка згодом перетворюється в цифрове зображення [8, 18, 19].

Чутливі до тиску сканери. У цих пристроях використовуються сенсори, що складаються з матриці п'єзоелементів. Під час прикладання пальця до скануючої поверхні гребені папілярного візерунка натискають на якусь підмножину елементів поверхні, відповідно западини ніякого тиску не чинять. Матриця отриманих з п'єзоелементів напруг перетвориться в зображення поверхні пальця.

У радіочастотних сканерах використовується матриця чутливих елементів, кожен з яких працює як маленька антена. Слабкий радіосигнал направляється на поверхню пальця, що

сканується, кожен з чутливих елементів матриці приймає відбитий сигнал від папілярного малюнка. Величина наведеної в кожній антені ЕРС залежить від наявності чи відсутності над нею гребеня папілярного малюнка. Отримана матриця напруг перетворюється в цифрове зображення [8, 18, 20].

Ємнісні сканери відбитка пальця виготовляють на кремнієвій пластині, що містить область мікроконденсаторів. Існує два типи таких сканерів: пасивні (кожна комірка сенсора має лише одну із пластин конденсатора); активні (комірка сенсора містить обидві пластини конденсатора). Активний метод має такі переваги: дозволяє використати додаткові функції обробки образу відбитка, вищу стійкість до зовнішніх впливів, має більш високе відношення сигнал – шум. Близькість поверхні пальця до пластини кремнію дозволяє реєструвати електричні імпульси, що виникають під час скорочень серця. Використання цієї особливості дозволяє ефективно протидіяти муляжам [8, 19, 20, 22].

Усі вищенаведені напівпровідникові сканери мають протяжні варіанти, що робить меншими їхні геометричні розміри й ціну.

Перевагою напівпровідникових сканерів є: малі габарити; висока точність отриманого зображення, яка не залежить від стану шкіри; отримання якісних відбитків навіть у тому разі, якщо палець забруднений.

Недоліками сканерів є: необхідність прикладання пальця безпосередньо до напівпровідникової поверхні (будь-який проміжний шар впливає на результати сканування), що веде до швидкого зношування сенсора сканера; висока чутливість до сильних зовнішніх електричних полів; чутливість до вібрацій і ударів [8, 18 – 20].

### Висновки

У статті проаналізовано основні методи дактилоскопічного сканування й наведено конструкції основних існуючих типів сканерів, вказано їхні переваги і недоліки. Встановлено, що основна проблема сьогодні, яка виявилася під час масового використання дактилоскопічних сканерів, – слабка захищеність від муляжів. Тому найбільш перспективним напрямком подальших розробок є сканери з реєстрацією біологічних ознак живого організму. До таких сканерів, насамперед належать напівпровідникові ємнісні й термосканери.

### СПИСОК ЛІТЕРАТУРИ

1. Общая характеристика биометрических технологий. Основные группы биометрических идентификаторов и технологий [Електронний ресурс] // ООО Биолінк Солюшенс, 2007. Режим доступу: <http://www.biolink.ru/technology/biometric.php>
2. Рынок биометрии будет каждый год расти на четверть [Електронний ресурс] // Security News : Информационно-аналитическое издание по техническим средствам и системам безопасности. Режим доступу: <http://www.secnews.ru/foreign/15660.htm>
3. Обзор биометрических технологий [Електронний ресурс]: Прогноз финансовых рисков 2000 – 2009. / В. Задорожный // Режим доступу: <http://www.bre.ru/security/20234.html>
4. Идентификация по отпечаткам пальцев. Часть 2 [Електронний ресурс]: Прогноз финансовых рисков 2000 – 2009. / В. Задорожный // PC Magazine/Russian Edition №2, 2004. Режим доступу: <http://www.bre.ru/security/21052.html>
5. Биометрия: итоги и ожидания [Електронний ресурс]: ООО Биолінк Солюшенс, 2007 – 2010. / А. Арсентьев // Режим доступу: <http://www.biolink.ru/technology/newss/4124/>
6. Немецкие хакеры грозят «пальцем» [Електронний ресурс]: Франкфурт-на-Майне. / К. Куц // Режим доступу: <http://vz.ru/society/2008/4/2/156615.html>
7. Система физической идентификации по отпечаткам пальцев Sagnier [Електронний ресурс]: Nicsaworld S.A. 2005. // Режим доступу: <http://www.nicsaworld.com/pdf/FIngrus.pdf>
8. Идентификация по отпечаткам пальцев. Часть 1 [Електронний ресурс]: Прогноз финансовых рисков 2000 – 2009. / В. Задорожный // PC Magazine / Russian Edition №2, 2004. Режим доступу: <http://www.bre.ru/security/20994.html>
9. Биометрическая идентификация по отпечаткам пальцев. Технология Finger Chip [Електронний ресурс] / О. Гуреева // Компоненты и технологии №4, 2007. Режим доступу: [http://www.kit-e.ru/articles/rfid/2007\\_4\\_176.php](http://www.kit-e.ru/articles/rfid/2007_4_176.php)

