УДК 57. 001

А.О. МОРОЗ

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ. МЕТОДИ ДАКТИЛОСКОПІЇ

Анотація. *У статті представлено загальний опис внутрішніх особливостей методів дактилоскопії, що набули найбільшого поширення біометричної технології. Детально розглянуті методи розпізнавання рисунка пальця та конфігурації приладів для їх здійснення.*
Ключові слова: *біометрія, біометричні технології, відбиток пальця, дактилоскопія, алгоритм розпізнавання.*

Аннотация. *В статье представлено общее описание внутренних особенностей методов дактилоскопии, которые получили наибольшее распространение в биометрических технологиях. Подробно рассмотрены методы распознавания рисунка пальца и конфигурации приборов для их осуществления.*
Ключевые слова: *биометрия, биометрические технологии, отпечаток пальца, дактилоскопия, алгоритм распознавания.*

Abstract. *The article covers the description of internal features that have become widely spread in biometric technology. The methods of fingerprint identification and configuration of equipment for the implementation of these methods are being described in details.*
Keywords: *biometrics, fingerprint, dactylography, recognition algorithm.*

1. Вступ

Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об'єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; системи електронної комерції; інформаційна безпека (доступ у мережу, вхід на ПК); облік робочого часу і реєстрація відвідувачів; системи голосування; проведення електронних платежів; аутентифікація на web-ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (перетин державних кордонів, видача віз на відвідини країни) і т.д.

Традиційні системи доступу (код, магнітна картка) мають один загальний недолік: засіб ідентифікації може бути використаний будь-якою особою, оскільки подібна система ідентифікує наявність відповідного «ключа», а не конкретної особи. Ідентифікаційний код може бути записаний, вкрадений, переданий; ідентифікаційна картка може бути втраченою, скопійованою і т.д. – все це залишає широке поле для отримання доступу неавторизованими особами.

Біометричні системи контролю доступу позбавлені цього недоліку, оскільки для ідентифікації особи використовують унікальні властивості самої особи, яку необхідно ідентифікувати. На сьогоднішній день біометричними системами, що виявилися найбільш потрібними, є системи ідентифікації класу AFIS (Automated Fingerprint Identification Biometric System – автоматична система ідентифікації за відбитком пальця), а також системи класу APFIS (Automated Palmprint and Fingerprint Identification Biometric System – автоматична система біометричної ідентифікації за формою долоні і відбитками пальців).

Діяльність приватних фірм, урядових організацій і лабораторій, які займаються питаннями біометрії, координується Біометричним Консорціумом BIOAPI Consortium. Провідними виробниками біометричних систем є: Biolink Technologies, Bioscrypt, Precise Biometrics, Neurotechnologiya, Digitalpersona, Ethentica, Identix, Staflink, Veridicom та ін. Враховуючи те, що основні біометричні технології розробляються й удосконалюються за кордоном, актуальним є створення власних біометричних технологій з метою ліквідації

прірви, що утворилася, в розробці біометричних систем між вітчизняними і зарубіжними виробниками і подальшого паралельного (а, можливо, і спільного) вдосконалення біометричних систем. У результаті власні розробки будуть як мінімум на порядок дешевше. При цьому ідентифікація особи за відбитком пальця є найвдалішою біометричною технологією завдяки простоті використання, зручності і надійності. Вірогідність помилки при ідентифікації користувача за відбитками пальців набагато менше порівняно з іншими біометричними методами. Крім того, сам пристрій ідентифікації за відбитком пальця малогабаритний і прийнятний за ціною [1].

2. Біометричні системи за відбитком пальця

Дактилоскопія – метод ідентифікації людини за відбитками пальців, заснований на унікальності рисунка шкіри.

Об'єктом дослідження в даній статті виступає зображення відбитка пальця. Унікальність кожного відбитка пальця можна визначити за узором, який утворюють виступи і борозенки, а також за іншими його деталями. Таким чином, у кожному відбитку пальця можна визначити два типи ознак:

1. Глобальні:

• папілярний узор – специфічний узор, що формується сукупністю виступів і западинок;

• виступ – лінія відбитка пальця підноситься і утворює виступ;

• западинка (борозенка) – жолобок між виступами;

• центр (ядро) – пункт, локалізований у середині відбитка або у деякій виділеній області; точка найбільшої кривизни виступу;

• дельта – зона, де виступ розгалужується на три лінії, а потім вони сходяться в одній точці;

• область інтересу – виділений фрагмент відбитка, в якому локалізовані всі ознаки (як правило, центральна область відбитка пальця).

