УДК 004.93

Г. М. Новіцький
Л. Г. Коваль
М. І. Паламарчук

ШЛЯХИ ПІДВИЩЕННЯ ТОЧНОСТІ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Вінницький національний технічний університет

Анотація. У доповіді розглянуто й проаналізовано основні методи підвищення точності біометричної ідентифікації, а також основні помилки методів біометричної ідентифікації.

Ключові слова: біометрична ідентифікація, профілі біометричні, розпізнавання, біометрична система, сканер, точність ідентифікації, біометрія.

Помилки під час ідентифікації людини можливі з ряду причин, наприклад, збою в роботі датчика, недоліків скануючого пристрою, обмежень методів обробки, мінливості біометричних характеристик, заміна зловмисниками відомостей у базі даних тощо. [1]

Головними задачами помилкової ідентифікації є мінімізація хибних невідповідностей і відповідностей. У першому випадку зчитування даних особи слід здійснювати згідно з переліком встановлених правил (наприклад, вірне положення пальця під час дактилоскопії, обличчя особи під час ідентифікації за геометрією обличчя, вірне положення ока під час сканування райдужної оболонки тощо). У другому випадку певна особа володіє дуже близькими чи подібними параметрами із тією, що записана в базі даних, і тоді система спрацює невірно, визнавши цю особу за істинну. Допоможе тут виключно дослідження іншої біометричної характеристики цієї людини. [2]

Оскільки первинним пристроєм зняття інформації для ідентифікації особи є сканер, то якість його роботи істотно впливатиме на подальшу обробку інформації. Тому з кожним роком системи біометричної ідентифікації обладнуються більш точними скануючими пристроями, а також такими, що володіють більшою роздільною здатністю; наприклад, оптичні сканери відбитків пальців замінюються в ряді випадків ультразвуковими сканерами. Щоправда, як ті, так і інші вірно знімуть дані лише за умови відповідної чистоти поверхні пальця досліджуваного об’єкта.

Інший спосіб підвищення точності біометричних систем – покращення якості алгоритмів, що використовуються. З кожним роком алгоритми вдосконалюються, оскільки технології біометрії розвиваються швидкими темпами, з’являються нові і вдосконалюються старі алгоритми ідентифікації.

Одним із способів підвищення точності систем біометричної ідентифікації, як вже було зазначено вище, є інтеграція різних методів ідентифікації особи. Це призводить до зростання матеріальних затрат на ідентифікацію, однак результат стає набагато ближчим до бажаного.

Інший спосіб боротьби із помилками під час ідентифікації – використання надійніших методів, які дозволяють усунути вплив як зовнішніх факторів (включаючи механічні пошкодження частин тіла, за якими здійснюється ідентифікація), так і можливості створення різноманітних макетів-замінників злочинцями. [1]

На відміну від методу ідентифікації за геометрією обличчя ідентифікація за венами долоні більш точна й надійна, порівнянна з точністю ідентифікації за райдужною оболонкою для одного ока. Стабільність отримуваних результатів ідентифікації пояснюється тим, що русла кровоносних судин не змінюються з віком. Їх форма й розташування мало залежать від різних захворювань, наприклад варикозу або тромбозу. Це забезпечує стабільні результати ідентифікації протягом багатьох років. На результати сканування вен практично не впливають зовнішні умови, наприклад, коли руки мокрі, обмерзлі або брудні. Ця особливість дозволяє успішно використовувати метод для ідентифікації на виробництві. Не потрібно безпосереднє торкання, що більш гігієнічно в порівнянні з ідентифікацією за відбитком пальця. Проведені медичні дослідження й отримані висновки, що даний метод ідентифікації абсолютно нешкідливий для людини.

Принцип сканування кровоносних судин використовується не тільки для ідентифікації за венами долоні, а й, наприклад, за венами пальця. У фалангах пальця значно менше кровоносних посудин, і така ідентифікація менш точна в порівнянні з ідентифікацією за венами долоні. Для підвищення точності пропонується проводити ідентифікацію одночасно за кількома пальцями.

Оскільки за звичайних умов малюнок вен неможливо побачити, то й створення муляжу для обману цього методу є абсолютно неможливим. Вени не залишають слідів на поверхні, їх не можна сфотографувати звичайним фотоапаратом або записати на диктофон. На теперішній момент це найбільш надійний метод біометричної ідентифікації, який не вдалося обдурити за допомогою різних муляжів. Він широко розповсюджений у Японії та країнах Скандинавії.