10. Сканер отпечатков пальцев Authentec AES1711 [Електронний ресурс] // Виробник Authentec. Режим доступу: <http://www.authentec.com/products-wireless-aes1711.cfm>
11. Сканер отпечатков пальцев BioLink U-Match 3.5 [Електронний ресурс] // Виробник BioLink. Режим доступу: <http://biolink.ru/products/scanners/>
12. Lock LH9-3 [Електронний ресурс] // Виробник ADEL. Режим доступу: [http://www.adellock.com/en/product\\_show.asp?id=66](http://www.adellock.com/en/product_show.asp?id=66)
13. Датчик отпечатков пальцев SMARTFINGER® IX 10-4 [Електронний ресурс] // Виробник IDEX. Режим доступу: [www.idex.no](http://www.idex.no)
14. Fingerprint Sensor FPC1011F [Електронний ресурс] // Fingerprint. Режим доступу: [http://www.fingerprint.se/en/Products/All%20products%20overview.aspx?sc\\_lang=en](http://www.fingerprint.se/en/Products/All%20products%20overview.aspx?sc_lang=en).
15. Product Specifications TCS5 TouchStrip® Fingerprint Sensor (TCEEA4 (TCS4C+TCD50A)) [Електронний ресурс] // Upek. Режим доступу: <http://www.upek.com/solutions/productfinder/>
16. AuthenTec Fingerprint Sensors AES2660 [Електронний ресурс] // Authentec. Режим доступу: <http://www.authentec.com/products-pesandperipherals.cfm>.
17. Сканер отпечатков пальцев Model [Електронний ресурс] // Виробник Ultra-scan. Режим доступу: <http://www.ultra-scan.com/Default.aspx?tabid=496>.
18. Введение в биометрию [Електронний ресурс] // ООО «н-Тегрити». Режим доступу: <http://www.n-trance.ru/?area=5&block=5>.
19. Биометрические технологии [Електронний ресурс] / М. Давлетханов // Р Контроль системы безопасности. Режим доступу: <http://www.r-control.ru/articles/8/>
20. Аппаратная реализация методов идентификации по отпечаткам пальцев [Електронний ресурс] / О. Никулин // Специальная Техника. – 1999 г. – №3. Режим доступу: <http://ess.ru/publications/articles/nikulin/nikulin.htm>.
21. Патент 67772 України МПК 7G06K9/20, A61B5 / 117. Спосіб та пристрій для ідентифікації особи шляхом безконтактного розпізнавання ліній руки і пальців / Хауке Рудольф, DE, Айнґхаммер Хайнс Й., DE, Айнґхаммер Йенс, DE., заявник і патентовласник – ТСТ-ТАЧЛЕСС СЕНСОР ТЕКНОЛОДЖИ СЕЙЛЗ ЕНД МАРКЕТИНГ АГ, СН – опубл. 15.07.2004, Бюл. №7, 2004 р.
22. Современные технологии идентификации личности по отпечатку пальца с использованием емкостных датчиков [Електронний ресурс] / Г. Рябов // Radioradar. Режим доступу: [http://www.radioradar.net/articles/scientific\\_technical/identif\\_otpech.html](http://www.radioradar.net/articles/scientific_technical/identif_otpech.html).

**Білинський Йосип Йосипович** – д. т. н., професор, завідувач кафедри електроніки.

**Юкиш Марина Йосипівна** – к. т. н., кафедра теоретичної електротехніки та електричних вимірювань.

**Павлюк Олександр Анатолійович** – студент.  
Вінницький національний технічний університет.