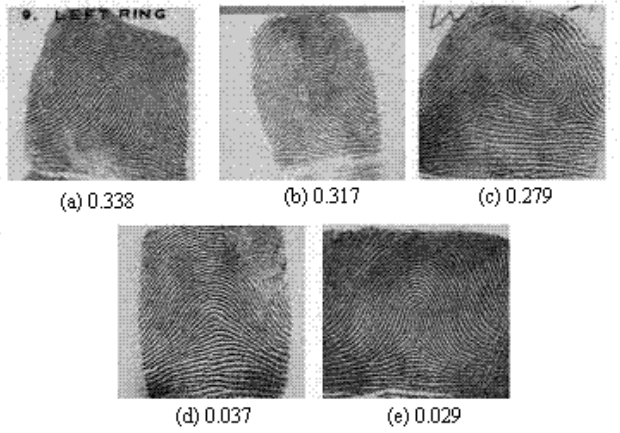

Рис. 1. Основні класи відбитків пальців з урахуванням натурального розподілу: a) ліва петля, b) права петля, c) завиток, d) дуга, e) півсфера

У традиційній дактилоскопії папілярні узори пальців рук діляться на три основні класи: дугові (близько 5% усіх відбитків), петлеві (65%) і завиткові (30%); для кожного класу проводиться детальніша класифікація на підкласи. Виділяються основні п'ять класів: завиток (W), права петля (R), ліва петля (L), дуга (A) і півсфера (T) (рис. 1) [2].

2. Локальні – це унікальні для кожного відбитка ознаки, що визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розриви і т.д.), орієнтацію папілярних ліній і координати в цих пунктах. Кожен відбиток містить до 70 деталей.

Стандарти на відбитки пальців

В основному використовуються стандарти ANSI і ФБР США. У них визначені такі вимоги до способу відбитка:

• кожен образ представляється у форматі нестисненого TIF;

• образ повинен мати дозвіл не нижче 500 dpi;

• образ повинен бути напівтоновим з 256 рівнями яскравості;

• максимальний кут повороту відбитка від вертикалі не більше 15 градусів;

• основні типи мінуцій: закінчення і роздвоєння.

Звичайно в базі даних зберігають більше, ніж один образ, що дозволяє поліпшити якість розпізнавання. Образи можуть відрізнятися один від одного зрушенням і поворотом. Масштаб не змінюється, тому що всі відбитки отримують з одного пристрою.

Відбиток, отриманий за допомогою спеціального сканера, датчика або сенсора, перетворюється в цифровий код і порівнюється з раніше введеним еталоном.

Переваги доступу за відбитком пальця – простота використання, зручність і надійність. Процес ідентифікації триває секунди і не вимагає зусиль. Сам пристрій займає мало місця. Але ідентифікація за відбитком пальця має один недолік. Приблизно у 1% людей пальці не можуть бути оброблені біометричною системою. Тобто, у них або немає відбитків, або вони мають такий вигляд, який неможливо перетворити в цифровий код.

Проблема пошкодження (поріз, опік) пальця вирішується просто. Якщо пошкодження не носить «складний» характер (папілярний узор відновлюється повністю), тоді систему необхідно лише "переучити" розпізнавати палець. На випадок, якщо палець пошкоджений серйозно, як правило, реєструється «резервний» відбиток (один або декілька, інколи для простоти реєструються відразу всі відбитки).

Біометричні системи, які використовують для розпізнавання відбиток пальця, найпоширеніші. Про це свідчить і кількість компаній-розробників: США – ATMEL, Digitalpersona Inc., Cross Match Technologies, Ethentica by Security First Corp., Biolink Technologies, Iridian Technologies Inc., Identix Inc., Sagem Morpho, Veridicom, Infineon, Bioscrypt, Secugen Corporation, Швеція – Precise Biometrics, Угорщина – Guardware Systems Ltd., Росія – ЦентрІнвест Софтвер SCANTI-RUS, Системи Папілон.

