УДК 343.982.325

Т. В. Юрчик
головний судовий експерт

Харківський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ В ДАКТИЛОСКОПІЇ

У цій статті автором розглянуті загальні питання і методи біометричних технологій, технічні аспекти реєстрації і розпізнавання відбитків пальців, достоїнства і недоліки процедури перевірки достовірності особи для необхідного рівня безпеки біометричних систем, наведені приклади технологій виготовлення фальшивих дактилоскопічних відбитків, а також переваги багатофакторної аутентифікації.

Ключові слова: *ідентифікація, аутентифікація, верифікація особи, мініатюри.*

Ідентифікація людини за відбитками пальців – одне з практичних застосувань біометричних технологій. Поняття біометрії з'явилося в кінці XIX століття та має на увазі розділ науки, що займається кількісними біологічними експериментами з залученням методів математичної статистики.

В кінці XX століття зацікавленість біометрією отримала новий стимул, у зв'язку з використанням так званих біометричних систем безпеки, суть яких полягає у використанні електронних систем розпізнавання особистості по унікальним біологічним ознаками і у визначенні, таким чином, прав доступу цієї особи до тієї чи іншої системи. Біометрія в основному займається двома питаннями: отримання даних та їх верифікація (ідентифікація особистості) – порівняння щойно отриманих даних з даними, які отримані раніше і зберігаються в пам'яті. Ідентифікація людини за відбитками пальців на сьогоднішній день – найпоширеніша з біотехнологій. Сканерами відбитків пальців обладнують комп'ютери, в тому числі ноутбуки, мобільні телефони, навіть комп'ютерні «миші». І, вже звичайно, в останні роки з'явилося безліч пристроїв доступу, що використовують як ключ малюнок на пальці [1].

Якщо спробувати проаналізувати періодику з даної теми, то створюється враження, що біометричні технології – панацея від усіх бід, пов'язаних з забуванням паролів, крадіжкою ключів (нехай навіть електронних, у вигляді пластикової картки), підглядання ПІН-кодів і так далі.

Основа будь-якої біометричної системи контролю доступу – сенсор, який «знімає» якісь фізичні характеристики людини. Вихідний

сигнал сенсора перекладається в цифрову форму, проводиться витяг тільки корисної інформації за допомогою математичних алгоритмів (цифровий процесор сигналів) і збереження отриманої інформації в пам'яті. Керуючий мікроконтролер забезпечує необхідну послідовність дій системи, управління потоками даних та взаємодією із зовнішнім світом (наприклад, відкриває двері при позитивній ідентифікації).

Чорно-білий малюнок відбитка пальця при 256 градаціях сірого займає приблизно 80 кілобайт пам'яті. Сучасні алгоритми перетворять таку картинку в шаблон обсягом близько 256 байт, що дозволяє зберігати в реальних системах сотні і тисячі таких шаблонів.

При ідентифікації людини проводиться повторне зняття відбитка, перетворення його в шаблон з використанням тих же алгоритмів, що і при занесенні шаблону в пам'ять і порівняння двох отриманих шаблонів між собою для прийняття рішення про їх ідентичність [2].

Головне, що треба мати на увазі – це те, що шаблон, одержуваний з одного і того ж пальця кілька разів поспіль, щоразу буде різним! Таким чином, просте порівняння двох 256-байтових масивів для визначення їх ідентичності ніколи не дасть бажаного результату – така система ніколи не впустить вас в приміщення.

У системах, що працюють з відбитками пальців, використовуються два основні методи: кореляційний і метод мініатюр. Перший з них є досить універсальним, і може використовуватися практично у всіх біометричних технологіях. Другий є основним методом саме в дактилоскопії.

Зі сканера ми отримуємо монохромне зображення папілярних ліній пальця. Для підвищення достовірності ідентифікації наступним кроком, як правило, є попередня обробка зображення, що сприяє підвищенню його чіткості і контрастності. Потім в зображенні визначаються тип, вид папілярного узору і його окремі ознаки (мініатюри) – початок, закінчення, розгалуження, злиття і т.і. [3, с. 67]. Отримані таким чином дані – опис типу і взаємного положення характерних точок зображення – і складають шаблон, який зберігається в пам'яті для подальшого порівняння.

