

МЕТОД АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЗА ВІДБИТКОМ ПАЛЬЦЯ

У статті запропоновано вдосконалений метод аутентифікації користувачів за особливими точками відбитка пальця, що дозволило підвищити швидкість та ефективність процедури розпізнавання. Метод використовує дані про координати трьох точок та кут між сусідніми точками триплета. Розроблено програмний комплекс аутентифікації користувачів автоматизованої системи для візуалізації результатів проведених досліджень.

Ключові слова: аутентифікація, відбиток пальця, триплет, бінаризація, скелетизація, особливі точки, сканування, швидкодія розпізнавання

Вступ

Для реалізації контролю доступу до ресурсів автоматизованої системи (АС) необхідно використовувати систему аутентифікації користувачів. Біометрія є одним із найперспективніших напрямків для використання в АС. В якості унікальних ознак користувача АС використовуються [1–5]:

1) статичні характеристики – папілярний візерунок на пальцях, райдужна оболонка ока, геометрія обличчя, геометрія рук, сітківка ока;

2) динамічні характеристики – голос, динаміка рукописного почерку тощо.

Вибір тієї чи іншої ознаки ґрунтується на допустимій швидкодії процедури аутентифікації користувачів АС, соціальній прийнятності, простоті використання, стійкості до підробки тощо. Найбільшу популярність отримав метод аутентифікації користувача за відбитком пальця, оснований на унікальності візерунку, що утворений папілярними лініями. Цей метод забезпечує високу достовірність розпізнавання, кращі статистичні показники, а вартість пристроїв для сканування відбитка пальця є невисокою [6–7]. Однак, відомі алгоритми аутентифікації користувачів за відбитками пальця потребують удосконалення і подальших досліджень.

Аналіз останніх досліджень і публікацій показує, що існують три класи методів порівняння відбитків пальців: кореляційне порівняння, порівняння за візерунком та особливими точками [8–9]. Основним недоліком першого класу методів є їх низька швидкодія. Для усунення цього недоліку застосовують методи порівняння за візерунком, що використовують особливості будови папілярних ліній пальця, однак вони мають високу обчислювальну складність [8]. Проблема швидкодії методів аутентифікації за відбитками пальця вирішена в алгоритмах порівняння за особливими точками. Зображення аналізується на предмет особливих точок, якими є точки закінчення папілярних ліній та точки розгалуження. Особливостями даного класу методів є простота реалізації і висока швидкодія. Однак, ці алгоритми чутливі до повороту та зміщення пальця при скануванні. Тому особливі точки групують по три у триплети та зберігають інформацію про їх взаємне розташування [9]. В даний час невирішеним є завдання визначення параметрів триплетів, що необхідні для ідентифікації відбитків, і які забезпечать зменшення чутливості методу до повороту та зміщення пальця при скануванні.

Постановка задачі

Метою досліджень є модифікація методу аутентифікації за відбитками пальця на основі особливих точок для підвищення ефективності розпізнавання користувачів АС. Завданнями дослідження є аналіз напрямів удосконалення методу аутентифікації на основі особливих точок, підвищення стійкості методу до якості зображення відбитка, формалізація процесу розпізнавання користувача та реалізація програмного комплексу на основі запропонованого методу.

Застосування вдосконаленого методу виокремлення особливих точок

В системах аутентифікації користувачів за відбитком пальця наявний модуль попередньої обробки сканованого зображення. Складність обробки залежить від якості отриманого зображення зі сканера та ефективності методу виділення особливих точок. Основними етапами роботи із зображенням в процесі аутентифікації є: бінаризація, скелетизація, виділення особливих точок [6, 9].

Бінаризація – це перетворення зображення до чорно-білого вигляду. Кожен піксель може бути або абсолютно чорним, або абсолютно білим, що відповідає максимальному і мінімальному значенню інтенсивності пікселя. Ця процедура дозволяє позбавитись надлишкової інформації. Після цього лінії на бінаризованому зображенні стоншуються до товщини в один піксель, а з отриманого скелета відбитка пальця вилучаються особливі точки [8–9]. Такими точками можуть служити точки закінчення папілярних ліній та їх розгалуження (рис. 1).