Пристрої для прочитування відбитків пальців знаходять різне застосування. Їх встановлюють на ноутбуки, в миші, клавіатури, флешки, а також застосовують у вигляді окремих зовнішніх пристроїв і терміналів, що продаються в комплекті з системами AFIS (Automated fingerprint identification systems – системи автоматизованої ідентифікації відбитків пальців).

Не дивлячись на зовнішні відмінності, всі сканери можна розділити на декілька видів.

Оптичні:

– ftir-сканери (рис. 2).

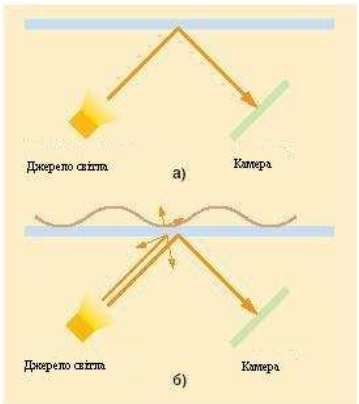

Рис. 2. Принцип роботи FTIR-сканерів

При падінні світла на кордон розділу двох середовищ світлова енергія ділиться на дві частини: одна відбивається від кордону, інша – проникає через кордон розділу в друге середовище. Доля енергії, що відбивається, залежить від кута падіння. Починаючи з деякої його величини, вся світлова енергія відбивається від кордону розділу. Це явище називається повним внутрішнім віддзеркаленням. Проте при контакті щільнішого оптичного середовища (у нашому випадку – поверхня пальця) з менш щільним (у практичній реалізації, як правило, поверхня призми) в точці повного внутрішнього віддзеркалення пучок світла проходить через цей кордон. Таким чином, від кордону відіб'ються лише пучки світла, що попали в такі точки повного внутрішнього віддзеркалення, до яких не були прикладені борозенки папілярного узору поверхні пальця. Для фіксації світлової картинки поверхні пальця використовується спеціальна камера (ПЗС або КМОП залежно від реалізації сканера);

– оптоволоконні (fiber optic scanners).

Являють собою оптоволоконну матрицю, кожне з волокон якої закінчується фотоелементом. Чутливість кожного фотоелемента дозволяє фіксувати залишкове світло, що

проходить через палець, у точці дотику рельєфу пальця до поверхні сканера. Зображення відбитка пальця формується за даними кожного з елементів;

– оптичні протяжні (sweep optical scanners).

У цілому вони аналогічні FTIR-пристроям. Їх особливість у тому, що палець потрібно не просто прикладати до сканера, а проводити ним по вузькій смужці-зчитувачу. При русі пальця по поверхні сканера робиться серія миттєвих знімків (кадрів). При цьому сусідні кадри знімаються з деяким накладенням, тобто перекривають один одного, що дозволяє значно зменшити розміри використовуваної призми і самого сканера. Для формування зображення відбитка пальця під час його руху по скануючій поверхні використовується спеціалізоване програмне забезпечення;

– роликові (roller-style scanners);

– безконтактні напівпровідникові.

В основі безконтактних напівпровідників для отримання зображення поверхні пальця лежить використання властивостей напівпровідників, що змінюються в місцях контакту гребенів папілярного узору з поверхнею сканера:

a) ємкісні (capacitive scanners);

b) чутливі до тиску (pressure scanners);

c) термо-сканери (thermal scanners);

d) радіочастотні (RF-Field scanners);

e) протяжні термо-сканери (thermal sweep scanners);

f) ємкісні протяжні (capacitive sweep scanners);

g) радіочастотні протяжні (RF-Field sweep scanners);

– ультразвукові (рис. 3).