Розглянемо останній із способів впливу на точність біометричної ідентифікації – захист шаблонів із бази даних, доступ до яких можуть отримати зловмисники. [1]

Існує два загальних принципи: трансформація біометричних рис та біометричні криптосистеми.

У випадку трансформації біометричних рис захищений шаблон отриманий за рахунок застосування незворотної функції трансформації до оригіналу шаблону. Така трансформація зазвичай базується на індивідуальних характеристиках користувача. У процесі автентифікації система застосовує ту ж функцію трансформації до запиту, і зіставлення відбувається вже для трансформованого зразка.

Біометричні криптосистеми зберігають тільки частину інформації, отриманої з біометричного шаблону, – ця частина називається захищеним ескізом. Хоча його самого недостатньо для відновлення оригінального шаблону, він все ж містить необхідну кількість даних для відновлення шаблону при наявності іншого біометричного зразка, схожого на отриманий під час реєстрації.

Захищений ескіз зазвичай отримують шляхом зв’язування біометричного шаблону із криптографічним ключем, однак захищений ескіз – це не те ж саме, що біометричний шаблон, зашифрований за допомогою стандартних методів. За звичайної криптографії зашифрований шаблон і ключ розшифрування – це дві різні одиниці, і шаблон захищений, тільки якщо захищений і ключ. У захищеному шаблоні ж вміщуються одночасно і біометричний шаблон, і криптографічний ключ. Ні ключ, ні шаблон не можна відновити, маючи тільки захищений ескіз. Коли системі надають біометричний запит, досить схожий на шаблон, вона може відновити і оригінальний шаблон, і криптоключ за допомогою стандартних методів розпізнавання помилок.

Дослідники запропонували два основні методи генерації захищеного ескізу: нечітке зобов’язання і нечіткий сейф. Перший можна використовувати для захисту біометричних шаблонів, представлених у вигляді двійкових рядків фіксованої довжини. Другий корисний для захисту шаблонів, представлених у вигляді наборів крапок.

Зіставлення у схемі із трансформацією рис часто відбувається прямо, і можлива навіть розробка функцій трансформації, що не міняють характеристик вихідного простору ознак. Однак буває складно створити вдалу функцію трансформації, незворотну й терпиму до неминучої зміни біометричних рис користувача згодом.

Хоча для біометричних систем існують методи генерації захищеного ескізу, які базуються на принципах теорії інформації, труднощі полягають у тому, щоб подати ці біометричні риси в стандартизованих форматах даних на зразок двійкових рядків і наборів крапок. Тому одна з актуальних тем досліджень – розробка алгоритмів, що перетворять оригінальний біометричний шаблон у такі формати без втрат значущої інформації. [2]

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних закладів] / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.:
2. SABI – биометрическая идентификация нового поколения [Електронний ресурс] /Режим доступу : https://xakep.ru/2018/10/10/sabi.

Новіцький Геннадій Михайлович – біомедичний інженер, випускник аспірантури, м. Вінниця, email: novitskyi@vntu.edu.ua

Коваль Леонід Григорович — канд. техн. наук, доцент кафедри біомедичної інженерії, Вінницький національний технічний університет, м. Вінниця, email: koval.l@vntu.edu.ua.

Паламарчук Михайло Ігорович – аспірант кафедри біомедичної інженерії, Вінницького національного технічного університету.

WAYS TO IMPROVE THE ACCURACY OF BIOMETRIC IDENTIFICATION SYSTEMS

Abstract. The main methods of increasing the accuracy of biometric identification, as well as the main errors of biometric identification methods are considered and analyzed in the article.

Key words: biometric identification, biometric profiles, recognition, biometric system, scanner, identification accuracy, biometrics.

Gennady Novitsky – biomedical engineer, graduate of Ph.D. programme, Vinnytsya, email: novitskyi@vntu.edu.ua

Koval Leonid - Cand. Sc. (Eng), Associate Professor of the Department of Biomedical Engineering, Vinnytsia National Technical University, Vinnytsia, email: koval.l@vntu.edu.ua.

Palamarchuk Mykhailo – Postgraduate of the Department of Biomedical Engineering, Vinnytsia National Technical University.