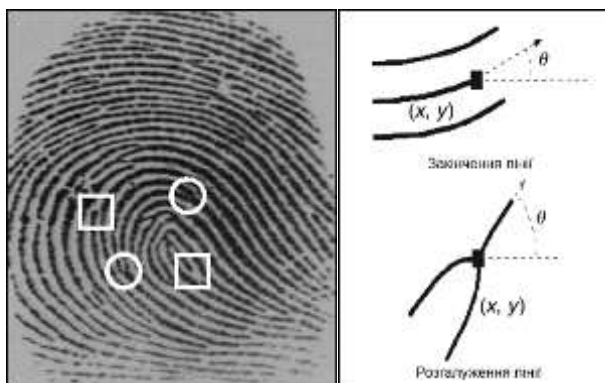


Рис. 1. Приклад особливих точок відбитка пальця

З отриманих на попередніх етапах точок формується масив об'єктів з наступними параметрами: координати точки; тип лінії; кут, утворений ними. Набір параметрів особливих точок, отриманий зі сканованого відбитку пальця, порівнюється з набором еталонних параметрів відбитків зареєстрованих користувачів АС. На наступному етапі визначаються відхилення в значеннях цих параметрів. Великий поріг відхилення збільшить ймовірність хибного збігу біометричних характеристик двох користувачів – FAR (False Acceptance Rate). З іншого боку, мале значення допустимого відхилення є причиною збільшенню ймовірності відмови законному користувачу АС – FRR (False Rejection Rate) [6–7]. Проблема вибору порогу допуску пов'язана із деформацією та зміщенням пальця при скануванні, що призводить до отримання щоразу різних параметрів вилучених точок.

В результаті проведених досліджень було встановлено, що доцільно зберігати інформацію про комбінацію трьох особливих. Така структура – триплет, наведена на рис. 2.

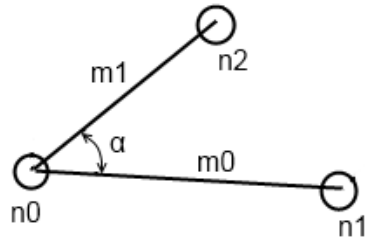


Рис. 2. Структура триплета

Для кожної центральної точки $n_0(x_{n0}, y_{n0})$ і двох сусідніх точок $n_1(x_{n1}, y_{n1})$ та $n_2(x_{n2}, y_{n2})$ формується вектор параметрів:

$$Tr_i = (m_0, m_1, \alpha, t_{n0}, t_{n1}, t_{n2}), \quad (1)$$

де m_1 та m_2 – це відстані від центральної точки до відповідних сусідніх точок; α – кут утворений m_1 і m_2 ; t_{n0}, t_{n1}, t_{n2} – типи відповідних точок.

Запропоновані параметри особливих точок є інваріантними до повороту та зміщення пальця, а також до деформації шкіри під час сканування. Координати точок не зберігаються, адже, як було описано раніше, вони не надійні. Коли одна особлива точка асоціюється лише з однією парою особливих точок, така структура не є надійною і стійкою до появи хибних точок чи пропуску точки (рис. 3).