Порівняння збереженого в пам'яті і знову отриманого шаблону ускладнюється тим, що неможливо двічі однаково прикласти палець до сканера. При цьому відбувається не тільки зміщення і поворот зображення, а й деформація, втрата частини мініатюр. Додайте до цього такі проблеми, як порізи, опіки, хвороби – і ви зрозумієте, що все це сильно ускладнює завдання математиків, що розробляють алгоритми ідентифікації, а також час, необхідний для сканування і порівняння одного відбитка в сучасних автономних системах ідентифікації по пальцях, становить від 0,1 до 1 секунди.

Це означає, що при установці чисто дактилоскопічної системи на прохідній, через яку проходить понад тисячу осіб, кожен буде чекати прийняття рішення про допуск більше хвилини.

Проблема швидкості реакції системи вирішується на сьогоднішній день таким способом: ідентифікацію, тобто порівняння отриманого шаблону з усією базою даних раніше запам'ятованих еталонних шаблонів, замінюється верифікацією, тобто порівнянням знову отриманого при скануванні відбитка з єдиним зразком. Цей єдиний зразок вибирається з бази даних за рахунок того, що користувач попередньо ідентифікує себе введенням коду з клавіатури, пред'явленням платіжної картки або іншим аналогічним способом. Один з оригінальних способів скорочення апаратних витрат і скорочення часу ідентифікації полягає в тому, що зразковий шаблон зберігається не в пам'яті системи, а в ідентифікаторі, який пред'являє користувач, тобто в карті або брелку. Система в цьому випадку сканує палець, витягуючи з відбитка поточний шаблон, а зразковий шаблон зчитує з ідентифікатора і порівнює їх для прийняття рішення.

Оскільки, дактилоскопічні системи свідомо не дають гарантії правильної ідентифікації, для їх характеристики фахівці ввели два дуже важливих параметри: рівень помилкового допуску і рівень помилкової відмови. Перший визначає ймовірність допуску до захищається стороннього, коли система приймає його за «свого». Другий параметр, навпаки, визначає ймовірність того, що людина, відбиток якого є в базі даних, не буде допущений (з першого разу – з другого або третього він, може бути, і пройде) [4, с. 13].

Будучи і так не надто високими, ці два параметри ще до того ж сильно пов'язані між собою, так що розробнику системи доводиться балансувати між двох крайнощів, вибираючи зовні найбільш привабливий варіант. Типові значення першої помилки – від 0,1 % до 0,001 %, другої помилки – від 1 % до 0,01%. Хоча деякі компанії і заявляють рівень обох помилок не гірше 0,0001%, ці дані є некоректними, оскільки не існує навіть єдиної об'єктивної методики вимірювання помилок.

Ще один сумний факт. Люди всі різні, і не тільки тому, що мають різні відбитки, але і тому, що одні їх мають, а інші – ні! І якщо вхід на фірму захищений дактилоскопічним зчитувачем, а у вас з відбитками між погано і дуже погано, то як ви потрапите на роботу? Така статистика є (в різних джерелах дані трохи відрізняються): близько 5–8 % людей мають «погані» з точки зору розпізнавання відбитки, а від 2 до 3 % – не мають їх взагалі (різні патології і захворювання шкірного покриву) [5, с. 38, 187].

Також варто відзначити, що немає такої системи, яку людина не може обдурити. Професор Мацумото і група його студентів в Університеті Йокогами – не професіонали в галузі тестування біометричних систем, а займаються математичними аспектами захисту інформації. Однак, з чисто аматорського ентузіазму дослідників вистачило, щоб створити дві дуже ефективні технології для виготовлення фальшивих дактилоскопічних відбитків.

У першому (тривіальний) методі японці безпосередньо робили зліпок з пальця «жертви», для чого використовувався харчовий желатин і формувальний пластик, застосовуваний авіа- і судомоделісти. Желатинову смужку-відбиток можна непомітно приліпити до власного пальця і обдурити комп'ютерну систему доступу навіть в присутності охоронця. Ця не хитра технологія спрацювала в 80 відсотках випадків при тестуванні більш десятка комерційних приладів біометричного захисту.

