УДК 681.301

Д.т.н., професор Зайцев В.Г., магістрант Степенко К.С.

**Національний технічний університету України
«Київський політехнічний інститут»**

СПОСІБ КОНТРОЛЮ ДОСТУПУ НА ПІДСТАВІ РОЗПІЗНАВАННЯ ВІДБИТКІВ ПАЛЬЦІВ

Вступ

Біометрична ідентифікація - автоматизований метод, за допомогою якого шляхом перевірки (дослідження) унікальних фізіологічних особливостей або поведінкових характеристик людини здійснюється ідентифікація особи. Фізіологічні особливості, наприклад, такі як папілярний узор пальця, геометрія долоні або малюнок (модель) райдужної оболонки ока, є постійними фізичними характеристиками людини. Даний тип вимірів (перевірки) практично незмінний також як і самі фізіологічні характеристики.

Останніми роками, процес ідентифікації особи по відбитку пальця звернув на себе увагу як біометрична технологія, яка цілком імовірно буде найширше використовуватися в майбутньому. Використання відбитку пальця для ідентифікації особи є найбільш зручним зі всіх біометричних методів. Ймовірність помилки при ідентифікації користувача набагато менша порівняно з іншими біометричними методами

У наші часи у зв'язку з появою нових технічних можливостей розпізнавання по відбитках пальців почало виходити за рамки використання лише в криміналістиці і знайшло своє застосування в найрізноманітніших галузях інформаційних технологій; в першу чергу такими галузями стали:

- системи управління доступом;
- інформаційна безпека;
- облік робочого часу і реєстрація відвідувачів; системи голосування;
- проведення електронних платежів;
- аутентифікація на web-ресурсах;
- різні соціальні проекти, де потрібна ідентифікація людей (добродійні акції тощо);
- проекти цивільної ідентифікації (перетин державних кордонів, видача віз на відвідини країни тощо)[2].

Постановка задачі

Існують певні труднощі при порівнянні декількох моделей відбитків одного пальця.

Одна з основних складнощів при порівнянні моделей відбитків одного пальця полягає в тому, що при неправильному розміщенні пальця на сканувальному пристрої відбиток пальця зазнає спотворення.

Основні зусилля в цьому напрямі спрямовуються до створення моделі спотворення відбитку пальця. Така модель дозволить не лише розробляти системи генерації відбитків пальця, але і створювати алгоритми розпізнавання відбитку пальця, стійкі до спотворень.

Інша проблема: ідентифікація за відбитком пальців має дуже низький рівень FAR ("пропустити чужого", тобто приймається рішення "свій", хоча, насправді, суб'єкт відсутній в списку зареєстрованих користувачів). Але в цього методу, як і у всіх інших, є свої проблеми, які можуть виникнути при ідентифікації. По-перше, проблема "муляжу" - можливість імітації папілярного малюнка живого пальця. По-друге, проблема "важких пальців" - приблизно 1% всіх людей зустрічаються з труднощами при скануванні папілярного малюнка через пошкодження, опіки, шкірних хвороб тощо[1].

Нарівні з проблемою "чужою серед своїх" можливий варіант "свій серед чужих", коли потрібний відбиток пальця відкидається і потрапляє в розряд "чужих", тобто він не розпізнається як "свій"[1].

Вибір методів

Робота автоматизованої біометричної системи зазвичай відбувається в одному з двох режимів - ідентифікації або верифікації. В обох випадках початкова установка, або так звана реєстрація, практично однакова і багато в чому залежить від правильного введення інформації. Результатом реєстрації повинен стати представлений в електронному вигляді інформаційний пакет, зручний для використання і розміщений в базі даних або ж на ідентифікаційних смарт-картах. Реєстрація є тим етапом, на якому вкрай важливим є ефективна взаємодія між всіма користувачами і точне виконання всіх процедур, оскільки від цього залежать подальше функціонування, працездатність і точність системи. Одне з важливих питань, які необхідно вирішити, полягає в тому, для чого планується використовувати систему - для ідентифікації або верифікації. Якщо говорити про ідентифікацію, то система намагається знайти, кому належить даний зразок, порівнюючи зразок з базою даних для того, щоб знайти збіг (також цей процес називають порівнянням одного з багатьма).