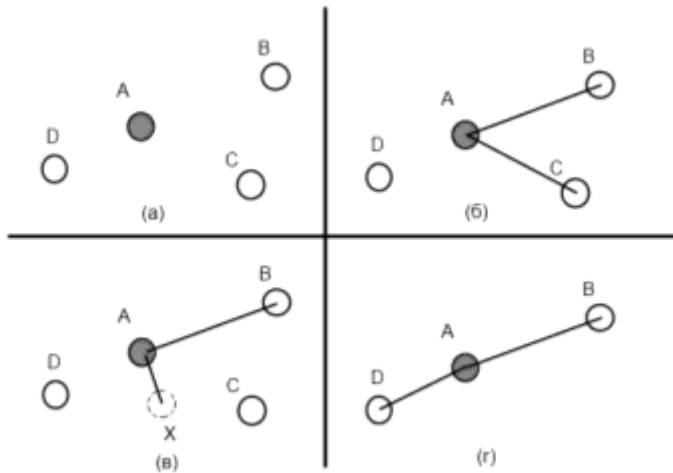


Рис. 3. Приклад генерації чотирьох особливих точок

На рис. 3 (а) наведено приклад для чотирьох вилучених особливих точок, де А – точка для якої генеруватимуться додаткові параметри. Згенеровані додаткові параметри для точки А наведені на рис. 3 (б). Результат генерації параметрів при появі хибної точки X близької до А представлений на рис. 3 (в), а випадок отриманих параметрів при пропусненні особливої точки С зображено на рис. 3 (г). Отже, доцільно зберігати параметри декількох триплетів для кожної точки.

В залежності від кількості сусідніх точок, можна утворити певну кількість триплетів:

$$s = \frac{n!}{2!(n-2)!}, \quad (2)$$

де n – кількість сусідніх точок, обраних для утворення триплетів; s – кількість можливих триплетів.

Запропоновані рішення не дозволяють уникнути впливу спотворень зображення відбитка пальця користувача АС повністю, тому слід використовувати динамічні допустимі відхилення параметрів відбитка (рис. 4).

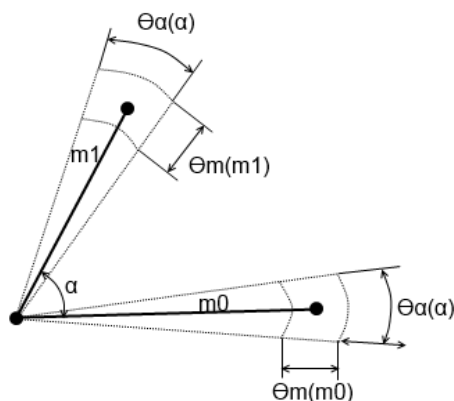


Рис. 4. Допустимі динамічні відхилення параметрів

Розмір відхилення параметрів відбитка визначається двома функціями визначення порогових значень Θ_α , Θ_m . Функція визначення допуску за відстанню Θ_m повертає менше значення порогу при меншому значенні відстані між точками m_0 та m_1 , і більше – при великих значеннях m_0 та m_1 . Інша функція Θ_α аналогічно визначає поріг допуску для кута α між сусідніми точками.

Отже, метод аутентифікації користувачів АС за особливими точками відбитків пальця полягає в наступному:

1. Типи точок, якими утворено триплет, повинні відповідати типам точок із еталонного зображення відбитка зареєстрованого користувача.
2. Відстань між центральною особливою точкою і її сусідніми точками має задовольняти умову:

$$|m_0 - m_{0e}| \leq \Theta_m(m_0) \cap |m_1 - m_{1e}| \leq \Theta_m(m_1),$$

де m_0 і m_1 – відстані між точками триплета сканованого відбитка; m_{0e} і m_{1e} – аналогічні параметри еталонного триплета, що зберігаються в системі; Θ_m – функція визначення допуску за відстанню між особливими точками.

3. Значення кута між m_0 і m_1 визначається наступною умовою:

$$|\alpha - \alpha_e| \leq \Theta_\alpha(\alpha),$$

де α – кут між m_0 і m_1 особливих точок сканованого відбитка; α_e – аналогічний кут еталонного триплета; Θ_α – функція визначення допуску за кутом.

Наступним етапом є визначення відсотка відповідності наборів параметрів сканованого відбитку та збережених у системі аутентифікації еталонних значень для за-

реєстрованих користувачів. Відсоток відповідності триплетів визначається за виразом:

$$R = \frac{\sum_i s_i}{\sum_j s_{ej}} 100\% , \quad (3)$$

де s_i – кількість триплетів, вилучених зі сканованого відбитку, що пройшли перевірку відповідності; s_{ej} – кількість триплетів з еталонного набору параметрів відбитка.

