УДК 681.325.5

О.З. Готра[1], Н.В. Дорош[2], Г.Л. Кучмій[2]
[1] Львівський національний медичний університет
імені Данила Галицького,
[2] Національний університет "Львівська політехніка",
кафедра електронних приладів

АНАЛІЗ СУЧАСНИХ ЕЛЕКТРОННИХ ЗАСОБІВ ДЛЯ БІОМЕТРІЇ

Проаналізовано сучасний стан та перспективи розвитку електронних біометричних засобів для ідентифікації особи. Описано узагальнений алгоритм проведення ідентифікації особи з використанням статичних та динамічних біометричних характеристик (БМХ) людини та структурну організацію таких систем. Розглянуто приклади та будову сенсорних пристроїв, які використовують для реєстрації дактилоскопічних БМХ людини.

The analysis of a modern state and prospects of development of electronic biometric equipments for personal identification is carried out. The generalized algorithm of realization of personal identification with use of the static and dynamical biometric characteristics (BMC) and structural organization of such systems are described. The examples and structure of sensor devices, which are used for registration of dactiloscopic BMC of the person are considered.

Під час розроблення сучасних систем захисту об'єктів та інформації від несанкціонованого доступу активно впроваджують біометричні технології.

Застосування пристроїв, створених на базі методів біометричної ідентифікації особи, дає змогу покращити надійність таких систем захисту та зробити їх зручнішими для користувача.

Основними завданнями автоматизованих біометричних систем є

– реєстрація біометричних параметрів (характеристик) особи за допомогою сенсорних пристроїв (1);

– формування вибірки біометричних даних (2);

– формування ознак ідентифікації (3);

– порівняння біометричних даних особи з еталонними персоніфікованими даними – аналіз (4);

– прийняття рішення про відповідність порівнювальних біометричних параметрів особи вимогам (персоніфікованому еталону) (5);

– формування рішення про надання доступу (досягнення ідентифікації), або повторення процедури ідентифікації, або відмова у доступі (6).

Узагальнений алгоритм ідентифікації особи на основі аналізу біометричних характеристик (БМХ) особи показано на рис. 1.

Біометричні характеристики людини поділяють на статичні (відбитки пальців, геометрія кисті руки, термограма кисті руки, сітківка та рогівка ока, форма та термограма обличчя, вуха, ДНК тощо) та динамічні (голос, рукописний та машинний почерк) [1].

Серед всіх біометричних характеристик найчастіше використовують дактилоскопічні параметри (видбитки пальців), які реєструють за допомогою дактилоскопічних давачів різного типу. Передавання даних від давачів у пристрій ідентифікації виконується через послідовний (SPI, USB) або паралельний порт (безпосередньо або з попереднім шифруванням). Для збереження персоніфікованих відбитків пальців використовують пам'ять типу DRAM, ROM, FLESH. Завдання перетворення інформації в цифровий код, порівняння та аналізу прийнятих даних та прийняття рішення про ідентифікацію виконують мікропроцесорні схеми. Прикладом такої високоінтегро-

ваної системи ідентифікації є система FI -710 (SONY), яка забезпечує ймовірність помилкових підтверджень незареєстрованих користувачів False-Reiect Rate (FAR) ≤ 0. 008 %, ймовірність помилкових відмовлень зареєстрованих користувачів False Acceptance Rate (FRR) ≤ 3. 99%, середній час ідентифікації ≤ 1с [2].

Система FI-710 має вбудований криптографічний співпроцесор і працює в середовищі операційної системи Windows усіх модифікацій. Давач відбитка пальця фірми Sony має такі параметри: розмір пікселя 80×80 мікрон, формат матриці 128×192 пікселя, розмір давача 10.2×15.4 мм. [2].