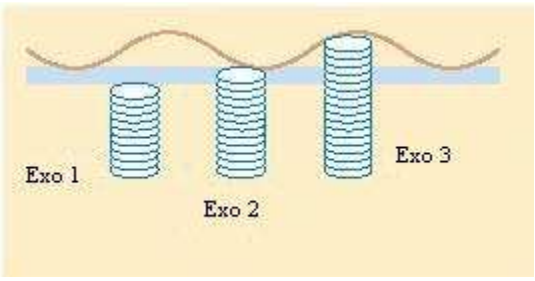

Рис. 3. Схема роботи ультразвукового сканера (Exo 1, Exo 2 – виявлено виступ, Exo 3 – виявлена впадина)

Сканування поверхні пальця ультразвуковими хвилями і вимір відстані між джерелом хвиль, западинами і виступами на поверхні пальця за відбитій від них exo-камері. Якість отримуваного в такий спосіб зображення в 10 разів краща, ніж отриманого будь-яким іншим, представленим на біометричному ринку, методом. Крім цього, слід зазначити, що даний спосіб практично повністю захищений від муляжів, оскільки дозволяє, крім відбитка пальця, отримувати і деякі додаткові характеристики про його стан (наприклад, пульс всередині пальця).

Слід зазначити, що між дактилоскопуванням (зняттям відтисків з пальців) і скануванням є істотна різниця. Вона полягає не в тому, що при скануванні відбувається автоматизація всього процесу, а в тому, що при скануванні відбитків пальців, замість збереження повного зображення папілярного узору, зберігається лише інформація про декілька характерних точок папілярного узору. Причому відновити повний образ відбитка пальця за збереженою інформацією неможливо. Остання обставина стала вирішальним чинником для широкого поширення сканування відбитків пальців серед цивільного населення [3].

ZKSoftware

Система будується на базі терміналів Zksoftware. Термінали можуть об'єднуватися в мережу по інтерфейсах Rs485, Ethernet. База відбитків пальців і права доступу зберігаються у внутрішній пам'яті терміналів, що дозволяє також працювати в автономному режимі (без зв'язку з комп'ютером).

У загальному випадку до терміналів під’єднуються: електрозамки, зчитувачі, кнопки виходу, геркони, дзвінки, домофони, аларми.

Рис. 4. Зчитувач відбитків пальця Zk4000

Програмне забезпечення: монітор реального часу, завантаження/вивантаження відбитків, записів, інформації про користувачів, відображення на екрані фото після проходу, віддалене (дистанційне) управління дверима.

Zk4000 (рис. 4) – зчитувач відбитків пальця. Пристрій знімає знімок відбитка пальця і передає його в комп'ютер по інтерфейсу USB. Пристрій сумісний з безліччю операційних систем сімейства Windows, у тому числі Windows 2000, XP, Vista, і Windows 7. Пристрій може бути легко інтегрований у системи, що розробляються. Продукт набув широкого вжитку в соціальній сфері, суспільній безпеці, додатках обліку робочого часу, шифруванні з використанням відбитка пальця, вбудовуваних системах, а також в інших галузях [4].

Virdi

Біометричні системи контролю і управління доступом. Основним елементом системи є біометричні термінали VIRDI (доступ за відбитком пальця і безконтактними картами), до яких підключаються електромеханічні замки, клямки. Температура експлуатації від -20 градусів за Цельсієм.

Системи VIRDI працюють як окремо (для однієї точки проходу), так і в мережевому режимі (TCP/IP мережі), під управлінням спеціального програмного забезпечення.

База відбитків пальців може зберігатися в самому терміналі або в комп'ютерній базі даних [5].

BioSmart

Система контролю і управління доступом (СКУД) Biosmart є мережевою, розподіленою системою, з розмежуванням прав доступу користувачів, при необхідності збільшення їх кількості, відкритою для інтеграції у пристрої інших виробників. Мережа будується з використанням інтерфейсу Rs485, виділених ліній зв'язку Ethernet, що вже існують на підприємстві, або стільникових мереж формату GSM. Контроллери Biosmart об'єднуються в магістраль Rs485 (до 255 шт.). Для підключення до ПК застосовуються перетворювачі інтерфейсів Usbrs485, Lanrs485.

Рис. 5. Ekey lock

Ekey (рис. 5)

Заснована в 2002 році, Ekey сьогодні є компанією №1 в Європі в галузі біометричних систем доступу за відбитками пальців.

Ekey lock – цифрові циліндри, поєднані з біометричними системами за відбитками пальців Ekey. Спрацьовування механізму циліндра відбувається по радіоканалу. Циліндр повністю автономний і обладнаний елементами живлення. До 30 000 циклів автономної роботи.