Проте, ще більш ефективним виявився другий («високотехнологічний») метод, розроблений надихнути від першого успіху групою Мацумото. Тут вже не потрібно палець «жертви», а обробляється один із залишених ним відбитків (згідно з дослідженнями експертів, людина щодня залишає на різних предметах в середньому близько 25 виразних «пальців»). Знявши відбиток пальця зі скла, дослідники поліпшили його якість за допомогою ціан-акрилатного адгезиву (парів супер-клею) і сфотографували результат цифровою камерою. Потім контрастність знімка була оптимізована за допомогою графічного редактора, після чого картинку роздрукували на прозорій плівці. Для виготовлення же об'ємного відбитка Мацумото скористався методом фотолітографії: в магазині для радіоаматорів студенти купили світлочутливу друковану плату-заготовку, спроектували на неї «палець» з плівки і витравили відбиток на міді. Ця плата стала формою для желатинового «фальшивого пальця», який виявився настільки хороший, що обманював практично всі з випробуваних біометричних систем, як з оптичними, так і ємкісними сенсорами.

Після деякого тренування желатиновий зліпок дозволив дослідникам-любителям обманювати і більш просунуті системи, обладнані «детекторами живого пальця», що реагують на вологість або електричний опір. Немає сумніву, що професіоналам в цій галузі вдається проробляти набагато більш вражаючі трюки [6].

Виходячи з викладеного вище, оцінити надійність системи не уявляється можливим. Занадто багато залежить від випадку. Звичайно, поки захист недостатньо вдосконалений, і до 100 % її надійність явно не дотягує, але в поєднанні з іншими способами захисту може дати непоганий ефект.

Крім біометричних систем, традиційно питання аутентифікації користувачів вирішується за допомогою логіна і пароля, пластикових карт з вбудованою мікросхемою (але при використанні смарт-карти як ідентифікатора неминуче з'являються нові проблеми: якщо для фальсифікації облікового запису необхідно якимось чином дізнатися пароль, то в даному випадку нічого, крім карти, не потрібно), сканера райдужної оболонки ока дає хорошу достовірність, але занадто дорогий, до того ж, є шанс його скомпрометувати за допомогою

фотографії високої роздільної якості; лазерний сканер дна ока надзвичайно складно обдурити, але він комерційно невигідний, а технології розпізнавання особи на поточному етапі їх розвитку мають недостатньо високу надійність.

Таким чином, кожен з вищеописаних методів аутентифікації має власні переваги і недоліки, і для забезпечення необхідного рівня безпеки раціонально їх комбінувати, тобто вводити багатофакторну аутентифікацію [7].

До кожного технічного рішення треба підходити розумно і зважено, особливо якщо це пов'язано з вкладенням грошей і забезпеченням безпеки підприємства.

Перелік посилань

1. *Двоеносова Г., Двоеносова М.* Біометрія як наука, метод та спосіб документування. Управление персоналом № 11. 2009 [Електронний ресурс]. Режим доступу: http://www.top-personal.ru/issue.html?2039.

2. *Лиса Н. В., Новікова К. Ю., Помулев В. В., Кавац О. О., Стовпченко І. В.* Методичні вказівки до виконання лабораторних робіт з дисципліни «Теорія алгоритмів і математичні основи подання знань» 2011 [Електронний ресурс]. Режим доступу: https://nmetau.edu.ua/file/teoriya_algoritmov_metodichka.

3. *Прокопович Р. О., Барташук С. С., Коректор О. П.* Методика дактилоскопічної експертизи. Експертна спеціальність 4.6 «Дактилоскопічні дослідження» 2014. *Лебеденко Ю. І.* Біометричні системи безпеки, 2012 [Електронний ресурс]. Режим доступу: https://books.google.com.ua/books?isbn=5767923779

4. *Самищенко С. С.* Атлас незвичайних папілярних узорів, 2001.