Рівень довіри до особи, що проходить процедуру аутентифікації, визначається з виконання умови $R \geq \delta$, де δ – порогове значення визнання ідентичності відбитків користувача АС. Змінюючи значення параметра δ контролюється чутливість системи аутентифікації до спотворення сканованого зображення відбитка. Однак, у випадку недостатньо великого значення порогового параметра системи існує можливість хибного визнання користувачем АС сторонньої особи. В результаті експериментальних досліджень встановлено, що бажане значення цього параметра для системи аутентифікації користувачів АС становить $\delta \approx 90\%$.

За результатами проведених досліджень було розроблено програмний комплекс "Fingerprint" із використанням засобів ICP Visual Studio та СКБД MS SQL Server, результати роботи якого наведені на рис. 5.



Рис. 5. Результати роботи програмного комплексу

Висновки

Запропонований метод аутентифікації користувачів АС на основі особливих точок за відбитками пальця дозволив підвищити ефективність процесу розпізнавання шляхом зменшення чутливості алгоритму до повороту та зміщення пальця при скануванні. При цьому зберігаються такі переваги даного класу алгоритмів аутентифікації, як швидкодія та невисока обчислювальна складність. Отже, використання розробленого методу в АС дозволить спростити процедуру аутентифікації користувачів та знизити вимоги до апаратних засобів системи. Предметом подальших досліджень є теоретичне обґрунтування порогових значень допустимих відхилень функції за кутом та координатою.

Література

1. *Кухарев Г. А.* Биометрические системы: Методы и средства идентификации личности человека / Г.А. Кухарев. – СПб.: Политехника, 2001. – 240 с.
2. *Давлетханов М.* Способы идентификации по отпечаткам пальцев [Электронный ресурс] / М. Давлетханов. – 2004. – Режим доступа: <http://www.infobez.ru/article>.
3. *Домарев В.В.* Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО ТИД Диа Софт, 2004. – 992 с.
4. *Евангели А.* Технологии биодентификации и биометрический рынок / А. Евангели // PC Week/RE/ – 2003. – №7 – С. 24–25.
5. *Зиятдинов А.И.* Принципы построения систем биометрической аутентификации / А.И. Зиятдинов // МФТИ. 2005. – 8 с.
6. *Сеньор Э.У.* Руководство по биометрии / Э. У. Сеньор, Н. К. Ратха, Ш. Панканти, Дж. Х. Коннел, Р. М. Болл. – М.: Техносфера, 2007. – 368 с.
7. *Задорожный В.* Идентификация по отпечаткам пальцев. Ч. 1 [Электронный ресурс] / В. Задорожный // PC Magazine/Russian Edition. – 2004. – №1. – Режим доступа: <http://bre.ru/security/20994.html>.
8. *Chaohong Wu* Advanced feature extraction algorithms for automatic fingerprint recognition systems / Chaohong Wu. – 2007. – 122 p.
9. *Chirag Dadlani* Fingerprint Recognition Using Minutiae-Based Features / Chirag Dadlani. – 2007. – 26 p.

Надійшла до редколегії 27.04.2013 р.

Рецензент: д.т.н., проф. Пількевич І.А.

Молодецкая К.В., Сохан А.В.

МЕТОД АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПО ОТПЕЧАТКУ ПАЛЬЦА

Предложен усовершенствованный метод аутентификации пользователей по особым точкам отпечатка пальца, что позволило повысить скорость и эффективность процедуры распознавания. Метод использует данные о координатах трех точек и угол между соседними точками триплета. Разработан программный комплекс аутентификации пользователей автоматизированной системы для визуализации результатов проведенных исследований.

Ключевые слова: аутентификация, отпечаток пальца, триплет, бинаризация, скелетизации, особые точки, сканирование, быстродействие распознавания.

Molodetska K.V., Sohan O.V.

USER FINGERPRINT AUTHENTICATION METHOD FOR AUTOMATED SYSTEMS

An improved method for authenticating users on specific points of the fingerprint, thus improving the speed and efficiency of the recognition procedure. The method uses information about the coordinates of three points and the angle between adjacent points of the triplet. Software system for automated system users authentication for visualizing the results of the research where designed.

Keywords: authentication, fingerprint, triplet, binarization, skeletonization, singular points, scanning, recognition performance.