3. Методи розпізнавання малюнка пальця

Залежно від якості отриманого із сканера зображення відбитків пальців можна виділити деякі характерні ознаки поверхні пальців, які надалі будуть використовуватись в цілях ідентифікації.

На найпростішому технічному рівні, наприклад, якщо дозвіл отриманого із сканера зображення складає 300–500 dpi, на зображенні поверхні пальця можна виділити чималу кількість дрібних деталей (minutiae), по яких можна їх класифікувати, але, як правило, в автоматизованих системах використовують усього два типи деталей узору (особливих точок) [6–8]:

- кінцеві точки – точки, в яких «виразно» закінчуються папілярні лінії;
- точки галуження – визначаються як точки, в яких папілярні лінії роздвоюються.

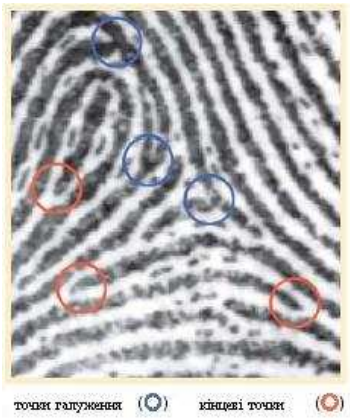

Рис. 6. Кінцеві точки та точки розгалуження


Рис. 7. Внутрішня будова папілярних ліній

На рис. 6 наведений приклад, на якому явно видно, що з себе представляють кінцеві точки і точки галуження.

Якщо є можливість отримати зображення поверхні пальця із роздільною здатністю, близькою до 1000 dpi, на ньому можна виявити деталі внутрішньої будови самих папілярних ліній, зокрема, пори потових залоз (рис. 7) (порожніми кільцями відмічені пори, чорними точками відмічені кінцеві точки і точки галуження) і відповідно використовувати їх розташування в цілях ідентифікації. Проте цей метод мало поширений через складність отримання зображень такої якості в нелабораторних умовах.

В автоматизованому розпізнаванні відбитків пальців, на відміну від традиційної дактилоскопії, виникає значно менше проблем, пов'язаних з різними зовнішніми чинниками, що впливають на сам процес розпізнавання. При отриманні відбитків пальців фарбованим способом (за допомогою відкатки) важливо виключити або, принаймні, максимально зменшити зсув або поворот пальця, зміну тиску, зміну якості поверхні шкіри і т.д.

З електронних безфарбових сканерів отримати зображення відбитка пальця з достатньою для обробки якістю істотно простіше.

Практика показує, що відбитки пальців різних людей можуть мати однакові глобальні ознаки, але абсолютно неможлива наявність однакових деталей. Тому глобальні ознаки використовують для розділення бази даних на класи і на етапі аутентифікації. На другому етапі розпізнавання (унікальна ідентифікація) використовують вже локальні ознаки.

У даний час виділяють такі класи алгоритмів порівняння відбитків пальців:

За локальними ознаками:

Етап 1. Поліпшення якості вихідного зображення відбитка. Збільшується різкість кордонів папілярних ліній.

Етап 2. Обчислення поля орієнтації папілярних ліній відбитка. Зображення розбивається на квадратні блоки зі стороною більше 4 пікселів, і по градієнтах яскравості обчислюється кут t орієнтації ліній для фрагмента відбитка.

Етап 3. Бінаризація зображення відбитка. Приведення до чорно-білого зображення (1 bit) порогової обробки.

Етап 4. Потоншення ліній зображення відбитка. Потоншення проводиться до тих пір, поки лінії не будуть шириною 1 піксель.

Етап 5. Виділення мінуцій. Зображення розбивається на блоки 9x9 пікселів. Після цього підраховується число чорних (ненульових) пікселів, що знаходяться навколо центра. Пікселем у центрі вважається мінуція, якщо він сам ненульовий, а сусідніх ненульових пікселів один (мінуція «закінчення») або два (мінуція «роздвоєння»).

Координати виявлених мінуцій і їхні кути орієнтації записуються у вектор: $W(p)=[(x1,\ y1,\ t1),\ (x2,\ y2,\ t2)...(xp,\ yp,\ tp)]$ (p – число мінуцій). При реєстрації користувачів цей вектор вважається еталоном і записується в базу даних. При розпізнаванні вектор визначає поточний відбиток (що цілком логічно).

