

БІОМЕТРИЧНІ СИСТЕМИ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

*Лазука В., студ. (гр. ФБ-42, ФТІ НТУУ «КПІ ім. Ігоря Сікорського»);
Чернушак І. І., ст. викл. (каф. ОПЦБ НТУУ «КПІ ім. Ігоря Сікорського»)*

У сучасному інформаційному суспільстві актуальним для кожної країни є прагнення загальної цифрової ідентифікації громадян. Впровадження для кожної людини обов'язкових атрибутів – ідентифікаційного коду, електронного цифрового підпису, паспортних даних, номеру соціального страхування – потребує надійної ідентифікації, пов'язаної з біологічними особливостями людини (статичними та динамічними), на основі яких можна встановити її особистість у розподілених інформаційних мережах. Біометричні розробки впроваджувались вже не один десяток років, але до цього часу застосовувались переважно в критичних інформаційних структурах, доступ до яких мала обмежена кількість людей. Це пояснює факт наявності пристроїв для проведення біометричної ідентифікації, які є надійними, але доволі складними та повільними, до того ж ті пристрої мають високу вартість, тому не можуть бути застосовані для великої кількості осіб в межах всього кіберпростору нашої планети.

На сьогодні все більше людей потребує надійної біометричної ідентифікації для можливості роботи з різноманітними інформаційними системами. Можна назвати багато таких систем: мобільний банкінг, банкомати, система відеоспостереження на автобанах, система електронного уряду та інші. Таки системи характеризуються великою кількістю учасників, так що їх можна називати масовими. Якщо розглядати міста, де можуть мешкати десятки мільйонів жителів (у Токіо на серпень 2016 року мешкало 38,5 млн. жителів, розмір міста визначався за світловою плямою вночі), то для інформаційних систем такого міста потрібна потужна система біометричної ідентифікації. При впровадженні масових систем біометричної ідентифікації доводиться йти на компроміс між швидкістю та результативністю (якістю розпізнавання). Таким чином, є необхідність у розробці масових систем біометричної ідентифікації, які б відповідали сучасним вимогам швидкодії та результативності.

На даний час невирішеною проблемою є вибір ефективних методів і засобів автентифікації та ідентифікації біометричних даних для конкретних інтелектуальних інформаційних систем.

Ідентифікація особи (лат. *Identificare*) - ототожнювати. Встановлення тотожності особистості людини за сукупністю ознак шляхом порівняльного їх дослідження. У слідчій та судовій практиці здійснюють Ідентифікація особи підозрюваних у скоєнні злочину, кримінальних злочинців, невідомих осіб, затриманих правоохоронними органами, невідомих трупів та ін.

Існує обмежена кількість характерних властивостей особистості, які можуть бути використані для її ідентифікації:

- те, чим володіє особистість (розпізнавальний знак, ключ або пластикова картка);
- те, що знає особистість (секретна інформація, пароль, персональний ідентифікатор);
- особливості поведінки (мова, почерк, характер роботи на клавіатурі);
- деякі фізичні характеристики (відбитки пальців, форма руки, візерунок кровоносних судин).

Ці властивості використовуються в повсякденній практиці при спілкуванні людей один з одним для впізнання візитерів, повідомлень і т.д. На їх основі створені спеціальні автоматичні прилади і розроблені методи ідентифікації особи.

Біометрія (англ. Biometrics) - технологія ідентифікації особи, яка використовує фізіологічні параметри суб'єкта (відбитки пальців, райдужна оболонка ока і т. д.)

Кожна людина індивідуальна, іншого такого немає, не було і не буде. Проведені більше 20 років дослідження підтверджують це. Розроблено математичні методи, що дозволяють по частині тіла людини, його фотографії, голосу, підпису стверджувати, що це один і той же чоловік (біометрична ідентифікація особи). Такі методи дозволяють впевнено ідентифікувати людину.

На сьогоднішній день існує велика кількість методів біометричної ідентифікації, які поділяють на 2 основні групи – статичні та динамічні.

Статистичні методи

Статичні методи біометричної аутентифікації ґрунтуються на фізіологічній (статичній) характеристиці людини, тобто унікальній характеристиці, даній їй від народження.

