

УДК 004.75

Ю.Р. Гарасим, Т.Б. Крет

Національний університет «Львівська політехніка», Львів

ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПЕРСПЕКТИВНИХ ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ ОСОБИ В ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖАХ ЗВ'ЯЗКУ

Робота присвячена дослідженню та аналізу технологій ідентифікації особи за її біометричними ознаками. Розглянуто найбільш перспективні та найбільш вживані в даний час технології біометричної ідентифікації особи. Проаналізовано існуючі методи ідентифікації, визначено їхні недоліки та переваги.

Ключові слова: ідентифікація особи, біометричні методи захисту, біометричні сканери, захищені корпоративні мережі зв'язку.

Вступ

В час бурхливого розвитку інформаційних технологій постають проблеми збору, оброблення та зберігання даних, а також несанкціонованого доступу до них. Захист інформації та доступу до неї стоїть на першому місці при проектуванні та розробленні захищених корпоративних мереж зв'язку. Для доступу користувача в мережу переважно використовуються паролі доступу, картки ініціалізації особи. В наш час широко починає використовуватися ще один метод захисту конфіденційної інформації – система біометричної ідентифікації особи.

Огляд та аналіз технологій ідентифікації особи

Ідентифікація особи чи об'єкта – це його отождолення, розпізнавання з чим-небудь. В галузі інформаційних технологій, даний термін означає встановлення особистості користувача (його ідентифікації, перевірка на легітимність). Ідентифікація є одним з основних понять в термінології інформаційної безпеки [1].

На сьогоднішній день існує три найпоширеніші види ідентифікації: парольна, апаратна, біометрична [2].

До недавнього часу парольна ідентифікація була чи не єдиним способом визначення особистості користувача. Вона проста в реалізації та у використанні. Її суть полягає в тому, що кожен зареєстрований користувач, одержує набір персональних даних (логін, пароль), які вводяться при вході в захищену корпоративну мережу зв'язку.

Апаратний принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, який перебуває в ексклюзивному користуванні даної особи, користувача.

Біометрія – це технологія ідентифікації особи, що використовує фізіологічні та поведінкові параметри суб'єкта. В залежності за якою особливістю здійснюється ідентифікація особи, біометричні системи поділяються на ідентифікацію за відбитком пальця, розпізнавання райдужної оболонки, розпізнавання за голосом, за допомогою підпису тощо. Розпізнавання за відбитками пальців вважається найбільш практичною технологією, оскільки їй притаманна висока надійність, ненав'язливість та економічна ефективність.

Ідентифікація особи за відбитками пальців

Відбитки пальців представляють собою рельєфні лінії, папілярні зображення, будова яких зумовлена рядами гребінчастих виступів шкіри, розділених межами.

Встановлення відповідних відбитків високої якості не складний процес і кожний алгоритм може справитися з цією задачею. Реальна проблема полягає у встановленні відповідності відбитків поганої якості: зсув пальця під час сканування, нелінійне спотворення, різний стан шкіри, тиск на сканер.

В кожному відбитку пальця можна визначити два типи ознак: глобальні і локальні. До глобальних відносяться ті ознаки, які можна побачити неозброєним оком, а саме: папілярне зображення; область образу – виділений фрагмент відбитка, в якому локалізовані всі ознаки; пункт «дельта»-початкова точка, місце, в якому відбувається поділ чи з'єднання меж папілярних ліній; тип лінії – дві найбільші лінії, які починаються як паралельні, а потім розходяться і огинають область образу тощо.

Інший тип ознак – локальні. Їх називають мінуціями – унікальні для кожного відбитка ознаки, визначаючі точки зміни структури папілярних ліній (закінчення, роздвоєння, розрив тощо), орієнтацію папілярних ліній і координат в цих пунктах. Кожен відбиток вміщує до 70 мінуцій.

Етапи порівняння двох відбитків:

1. Покращення якості вихідного зображення відбитку. Збільшується різкість границь папілярних ліній.

2. Розрахунок поля орієнтації папілярних ліній

відбитка. Зображення розбивається на квадратні блоки, зі сторонами більше 4 пікселів і за градієнтами яскравості, розраховується кут t орієнтації ліній для фрагментів відбитка (рис. 1).

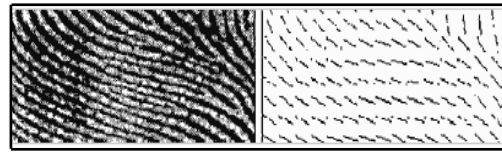


Рис. 1. Розрахунок поля орієнтації папілярних ліній

3. Бінаризація зображення відбитку. Приведення до чорно-білого зображення (1bit) пороговою обробкою.

