ОГЛЯД СУЧАСНИХ ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ ДАКТИЛОСКОПІЧНОЇ ІНФОРМАЦІЇ

Анатолій Іванович ЦІНИК,

завідувач сектору дактилоскопічного обліку, Закарпатський науково-дослідний експертно-криміналістичний центр МВС України

Бурхливий розвиток інформаційних технологій протягом останніх десятиліть, що проявляється у зменшенні розмірів електронних компонентів і кратним збільшенням їх обчислювальної потужності, дозволив значно розширити спектр застосування дактилоскопічної інформації особи. Унікальність, стійкість, відновлюваність папілярного узору людини не могли залишитися поза увагою технічного прогресу.

Якщо раніше сканери відбитків пальців рук розміщувалися в аеропортах, на об'єктах критичної інфраструктури, об'єктах у сфері оборони, стояли на захисті державної і комерційної таємниці, то на сьогодні важко уявити сучасний мобільний телефон, ноутбук без вбудованого сканеру відбитків пальців. Такі ж засоби контролю доступу у вигляді окремих модулів можна собі встановити на двері до приміщення чи сховища. Ми маємо підстави вважати, що такі засоби у подальшому будуть застосовуватися ще ширше і, відповідно, частіше будуть ставати об'єктом протиправних дій. Адже вже сьогодні, маючи доступ до мобільного телефону, зловмисник має доступ до банківських рахунків та може безперешкодно здійснювати будь-які фінансові операції. Можливо, в перспективі, відбиток пальця руки замінить підпис або буде слугувати для ідентифікації особи при її зверненні до фінансової установи чи державного органу. То ж ціна помилки при підміні відбитку, обмані засобів контролю доступу буде тільки зростати, що, на нашу думку, буде викликати все більшу зацікавленість з боку зловмисників.

Необхідно зазначити, що ідентифікація особи за будовою папілярного узору пальця руки в контексті забезпечення безпеки та контролю доступу є не найдосконалішим, проте найбільш масовим методом. Цей та інші методи об'єднує та вивчає відносно нова галузь науки під назвою біометрія, яка виникла на стику кібернетики, біології, математичного аналізу. Далеко не останнє місце у формуванні цієї галузі знань зайняла криміналістична наука, яка за століття свого існування

вивчила та систематизувала широке коло аспектів ідентифікації людини за найрізноманітнішими індивідуальними особливостями будови тіла та її рухових навиків. Для підтвердження цього досить лише перерахувати актуальні галузі біометрії: автоматизоване розпізнавання особи за її підписом та почерком, розпізнавання обличчя, розпізнавання голосу, ідентифікація особи за будовою райдужної оболонки ока (англійською - «айріс»), ототожнення ДНК, та, власне предмет нашого огляду – розпізнавання будови папілярного узору, і ідентифікація особи за будовою кисті руки в цілому.

В основі будь-якої біометричної системи контролю доступу лежить баланс двох параметрів: поріг чутливості, при якому одна людина може бути хибно розпізнана, як інша та імовірність того, що людина, яка володіє доступом може бути розпізнана як стороння особа. Дані параметри повинні бути збалансовані, однак вже самим алгоритмом ідентифікації закладена похибка, яку і намагаються виявити зловмисники. Але якщо математичний апарат, яким керується система вже напрацьований, то з боку інженерії, якраз ведуться активні роботи.