- Автоматичний face-контроль

Макіяж, вікові зміни, вживання міцних напоїв — всі ці чинники погіршують ідентифікацію особи по обличчю. Навіть для експерта ідентифікація людини по фотографії десятирічної давності може виявитися дуже складним завданням. Біометричні технології дозволяють проводити face-контроль в автоматичному режимі, вони звіряють параметри обличчя об'єкта, який зафіксований камерою, з даними в базі. І достовірність такого аналізу складає 86–93%. Це значно більше за звичайні людські можливості. Проте проблема полягає в тому, що для здійснення цієї функції необхідне устаткування високої якості. Навіть для проведення візуальної ідентифікації особи відстань між центрами зіниць має бути еквівалентною 200 пікселям.

Сюди входять такі методи, як аутентифікація людини за формою обличчя, термограмою обличчя.

- За формою обличчя

У даному методі ідентифікації будується тривимірний образ обличчя людини. На обличчі виділяються контури брів, очей, носа, губ і т.д., обчислюється відстань між ними і будується не просто образ, а ще безліч його

варіантів на випадки повороту особи, нахилу, зміни виразу. Кількість образів варіюється залежно від мети використання даного способу (для аутентифікації, верифікації, видаленого пошуку на великих територіях і т.д.).

- За термограмою обличчя

В основі даного способу аутентифікації лежить унікальність розподілу на обличчі артерій, що забезпечують кров'ю шкіру і виділяють тепло. Для здобуття термограми використовуються спеціальні камери інфрачервоного діапазону. На відміну від попереднього цей метод дозволяє розрізняти близнят.

- За відбитком пальця

В основі цього методу лежить унікальність для кожної людини малюнка папілярних узорів на пальцях. Відбиток, отриманий за допомогою спеціального сканера, перетворюється в цифровий код (згортку) і порівнюється з раніше введеним еталоном. Дана технологія є найрозповсюдженішою в порівнянні з іншими методами біометричної аутентифікації.

- За формою долоні

Даний метод побудований на геометрії грона руки. За допомогою спеціального пристрою, що складається з камери і декількох підсвічуючих діодів (включаючись по черзі, вони дають різні проекції долоні), будується тривимірний образ грона руки, за яким формується згортка і розпізнається людина.

- За розташуванням вен на лицьовій стороні долоні

За допомогою інфрачервоної камери прочитується малюнок вен на лицьовій стороні долоні або грона руки. Отримана картинка обробляється, і за схемою розташування вен формується цифрова згортка. Ця технологія досить надійна. Основний її недолік полягає в тому, що якщо за відбитками пальців можна перевірити, чи не знаходиться людина в розшуку, чи має вона судимість, то для таких біометричних параметрів, як венозний малюнок, єдиної бази не існує.

- За сітківкою ока

Це спосіб ідентифікації по малюнку кровоносних судин очного дна. Для того, щоб цей малюнок став видний, людині потрібно поглянути на видалену світлову крапку, і очне дно, що таким чином підсвічується, сканується спеціальною камерою.

- За радужною оболонкою ока

Малюнок радужної оболонки ока також є унікальною характеристикою людини. Причому для її сканування досить портативної камери із спеціалізованим програмним забезпеченням, що дозволяє захоплювати зображення частини лица, з якого виділяється зображення ока, з якого, у свою чергу, виділяється малюнок веселкової оболонки, за яким і будується цифровий код для ідентифікації людини.

При використанні цієї технології об'єкта необхідно позиціонувати свою особу для реєстрації якісного зображення веселкової оболонки очей, що, звичайно, не завжди зручно. Наприклад, при фасе-контролі подібних вимог не існує. Людина йде по коридору, в той момент, коли вона попаде в зону

найкращого бачення, камера робить контрольний знімок. При ідентифікації особи за зображенням обличчя і радужної оболонки ока необхідно враховувати також і зовнішні умови. Залежно від фону і рівня освітленості вірогідність розпізнавання міняється. Тому в ідеалі треба помістити людину в стандартизовані умови, наприклад, в ізольовану кабінку.

- За ДНК

Переваги даного способу очевидні, проте використовувані в даний час методи здобуття і обробки ДНК працюють настільки довго, що такі системи використовуються лише для спеціалізованих експертиз.

- Інші методи

У даній статті описані лише найпоширеніші методи. Існують ще такі унікальні способи, як ідентифікація за піднігтьовим шаром шкіри, за об'ємом вказаних для сканування пальців, формою вуха, запахом тіла тощо.