Етап 6. Зіставлення мінуцій.

Два відбитка одного пальця будуть відрізнятися один від одного поворотом, зміщенням, зміною масштабу і / або площею дотику у залежності від того, як користувач прикладає палець до сканера. Тому не можна сказати, чи належить відбиток даній людині, чи

ні, на підставі простого їх порівняння (вектори еталона та поточного відбитка можуть відрізнятися по довжині, містити невідповідні мінуції і т.д.). Через це процес зіставлення повинен бути реалізований для кожної мінуції окремо.

Етапи порівняння:

• реєстрація даних;

• пошук пар відповідних мінуцій;

• оцінка відповідності відбитків.

При реєстрації визначаються параметри афінних перетворень (кут повороту, масштаб і зрушення), при яких деяка мінуція з одного вектора є певною мінуцією з другого.

При пошуку для кожної мінуції потрібно перебрати до 30 значень повороту (від -15 градусів до +15), 500 значень зсуву (від -250 пкс до +250 пкс) і 10 значень масштабу (від 0,5 до 1,5 з кроком 0,1). Разом до 150 000 кроків для кожної з 70 можливих мінуцій. На практиці всі можливі варіанти не перебираються. Після підбору потрібних значень для однієї мінуції їх намагаються підставити і до інших мінуцій, інакше було б можливо зіставити практично будь-які відбитки один одному.

Оцінка відповідності відбитків виконується за формулою K = (D * D * 100%) / (p * q), де D – кількість мінуцій, що збігаються, p – кількість мінуцій еталону, q – кількість мінуцій ідентифікованого відбитка. У випадку, якщо результат перевищує 65%, відбитки вважаються ідентичними (поріг може бути знижений виставленням іншого рівня пильності).

Якщо виконувалась аутентифікація, то на цьому процес закінчується. Для ідентифікації необхідно повторити цей процес для всіх відбитків у базі даних (потім вибирається користувач, у якого найбільший рівень відповідності (зрозуміло, його результат має бути вищим за поріг 65%)).

Кореляційне порівняння – два зображення відбитка пальця накладаються одне на одне, і підраховується кореляція (по рівню інтенсивності) між відповідними пікселями, обчислена для різних вирівнювань зображень один відносно одного (наприклад, шляхом різних зсувів і обертань) (рис. 8). За відповідним коефіцієнтом приймається рішення про ідентичність відбитків. Внаслідок складності і тривалості роботи даного алгоритму, особливо при вирішенні завдань ідентифікації (порівняння «один-до-багатьох»), системи, побудовані з його використанням, зараз практично не використовуються [9, 10].

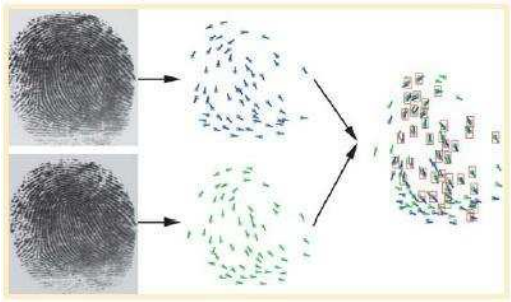

Рис. 8. Кореляційне порівняння

Порівняння по особливих точках – по одному або декількох зображеннях відбитків пальців із сканера формується шаблон, що є двовимірною поверхнею, на якій виділені кінцеві точки і точки галуження. При порівнянні на відсканованому зображенні відбитка також виділяються ці точки, карта їх точок порівнюється із шаблоном, і по кількості точок, що збіглися, приймається рішення про ідентичність відбитків (рис. 9).

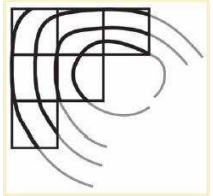

Рис. 9. Визначення ідентичності відбитків

Завдяки простоті реалізації і швидкості роботи алгоритми даного класу є найбільш поширеними. Єдиним істотним недоліком даного методу порівняння є досить високі вимоги до якості отриманого зображення (близько 500 dpi) [9–11].

Порівняння за узором – у даному алгоритмі порівняння використовує безпосередньо особливості будови папілярного узору на поверхні пальців. Отримане зі сканера зображення відбитка пальця розбивається на безліч дрібних вічок, як показано на рис. 9.