5. *Берд К.* Біометрія як вона є [Електронний ресурс]. Режим доступу: https: www/kinet.ru/cterra/445/18034.html

6. *Шаханова М. В.* Сучасні технології інформаційної безпеки, 2015 [Електронний ресурс]. Режим доступу: https://books.google.com.ua/books?isbn=539218958X

АСПЕКТЫ ДАКТИЛОСКОПИИ В ІНДУСТРИИ

Т. В. Юрчик

Суть биометрических систем безопасности, заключается в использовании электронных систем распознавания личности по уникальным биологическим признакам и в определении прав доступа этого лица к той или иной системе. Биометрия занимается двумя вопросами: получение данных и их верификация (идентификация личности) – сравнение только что полученных данных с данными, полученными ранее и хранящимися в памяти. Идентификация человека по отпечаткам пальцев на сегодняшний день – самая распространенная биотехнология.

Основа любой биометрической системы контроля доступа – сенсор, который «снимает» какие-то физические характеристики человека. Выходной сигнал сенсора переводится в цифровую форму, проводится извлечение только полезной информации с помощью математических алгоритмов и сохранения полученной информации в памяти.

При идентификации человека производится повторное снятие отпечатка, превращение его в шаблон с использованием тех же алгоритмов, что и при занесении шаблона в память и сравнение двух полученных шаблонов между собой для принятия решения об их идентичности.

В системах, работающих с отпечатками пальцев, используются два основных метода: корреляционный и метод миниатюр. Первый из них является достаточно универсальным и может использоваться практически во всех биометрических технологиях. Второй является основным методом именно в дактилоскопии, но сравнение сохраненного в памяти и вновь полученного шаблона осложняется тем, что невозможно дважды одинаково приложить палец к сканеру. При этом происходит не только сдвиг и поворот рисунков, но и деформация, потеря части миниатюр.

Проблему сокращения аппаратных расходов можно решить, заменив идентификацию, то есть сравнения полученного шаблона со всей базой данных ранее воспринятых и сохраненных эталонных шаблонов, верификацией, то есть сравнением вновь полученного при сканировании отпечатка с единственным образцом. Этот единственный образец выбирается из базы данных за счет того, что пользователь предварительно идентифицирует себя введением кода с клавиатуры, предъявлением платежной карты или другим аналогичным способом.

Дактилоскопические системы не дают гарантии правильной идентификации, на этот счет ввели два очень важных параметра: уровень ложного допуска и уровень ложного отказа. Первый определяет вероятность допуска к защищаемому стороннего, когда система принимает его за «своего». Второй параметр, наоборот, определяет вероятность того, что человек, отпечаток которого в базе данных, не будет допущен (с первого раза – со второго или третьего он, может быть, и пройдет).

Еще один печальный факт. Некоторые люди не имеют на пальцах папиллярного узора. Такая статистика есть: около 5 – 8% людей имеют «плохие» с точки зрения распознавания отпечатки, а от 2 до 3% – не имеют их вообще (различные патологии и заболевания кожного покрова). Также установлены факты изготовления фальшивых отпечатков.

Помимо биометрических систем, вопрос аутентификации пользователей решается с помощью:

– логина и пароля;

– пластиковых карт со встроенной микросхемой (но при использовании смарт-карты в качестве идентификатора неизбежно появляются новые проблемы: если для фальсификации учетной записи необходимо каким-то образом узнать пароль, то в данном случае ничего, кроме карты, не требуется);

– сканера радужной оболочки глаза (дает хорошую достоверность, но чересчур дорог, к тому же, есть шанс его скомпрометировать с помощью фотографии высокого разрешения);

– лазерный сканер дна глаза чрезвычайно сложно обмануть, но он коммерчески невыгоден.

Каждый из вышеописанных методов аутентификации имеет собственные преимущества и недостатки, и для обеспечения необходимого уровня безопасности рационально их комбинировать, то есть вводить многофакторную аутентификацию. К каждому техническому решению надо подходить разумно и взвешенно, особенно если это связано с вложением денег и обеспечением безопасности предприятия.