Розглянемо найпростіший алгоритм роботи сканеру відбитків пальця руки. Особа, що ідентифікується, взаємодіє з сенсором, який робить електронну копію папілярного узору. Дані з сенсору обробляються, їм надається необхідний контраст, після чого в роботу вступає модуль, що виділяє індивідуальні ознаки та формує із їх сукупності геометричний візерунок у координатній площині. Побудова даного візерунку, а вірніше, відстаней між окремими точками і кутами між лініями, що їх з'єднують, і є тим «ідеальним» відбитком, який обробляє та зберігає машина. Наступний модуль порівнює відбиток з базою даних та на основі закладеної у алгоритм математичної похибки, дає «зелений» сигнал системі управління. У разі, якщо похибка у сліді перевищує певну запрограмовану межу, сканер відмовляє у доступі. Дана схема є типовою, вона може ускладнюватися двоступеневою верифікацією (коли крім відбитку пальця необхідний пароль), обчислювачами похибки, які дозволяють сканувати палець у різних положеннях і так далі, але у тому чи іншому вигляді, усі перераховані компоненти будуть у наявності. Більше того, даний алгоритм був розроблений ще у 70-х роках минулого століття, коли постало завдання розробити машинний спосіб обробки масивів дактилоскопічної інформації.

З точки зору криміналістики, найбільший інтерес, на нашу думку, викликає сенсор, що безпосередньо зчитує папілярний узор. Саме цей компонент системи розвивається найбільш бурхливо та за останні роки покращив не тільки якість зчитування, роздільну здатність, а і декілька разів повністю змінив фізичні принципи, на основі яких він діє. Та саме сенсор першим стає на заваді протиправного посягання на пристрій.

Сенсори перших поколінь базувалися на оптичному методі зчитування. Палець прикладався до грані перевернутої призми, де за допомогою підсвітки та зчитуючих елементів, формувалося зображення папілярного узору. Незважаючи на простоту та високу якість зображення, сенсори даного типу є дуже вразливими до механічних

пошкоджень, мають доволі істотну затримку у отриманні зображення, відмовляються сканувати відбиток з забрудненням, велике значення має щільність прилягання пальця. Перераховані фактори не дозволили засобам контролю доступу на основі дактилоскопічної інформації отримати таке широке застосування у мобільних електронних пристроях, яке вони мають зараз, однак оптичні сенсори постійно вдосконалюються.

Наступним кроком у розвитку стали сенсори ємнісного типу. Дані пристрої практично позбавлені недоліків: механічно стійкі, швидко формують умовне зображення, в розумних межах не зважають на забруднення пальця. Окрім того, мають ще один великий «плюс»: здатні розрізнити палець виключно фізично живої особи, на відміну від оптичних сканерів. З масовим запровадженням сенсорів такого типу, ми можемо спостерігати бурхливе зростання кількості мобільних пристроїв з вбудованими засобами контролю доступу.

В основі принципу роботи сенсорів ємнісного типу лежить здатність будь-якого живого організму нести електричний заряд. Саме на різниці електричного потенціалу між валиками папілярних ліній та міжпапілярними проміжками, пристрій формує «карту» папілярного узору. Матриця таких сканерів має роздільну здатність близько 500 точок на дюйм, один піксель має розмір 50 мікрон. Пристрої такого типу безперешкодно зчитують будову папілярного узору незалежно від щільності прикладання чи кута нахилу.

Найостанніша розробка у цій галузі – сенсор, що базуються на ультразвуковому скануванні папілярного узору. Для роботи такого сканеру не потрібне спеціальне місце, до якого потрібно прикладати палець. Такий пристрій може отримувати зображення навіть без безпосереднього контакту, через скло, метал, пластик. Ще однією важливою перевагою є те, що сенсор не просто формує зображення у площині координат, а сканує його з такою роздільною здатністю та глибиною різкості, що дозволяє отримати повний тривимірний відбиток пальця, у якому відображений весь спектр пороеджіоскопічної інформації.

З моменту появи, сенсори та засоби контролю доступу в цілому стали об'єктом, що викликають надзвичайну зацікавленість у зловмисників, тому у їх вдосконалення вкладаються значні ресурси. Як і будь-яка інша перешкода для протиправних дій, засоби контролю доступу не позбавлені недоліків та все-таки піддаються обходу різними способами. Разом з тим, необхідно зазначити, що ці способи чимдалі стають все більш складними і потребують значних ресурсів та спеціальних знань, окрім того, не гарантують позитивного результату.