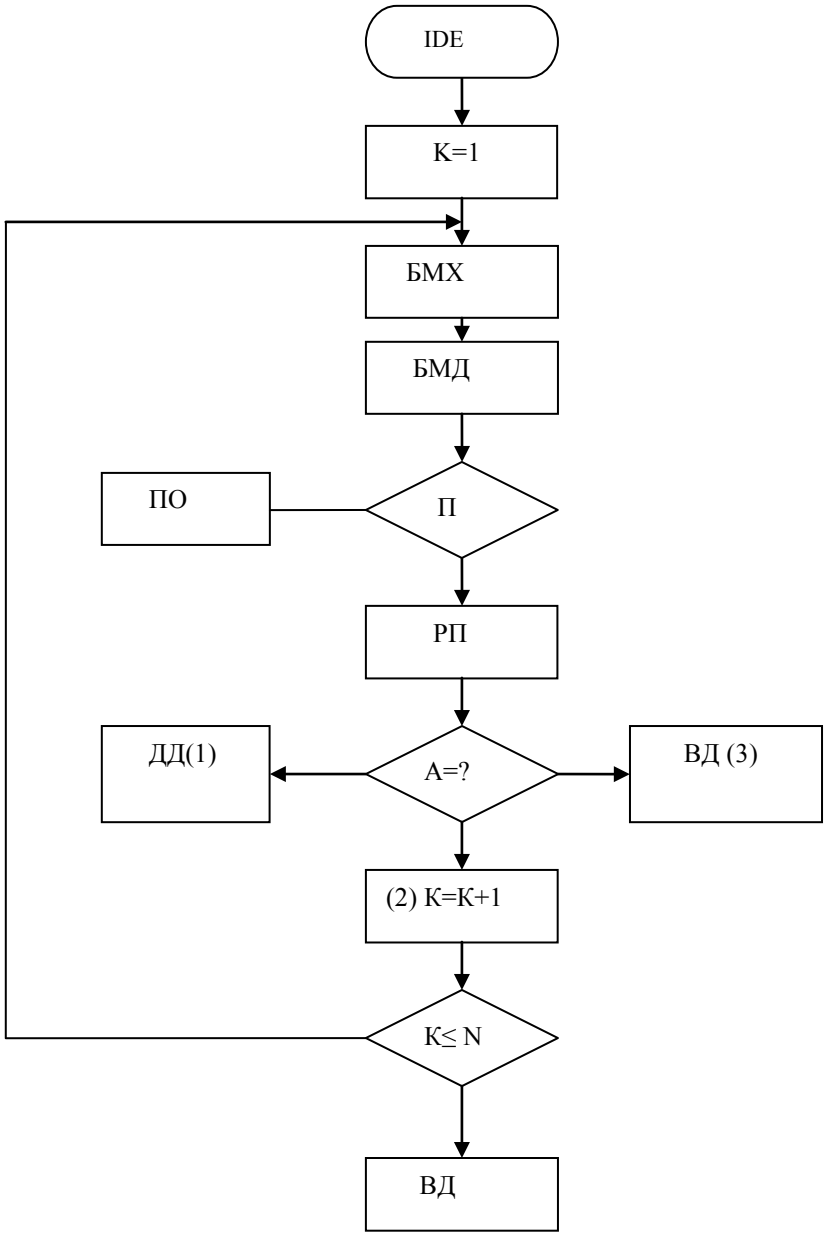

Рис. 1. Узагальнений алгоритм ідентифікації особи на основі БМХ
К=1 – встановлення лічильника кількості варіантів повторення вводу даних;
БМХ – реєстрація БМХ людини; БМД – формування вибірки БМ даних; ПО – формування вектора персоніфікованих ознак БМХ; П – порівняння введених ознак БМХ з персоніфікованими;
РП – формування вектора результатів порівняння ознак; А – аналіз результатів порівняння (1 – доступ дозволено ДД, 2 – повторення варіанта вводу, 3 – у доступі відмовлено ВД);
К=К+1 – перехід до перевірки наступного варіанта; К≤ N – перевірка умови кількості варіантів вводу, якщо К≥N – відмова в доступі

Технології реєстрації відбитків пальців

Ідентифікація людей за відбитками пальців – найпоширеніший спосіб, що використовується біометричними системами захисту інформації. На рис. 2 показаний розподіл різних технологій , що використовують для ідентифікації особи.

Рис. 2. Розподіл технологій , що використовують для ідентифікації особи

Найчастіше для реєстрації дактилоскопічних параметрів особи використовують оптичні сканери. Принцип дії цих пристроїв практично ідентичний принципам роботи звичайних сканерів. Основне значення приділяється внутрішньому джерелу світла, декільком призмам і лінзам. Головна перевага оптичних сканерів – це їхня дешевизна, але відбиток, отриманий за допомогою оптичного сканера, дуже залежить від стану шкіри. Жирна або, навпаки, суха і тим більше потріскана шкіра може бути причиною розмитості зображення і неможливості ідентифікації особи [3].

Друга технологія заснована на використанні напівпровідникових сканерів. В основі напівпровідникових сканерів лежить використання для одержання зображення поверхні пальця властивостей напівпровідників, які змінюються в місцях контакту гребенів папілярного візерунка з поверхнею сканера. Технологія ємнісних сенсорів (найпоширенішого типу напівпровідникових сканерів) полягає ось у чому. Користувач прикладає палець до спеціальної пластини, що складається з кремнієвої підкладки, яка містить 90 тис. конденсаторних пластин із кроком зчитування 500 dpi (dots per inch – точок на дюйм). При цьому виходить своєрідний конденсатор. Одна пластина – це поверхня сенсора, друга – палець людини. А оскільки потенціал електричного поля усередині конденсатора залежить від відстані між пластинами, то карта цього поля повторює папілярний малюнок пальця. Електричне поле вимірюється, а отримані дані перетворюються у восьмибітове растрове зображення.