ASPECTS OF SCIENCE OF FINGERPRINTS IN THE INDUSTRY

T. Yurchuk

The essence of biometric security consists in the use of electronic identification systems based on unique biological features and in determining the access rights of this person to one or another system. Biometrics deals with two issues: data acquisition and verification (identification of the personality) – comparison of newly obtained data with data obtained earlier and stored in memory. Identification of fingerprints by today is the most commonly used biotechnology.

The basis of any biometric access control system is a sensor that “removes” some physical characteristics of a person. The output signal of the sensor is translated into a digital form, extracting only useful information using mathematical algorithms and preserving the received information in memory.

When identifying a person, a reprint is taken, transforming it into a template using the same algorithms as when inserting the template into memory and comparing the two templates obtained with each other to decide on their identity.

In systems that work with fingerprints are used two main methods: correlation and method of miniatures. The first one is rather universal and can be used practically all biometric technologies. The second is the main method in fingerprinting, but the comparison of the template in memory and the newly received template is complicated by the fact that it is impossible to attach the finger to the scanner twice equally. In this case, there is not only a shift and rotation of the drawings, but also deformation, the loss of part of the miniatures.

The problem of reduction of hardware expenses can be solved having replaced identification that is comparisons of the received template with the database of earlier remembered reference templates, verification that is comparisons of the print which is again received when scanning with the only sample. This only sample gets out of the database because the user identifies previously also make introduction of a code from the keyboard, presentation of the payment card or other similar way.

Dactyloscopic systems do not guarantee the correct identification, on this account, introduced two very important parameters: the level of false admission and the level of false failure. The first determines the probability of admittance to the third party protected when the system accepts it as its own. The second parameter, on the contrary, determines the probability that a person whose imprint in the database will not be allowed (from the first time, from the second or third time, perhaps, a person may be passed).

And it is one more sad fact... Some people do not have a papillary pattern on their fingers. There is a following statistics: about 5-8% of people have “bad” prints from the point of view of recognition, and from 2 to 3% do not have them at all in general (various pathologies and skin diseases). The facts of making false prints are also established.

Besides biometric systems, the question of authentication of users is solved with the help:

– login and password;

– plastic cards with the built-in chip (but when using a smart card as the identifier new problems inevitably appear: if there is a need to learn the password in some way for falsification of the account, then in this case nothing except the card is required);

– an iris scanner (gives good reliability, but too expensive, moreover, there is a chance to compromise it by means of the photo of high resolution);

– the laser scanner of a bottom of an eye it is extremely difficult to deceive, but it is commercially unprofitable.

Each of the above described methods of authentication has its own advantages and disadvantages, and for ensuring necessary level of safety it is rational to combine them, that is to implement multiple-factor authentication. It is necessary to approach each technical solution reasonably and deliberately, especially if it is connected with an investment of money and safety of the enterprise.

УДК 343.983

А. В. Кофанов
кандидат юридичних наук,
доцент, доктор філософії, професор

Національна академія внутрішніх справ

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ АСПЕКТИ МОДЕЛЮВАННЯ РИКОШЕТУВАННЯ ВОГНЕПАЛЬНОГО СНАРЯДА ПРИ ПРОВЕДЕННІ ЕКСПЕРТНОГО ЕКСПЕРИМЕНТУ

У статті розглянуто теоретичні та практичні аспекти моделювання рикошету при проведенні експертного експерименту в умовах обмеженого простору (в лабораторних умовах). Проаналізовано методологічні засади та передумови створення і вдосконалення відповідної криміналістичної техніки. Наведено статистичні результати проведених експертних експериментів із різними поверхнями перешкод, що найбільш часто зустрічаються при оглядах місць події за фактами використання (застосування) вогнепальної зброї або конструктивно схожих із нею предметів. Лаконічно сформульовані можливості і переваги використання комплексу технічних засобів моделювання та дослідження рикошетування вогнепального снаряда при проведенні експертного експерименту.

Ключові слова: *моделювання, рикошетування, вогнепальне, снаряд, експертний експеримент.*

Історія вивчення вогнепальних ушкоджень налічує кілька століть. До початку 21-го століття у вивченні судово-медичної балістики