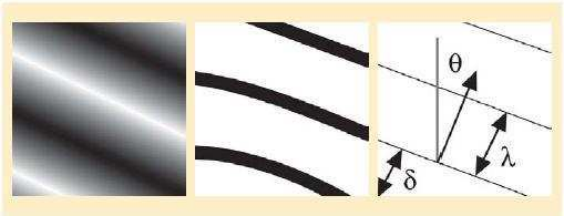

Рис. 10. Синусоїдальна хвиля розташування ліній

Розташування ліній у кожному вічку описується параметрами синусоїдальної хвилі (рис. 10), тобто, задаються початкове зрушення фази (δ), довжина хвилі (λ) і напрям її поширення (θ).

Спеціальний модуль розглядає папілярні лінії в квадратиках по черзі, і кожен з них описує рівнянням синусоїдальної хвилі, тобто встановлює початкове зрушення фази, довжину хвилі і напрям її поширення. Саме ці дані і використовуються для ідентифікації: у базі даних еталонів зберігаються параметри всіх відрізань горбків у кожній області. Потім порівнюються параметри хвилевих представлень відповідних вічок еталонного зображення і зображення, отриманого при скануванні.

Перевагою алгоритмів цього класу є те, що дані алгоритми порівняння не потребують отримання зображення високої якості [9–11].

На жаль, метод порівняння за узором відбитка пальця поки не набув широкого застосування. Даний метод дуже складний для реалізації і вимагає солідної математичної бази. Лише небагато компаній узяли на озброєння подібний підхід.

4. Висновки

У даній статті було представлено загальний опис внутрішніх особливостей, що набули найбільшого поширення у технологіях дактилоскопії. За межами статті залишилося ще дуже багато аспектів побудови систем, заснованих на автоматизованому розпізнаванні людини за відбитками пальців, такі як обробка і нормалізація зображень, особливості побудови корпоративних мережевих систем, сервери біометричної аутентифікації, види атак на біометричні системи і способи захисту від них і т.д., кожна з яких є окремою темою для масштабного дослідження. Розпізнавання за відбитками пальців стає цікавим у світлі запланованих у найближчі декілька років реформ відносно українських, закордонних і внутрішніх паспортів і вже впроваджуваних у деяких країнах правил в'їзду за візами, що містять біометричні дані і, в першу чергу, відбитки пальців.

СПИСОК ЛІТЕРАТУРИ

1. Биометрия или Сам себе идентификатор. – Режим доступа: http://www.artkis.ru/biometria.php.
2. Handbook of Fingerprint Recognition / D. Maltoni, D. Maio, A.K. Jain [et al.]. – New York: Springer, 2003. – P. 811 – 814.
3. http://www.ekeyrus.ru.
4. http://www.zk-software.ru.
5. http://www.virdi-software.com.
6. Задорожный В. Идентификация по отпечаткам пальцев. Ч. 1 [Электронный ресурс] / В. Задорожный // PC Magazine/Russian Edition. – 2004. – N 1. – Режим доступа: http://bre.ru/security/20994.html.
7. Давлетханов М. Способы идентификации по отпечаткам пальцев [Электронный ресурс] / М. Давлетханов. – 2004. – Режим доступа: http://www.infobez.ru/article.
8. Jain A.K. A Multichannel Approach to Fingerprint Classification"// A.K. Jain, S. Prabhakar, L. Hong // IEEE transactions on pattern analysis and machine intelligence. – 1999. – Vol. 21, N 4. – P. 348 – 359.
9. Задорожный В. Идентификация по отпечаткам пальцев. Ч. 2 [Электронный ресурс] / В. Задорожный // PC Magazine/Russian Edition. – 2004. – N 2. – Режим доступа: http://bre.ru/security/21052.html.
10. Зиятдинов А.И. Принципы построения систем биометрической аутентификации / Зиятдинов А.И. – М.: МФТИ, 2005. – 8 с.
11. Кухарев Г.А. Материалы из монографии "Биометрические системы" / Кухарев Г.А. – СПб.: Политехника, 2001. – 240 с.

Стаття надійшла до редакції 11.05.2011