Такі системи мають невеликі розміри, прості в застосуванні і відрізняються високим рівнем ідентифікації. На рис. 3 зображена мікросхема сенсора TCS1A фірми STMicroelectronics. Принцип дії цього КМОН сенсора заснований на використанні конденсаторних елементів (пікселів) для зчитування зображення з поверхні пальця (рис. 4).

Рис. 3. Мікросхема біосенсора TCS1A

Рис. 4. Конденсаторний елемент для зчитування зображення

Розміри поверхні зчитувального сенсора становлять 18×12.8 мм або 256×360 пікселів. Відстань між пікселями 50 мкм. Розширення сенсора 508 dpi, швидкість зчитування 15 зображень за секунду. Захист сенсора від електростатичних полів становить 8 кВ, струм споживання 200 мА, діапазон робочих температур 0–40 ºС. У неактивному режимі споживання сенсора не більше 1 мА.

До переваг цієї технології можна зарахувати високу точність одержуваного відбитка пальця, що не залежить від стану шкіри користувача.

Крім того, сам пристрій має маленькі розміри, що дає змогу використовувати його в багатьох місцях. Недоліки електричного сканера:

- дорога технологія виготовлення сенсора ;
- необхідність герметичної оболонки для кремнієвого кристала, що лежить в основі сканера;
- обмеження на умови застосування системи, зокрема на зовнішнє середовище, наявність вібрації й ударів.
- можливе порушення роботи сканера за наявності сильного електромагнітного випромінювання.

Наступною технологією є використання теплових сенсорів для зчитування відбитків пальців. Фірма Atmel Grenoble запропонувала сканер для сканування відбитків пальців, у складі якого кристал теплового сенсора зображення FCD4A14.

Цей сканер не вимагає оптичних пристроїв і джерела світла. Палець (відбиток якого підлягає зчитуванню) виділяє необхідну кількість тепла для зчитування зображення. Сенсор зчитує з розширенням 500 dpi зображення вимірюванням різниці між тепловою провідністю опуклостей і западин на поверхні пальця (рис. 5).

Рис. 5. Тепловий сенсор

Тепловий сенсор (на відміну від КМОН сенсора) не вимагає захисту від електростатичних полів і не має потреби в спеціальних покриттях, що охороняють його поверхню від вологи й інших факторів [4, 5].

Перспективною технологією ідентифікації людей за відбитками пальців є TactileSense. У цих сканерах використовується спеціальний полімерний матеріал, чутливий до різниці електричного поля між гребенями і западинами шкіри. Тобто, фактично принцип роботи пристроїв TactileSense такий самий, як і в електричних сканерів, але вони мають деякі переваги. По-перше, вартість виробництва полімерного сенсора в сотні разів менша , ніж ціна кремнієвого. Крім того, відсутність тендітної основи забезпечує високу міцність як поверхні сканера, так і усього пристрою. Третя перевага TactileSense – це мініатюрні розміри сенсора. Фактично для одержання відбитка потрібна тільки пластинка площею, яка дорівнює площі подушечки пальця, і товщиною усього 0,075 мм. Сенсор настільки малий, що його можна вмонтувати практично в будь-який комп'ютерний пристрій.

Наступним є спосіб одержання зображення візерунків папілярних ліній (ПЛ) з використанням ультразвукових давачів, який забезпечує високу точність. У цьому способі застосовується ехографія поверхні шкіри пальця, причому основна його перевага полягає в тому, що сканується не поверхня шкіри, а підшкірний шар, тобто стан поверхні пальця не впливає на якість отриманого зображення. Однак для одержання зображення прийнятної якості розміри ультразвукових давачів внаслідок їхньої малої чутливості необхідно збільшувати, що одночасно призводить до збільшення їхньої вартості і розмірів пристроїв ідентифікації. Крім того, формування зображення виконується протягом декількох секунд, що неприйнятно для деяких завдань ідентифікації. Цей спосіб має багато переваг і його можна зарахувати до розряду перспективних, що підтверджується експлуатацією пристроїв, побудованих на його базі [6].

Ідентифікація за відбитками пальців — на сьогодні найпоширеніша біометрична технологія. За даними International Biometric Group, частка систем розпізнавання за відбитками пальців становить майже половину від усіх використовуваних у світі біометричних технологій, і за прогнозами обсяг продажів таких систем має тенденцією подвоєння щороку.

1. http://www.biometrics.ru.

2. http://www.chip.ua.

3. Дактилоскопия и типы датчиков отпечатка пальца // ЭКиС. – К.:VD MAIS. – 2002. – №8.

4. Полупроводниковые датчики отпечатка пальца // ЭКиС. – К.:VD MAIS. – 2002. – №10.

5. Рябов Г.І. Современные технологии идентификации личности по отпечатку пальца с использованием емкостных датчиков // Электронные компоненты. 2002. – № 4.

6. Лазаренко М.І. Датчики отпечатка пальца и система аутентификации STM-UPEK // Chip News Украина. – 2005. – № 3.