4. Лінії відбитку пальця робляться тоншими, проводиться до того часу поки лінії не будуть шириною в 1 піксель. Виділення мінуцій. Зображення розбивається на блоки 9x9 пікселів. Після чого підраховується число чорних (нульових) пікселів, які знаходяться навколо центру. Піксель в центрі вважається мінуцією, якщо він сам не нульовий, і сусідні нульові пікселі один (мінуція «закінчення») чи два (мінуція «роздвоєння») (рис. 2).

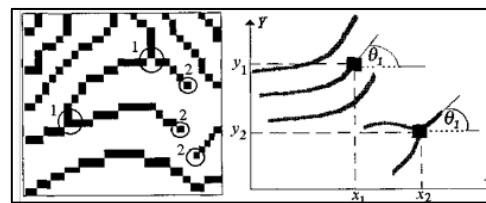


Рис. 2. Виділення мінуцій

5. Координати знайдених мінуцій і їхні кути орієнтування записуються у вектор

$$W(p) = [(x_1, y_1, t_1), (x_2, y_2, t_2) \dots (x_p, y_p, t_p)],$$

де p – число мінуцій.

6. При реєстрації користувача цей вектор вважається еталоном і записується в базу даних.

7. Співставлення мінуцій. Два відбитка одного пальця будуть відрізнятися один від одного поворотом, зміщенням, зміною масштабу чи площею дотику, в залежності від того, як користувач приклав палець до сканера. Тому не можна сказати, належить відбиток людині чи ні на основі простого їхнього порівняння (вектор еталону і поточного відбитку можуть відрізнятися за довжиною, вмістом невідповідних мінуцій тощо). Через це процес співставлення повинен бути реалізований для кожної мінуції окремо.

Етапи порівняння: реєстрація даних, пошук пар відповідних мінуцій, оцінка відповідності відбитків.

При реєстрації визначається кут повороту, масштаб і зсув, при яких деякі мінуції з одного век-

тора відповідають деяким мінущім з іншого вектора.

При пошуку для кожної мінущі необхідно 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). Отже, до 150000 кроків для кожної з 70 можливих мінущій.

Оцінку відповідності відбитків виконують за формулою:

$$K = (D * D * 100\%) / (p * q),$$

де D – кількість співпадінь мінущій, p – кількість мінущій еталону, q – кількість мінущій відбитку, який ідентифікується.

У випадку, коли результат перевищує 65%, відбитки вважаються ідентичними [3].

Ідентифікація на основі райдужної оболонки ока

В даний час використовуються два основні підходи для ідентифікації особи за райдужною оболонкою ока, які відрізняються способами представлення образів. В першому підході райдужна оболонка виділяється з зображення ока, в другому випадку – образом є матриця штрих кодів, що відповідає райдужній оболонці [4].

В першому підході є два способи представлення:

1) у вигляді кілець, які відносяться до області райдужної оболонки;

2) у вигляді прямокутника, який отримується шляхом перетворення декартової системи координат в полярну.

Спочатку знаходиться центр зіниці і два радіуси відносно нього – радіус зіниці і радіус зовнішнього краю райдужної оболонки.

Межі зіниці і райдужної оболонки не є при цьому круглими. Вони стають такими після додаткового оброблення. Після цього виконується збільшення чіткості зображення. (рис. 3).

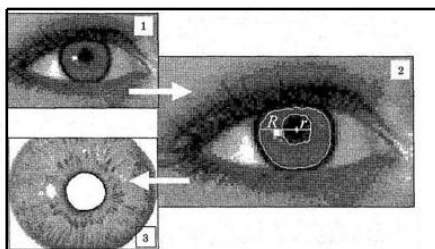


Рис. 3. Спосіб представлення райдужної оболонки у вигляді кілець

Коротко другий спосіб можна описати так:

1) визначення місця розташування, центру і контуру зіниці;

2) визначення радіусів зіниці і зовнішнього краю райдужної оболонки;

3) формування координат полярної системи;

4) перетворення кожного пікселя з декартової системи в полярну.

В результаті на осі X відкладені кути полярної системи координат, а на осі Y – значення радіуса.

Другий підхід, хоч і потребує більше розрахунків на етапі реєстрації, практичніший через те, що поворот зображення, перетвореного з декартової системи координат в полярну, замінюється циклічним зсувом.

Другий випадок представлення, коли образом є матриця штрих кодів, що відповідає райдужній оболонці. Спочатку зображення ока виділяється з зображення обличчя; на райдужну оболонку ока накладається спеціальна маска штрих-кодів. Результатом буде матриця, що отримується шляхом логічного множення маски на райдужну оболонку.

До переваг цього методу ідентифікації належить: висока ступінь розпізнавання; невелика кількість помилок першого і другого типу; безконтактний спосіб сканування;

Недоліки: неможливість використання цього методу під час захворювань очей; вартість [5].

Ідентифікація особи за технологією розпізнавання обличчя

Для ідентифікації особи найкраще підходить технологія розпізнавання за рисами обличчя. Вона не є нав'язливою (розпізнавання людини проходить на відстані, без затримки і відволікання уваги), як правило, пасивна (не потребує жодних дій зі сторони людини), не обмежують користувача у вільному переміщенні та відносно недорогога.