Верифікація - це порівняння, при якому біометрична система намагається веріфікувати особу людини. У такому разі новий біометричний зразок порівнюється з раніше збереженим зразком. Порівнюючи ці два зразки, система підтверджує, що дана людина дійсно та, за кого вона себе видає. В процесі ідентифікації система порівнює один зразок з багатьма, тоді як процес аутентифікації або верифікації порівнює один з одним. В разі ідентифікації необхідна центральна база даних біометричної інформації, з якою порівнюватиметься конкретний зразок. У другому випадку біометричні дані людини перевіряються на схожість з електронними даними, що містяться, наприклад, на смарт-карті [4].

Для вибору алгоритму розпізнавання (ідентифікації та верифікації) було проаналізовано три відомих алгоритми: кореляційне порівняння, порівняння особливих крапок, порівняння узору [3].

Кореляційне порівняння. Отриманий із сканера відбиток пальця накладається на кожен еталон з бази даних по черзі, після чого по пікселях зображення здійснюється пошук відмінностей між ними. При цьому виникає проблема порівняння - людина кожного разу прикладає палець під різними кутами і не точно в одне і те ж місце робочої області сканера. А це означає, що процес порівняння відбитку пальця з еталонами повинен включати безліч ітерацій, на кожній з яких зображення, отримане із сканера, повертається під невеликим кутом або трохи зміщується. Головною перевагою цього методу ідентифікації є низькі вимоги до якості зображення відбитку пальця. Недоліком залишається велика тривалість процедури порівняння отриманого папілярного узору з еталонами, що сильно обмежує сферу застосування кореляційного порівняння.

Порівняння особливих крапок – по одному або декільком зображенням відбитків пальців із сканера формується шаблон, що є двомірною поверхнею, на якій виділені кінцеві крапки. При порівнянні - на відсканованому зображенні відбитку також виділяються ці крапки. Карта цих крапок порівнюється з шаблоном і по кількості крапок, що збіглися, приймається рішення по ідентичності відбитків. Головною перевагою алгоритму порівняння відбитків пальців по особливих крапках є швидкість його виконання. Основний час в процесі ідентифікації займає перебір еталонів в пошуку відбитку, ідентичного тимчасовому. Недоліком алгоритму є відносно висока вимога до якості зображення папілярного узору.

В алгоритмі порівняння узору використовуються особливості будови папілярного узору на поверхні пальців. Отримане із сканера зображення відбитку пальця, розбивається на безліч дрібних вічок. Розташування ліній в кожному вічку описується параметрами деякої синусоїдальної хвилі, тобто, задається початкове зрушення фази, довжина хвилі і напрям її

поширення. Спеціальний модуль розглядає папілярні лінії в квадратиках по черзі і кожну з них описує рівнянням синусоїдальної хвилі, тобто встановлює початкове зрушення фази, довжину хвилі і напрям її поширення. Саме ці дані використовуються для ідентифікації: у базі даних еталонів зберігаються параметри всіх відрізків горбків в кожній області. І саме вони порівнюються з даними, отриманими при скануванні. Головними плюсами розглянутого алгоритму є досить висока швидкість його роботи і низькі вимоги до якості отримуваного зображення.

Теоретичні дослідження

Проведений аналіз по надійності і ефективності розпізнавати зображення з використанням цих алгоритмів дозволяє стверджувати, що алгоритм порівняння узору найбільш підходить для вирішення задачі розпізнавання відбитків пальців. Запропонована система виконує наступні функції:

- навчання (створення елементної бази відбитків пальців),
- розпізнавання на основі алгоритму порівняння узору,
- поповнення бази даних.

Висновки

Проведене дослідження доводить, що алгоритм порівняння узору є найбільш ефективним для вирішення задачі порівняння сканованих зображень відбитків пальців. Слід зазначити, що якість отримуваного зі сканера зображення папілярного узору пальця є одним з факторів, від якого залежить обираний алгоритм.

За допомогою алгоритму порівняння узору може бути створена система контролю доступу на основі розпізнавання відбитків пальців з використанням існуючих засобів обчислювальної техніки.

Література

1. *A. Jain and S. Pankanti*, "Automated Fingerprint Identification and Imaging Systems", Advances in Fingerprint Technology – pp.5-7.
2. PC Magazine/Russian Edition - 2004 - №1 - С.21-23.
3. PC Magazine/Russian Edition - 2004 - №2 - С.12-14.
4. *Anil K. Jain and Robert P. W. Duin and Jianchang Mao*, "Statistical Pattern Recognition: A Review". // IEEE Transactions on Pattern Analysis and Machine Intelligence – 2002 - vol. 22, no. 1 - pp. 4-37.