Динамічні методи

Динамічні методи біометричної аутентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії.

Розглянемо методи аутентифікації цієї групи.

- За почерком

Як правило, для цього виду ідентифікації людини використовується його розпис (інколи написання кодового слова). Цифровий код ідентифікації формується залежно від необхідної міри захисту і наявності устаткування (графічний планшет, екран карманного комп'ютера Palm і т.д.) двох типів:

За самим розписом, тобто для ідентифікації використовується просто міра збігу двох картинок.

За розписом і динамічними характеристиками написання, тобто для ідентифікації будується згортка, в яку входить інформація по безпосередньому підпису, тимчасовим характеристикам нанесення розпису і статистичним характеристикам динаміки натиску на поверхню.

- За клавіатурним почерком

Метод у цілому аналогічний описаному, але замість розпису використовується кодове слово (коли для цього використовується особистий пароль користувача, таку аутентифікацію називають двофакторною) і не потрібно жодного спеціального устаткування, окрім стандартної клавіатури. Основною характеристикою, за якою будується згортка для ідентифікації, є динаміка набору кодового слова.

- За голосом

Одна із старих технологій, у даний час її розвиток прискорився, оскільки передбачається її широке використання в побудові «інтелектуальних будівель». Існує досить багато способів побудови ідентифікації за голосом, як правило, це різні поєднання частотних і статистичних характеристик голосу.

- Інші методи

Для даної групи методів також описані лише найпоширеніші методи. Існують такі унікальні способи, як ідентифікація за рухом губ при відтворенні кодового слова, за динамікою повороту ключа в дверному замку і т.д.

Загальною характеристикою, яку використовують для порівняння різних методів і способів біометричної ідентифікації, є статистичні показники: помилка першого роду (не пустити в систему «свого») і помилка другого роду (пустити в систему чужого).

Сортувати і порівнювати описані вище біометричні методи за свідченнями помилок першого роду дуже складно, оскільки вони є різними для одних і тих же методів у зв'язку з залежністю від устаткування, на якому вони реалізовані.

За показниками помилок другого роду загальне сортування методів біометричної аутентифікації виглядає приблизно так (від кращих до гірших):

- ДНК.
- Радужна оболонка ока, сітківка ока.
- Відбиток пальця, термограма обличчя, форма долоні.
- Форма обличчя, розміщення вен на долоні та кисті руки.
- Розпис.
- Клавіатурний почерк.
- Голос

Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об'єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; системи електронної комерції; інформаційна безпека (доступ в мережу, вхід на ПК); облік робочого часу і реєстрація відвідувачів; системи голосування; проведення електронних платежів; аутентифікація на web-ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (пересічення державних кордонів, видача віз на відвідини країни) і т.д.

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або до пристрою може бути прикладена велика фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої вже не попадаються на такі прості виверти. Так що зловмисникам доводиться видумувати все нові й нові способи обману біометричних сканерів.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер. Варто також відзначити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова в доступі зареєстрованому користувачеві). Тому користувачеві

доводиться вибирати, який пристрій придбати – дорожчий й кращий або дешевший й гірший.

Враховуючи, що більшість методів представляє собою комерційну таємницю, в даному випадку важко виділити кращий метод, оскільки порівнювати доцільно алгоритмічно-апаратний комплекс. Зараз проводяться розробки по зменшенню розмірів та ціни системи, збільшенню надійності роботи. Для систем, що вимагають особливі вимоги до безпеки, використовуватимуться мультимодальні біометрики. Використання біометричних засобів спрощує процедуру аутентифікації особи, а також піднімає надійність систем безпеки.

Література

1. Біометрія як універсальний спосіб ідентифікації людини [Електронний ресурс]. – Режим доступу: <http://bablyukh.clan.su/publ/1-1-0-4>
2. DigitalPersona Fingerprint Identity Solutions for Identity Protection, Security and Compliance [Електронний ресурс]. – Режим доступу: <http://www.digitalpersona.com>.
3. Identix – Protecting and Securing Personal Identities and Assets [Електронний ресурс]. – Режим доступу: <http://www.11id.com/pages/17>.
4. BioAPI Consortium (Биометрический консорциум) [Електронний ресурс]. – Режим доступу: <http://www.bioapi.org>
5. А. Мороз «Біометричні технології ідентифікації людини. Огляд систем»