Найчастіше в технічній літературі згадується 3 методи: кореляційний (метод узгодженої фільтрації); метод на основі перетворень Каруна-Лоева і поняття «власних облич» (EigenFace); метод на основі лінійного дискримінантного аналізу і поняття Fisherface (від імені вченого Роберта Фішера).

В даний час розвиваються методи, які орієнтуються на: репрезентативний характер вихідних даних – навчання системи в різних умовах; зменшення розмірності вихідних даних; розпізнавання в обмеженому просторі ознак.

Якщо умови отримання нових образів відповідають умовам отримання еталона (освітлення, точка огляду лица, поворот, масштаб, фон), то кореляція між ними близька до одиниці. Рівень розпізнавання сягає 96%.

Проте, якщо умови змінюються лінійна корекція стає непотрібною. Розвитком цього методу є перехід від вихідних ознак до інваріантів Фур'є-Мелліна (замінують поворот на циклічний зсув), що дозволяє досягти високої кореляції між образами.

Метод на основі перетворень Каруна-Лоева дозволяє значно зменшити розміри еталону, залишаючи тільки ті ознаки, які мають принципове значення для конкретного образу. При цьому вплив умов отримання образу не такі помітні, а порівняння образів спрощується. Рівень правильного розпізнавання стабільно сягає 80% навіть при сильних змінах умов.

Метод на основі лінійного дискримінантного аналізу (ЛДА), як і попередній дозволяє скоротити кількість ознак, при цьому суттєво покращити класифікацію образів (відділення один від одного). Це дозволяє збільшити рівень розпізнавання до 99% навіть при умовах, які сильно відрізняються.

Якщо взяти результат після перетворень Каруна-Лоева в якості вихідних даних і застосувати метод ЛДА, можна додатково скоротити простір ознак.

Після застосування методу ЛДА, окремі образи в кластері стали ближчими до центру і практично не перекривають чужої території, самі центри віддалилися один від одного ще далше. Вибір виділення ознак відіграє ключову роль в розпізнаванні образів [6].

Висновок

В даній роботі було розглянуто найперспективніші технології ідентифікації особи і описано принцип роботи кожної з цих технологій. Ідентифікація за відбитком пальця найбільш поширеніший метод, проте в даний час великого розвитку набувають технології ідентифікації особи на основі розпізнавання обличчя та райдужної оболонки ока. Ці методи в залежності від технології і способу розпізнавання мають малий рівень помилок першого і другого роду.

Для ефективної ідентифікації необхідно використовувати одночасно кілька технологій, наприклад, ідентифікацію відбитка пальця і обличчя, що створює найбільшу ймовірність точної ідентифікації особи.

Список літератури

1. Вікіпедія [Електронний ресурс]. – Режим доступу до док.: <http://uk.wikipedia.org/wiki/Ідентифікація>.
2. Типи ідентифікації користувачів [Електронний ресурс]. – Режим доступу до док.: <http://www.infobezpeka.com/publications/?id=92>.
3. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека / Г.А. Кухарев. – Политехника, 2001. – 240 с.
4. Revett Kenneth. Behavioral biometrics / Kenneth Revett. – John Wiley and Sons, 2008. – 480 p.
5. Ratha Nalini K. Advances in Biometrics / Nalini K. Ratha, Venu Govindaraju. – Springer Science+Business Media, 2008. – 660 p.
6. Dunstone Ted. Biometric system and data analysis / Ted Dunstone, Neil Yager. – Springer Science+Business Media, 2009. – 720 p.

Надійшла до редколегії 30.03.2010

Рецензент: д-р техн. наук, проф. В.Б. Дудикевич, Національний університет «Львівська політехніка», Львів.

ИССЛЕДОВАНИЯ И АНАЛИЗ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ В ЗАЩИЩЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ СВЯЗИ

Ю.Р. Гарасим, Т.Б. Крет

Работа посвящена исследованию и анализу технологий идентификации лица по его биометрическим признакам. Рассмотрены наиболее перспективные и наиболее актуальные в настоящее время технологии биометрической идентификации лица. Проанализированы существующие методы идентификации, определены их недостатки и преимущества.

Ключевые слова: идентификация лица, биометрические методы защиты, биометрические сканеры, защищенные корпоративные сети связи.

PERSON IDENTIFICATION PERSPECTIVE TECHNOLOGIES IN SECURE ENTERPRISE COMMUNICATION NETWORKS RESEARCH AND ANALYSES

I.R. Garasym, T.B. Kret

Work is devoted research and analysis of technologies of authentication of person on his biometrical signs. The most perspective are considered and the most actual presently technologies of biometrical authentication of person. The existent methods of authentication are analysed, their failings and advantages are certain.

Keywords: authentication of person, biometrical methods of defence, biometrical scanners, protected corporate communication networks.