ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

ОСНОВНІ БІОМЕТРИЧНІ ХАРАКТЕРИСТИКИ, СУЧАСНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

Валеріян Швець, Андрій Фесенко

Національний авіаційний університет, Україна

ШВЕЦЬ Валеріян Анатолійович, к.т.н., доцент

Рік та місце народження: 1959 рік, с. Окниця, Молдова.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1986 рік.
Посада: завідувач кафедри засобів захисту інформації з 2004 року.
Наукові інтереси: цифрова обробка сигналів, біометрика, інформаційна безпека.
Публікації: понад 60 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: hvan@nau.edu.ua

ФЕСЕНКО Андрій Олексійович

Рік та місце народження: 1988 рік, смт. Дігтярі, Чернігівська обл., Україна.
Освіта: Національний авіаційний університет, 2011 рік.
Посада: аспірант з 2012 року.
Наукові інтереси: інформаційна безпека, біометрична аутентифікація.
Публікації: 3 наукові статті у фахових виданнях України.
E-mail: a.fesenko@meta.ua

Анотація. *У даній статті досліджено біометричні характеристики людини, за допомогою яких здійснюється їх ідентифікація. Наведено основні характеристики сучасних біометричних технологій, а також класифікацію біометричних методів ідентифікації. Крім того, проведено аналітичне дослідження сучасних методів біометричної аутентифікації, виділено їх переваги та недоліки.*

Ключові слова: *захист інформації, біометрія, біометрична характеристика, біометрична технологія, ідентифікація, аутентифікація, характеристики біометричних технологій.*

Постановка задачі дослідження. Слово *біометрія* має грецьке походження – «*bio*» – життя, «*metron*» – вимірювання. Саме поняття «біометрія» з'явилося наприкінці дев'ятнадцятого століття і має на увазі розділ науки, що займається кількісними біологічними експериментами з залученням методів математичної статистики. Наприкінці двадцятого століття інтерес до біометрії значно зріс завдяки тому, що ця галузь науки знайшла своє застосування в розробках нових технологій безпеки, суть яких зводиться до використання комп'ютерних систем розпізнавання особистості за унікальним генетичним кодом людини. Фізіологічні особливості, наприклад, такі, як папілярний візерунок пальця, геометрія особи, температура шкіри обличчя, модель райдужної оболонки ока, геометрія долоні, сітківка ока, структура ДНК, форма вуха, характеристики клавіатурного набору, особливості підпису та багато інших є постійними і незмінними характеристиками людини. Ваш голос відкриває двері будинку, де ви живете, модель райдужної оболонки ока дозволяє пройти в офіс знайомої вам компанії, відбиток вашого пальця відкриває доступ до комп'ютерної системи. Таким чином, ви самі є ключем. Проте, сучасні наукові джерела [1-6] не містять детального опису основних біометричних характеристик, класифікації методів та порівняльного аналізу сучасних систем і технологій

біометричної аутентифікації. З огляду на це, **метою** статті є ґрунтовний аналіз основних біометричних характеристик, сучасних систем і технологій біометричної аутентифікації класифікація.

Основна частина дослідження. *Біометричними характеристиками людини (БХЛ)* називається її вимірювана фізична характеристика або персональна поведінкова риса. Ідентифікація людини реалізується в процесі перевірки БХЛ на ідентичність зареєстрованому користувачеві [2]. Перелічимо *основні біометричні характеристики людини,* за допомогою яких здійснюється їх ідентифікація (табл. 1) [3]: відбитки пальців; форма і геометрія обличчя; форма і будова черепа; сітківка ока; райдужна оболонка ока; геометрія долоні, кисті руки або пальця; термографія особи, термографія руки; малюнок вен на долоні або пальці руки; ДНК; запах тіла; форма вуха; динаміка підпису; динаміка клавіатурного набору; голос; рух губ; хода; особливості накреслення рукописного тексту. Ідеальна характеристика повинна легко збиратись, бути універсальною, унікальною и постійною [3]. *Універсальність* – можливість представлення людини однією характеристикою. *Унікальність* означає, що не повинно бути двох осіб з ідентичними характеристиками. *Сталість (перманентність)* – характеристика не повинна змінюватися з часом. *Збирання (вимірюваність)* – можливість швидко і легко одержати та деталізувати характеристику від індивідуума.

Таблиця 1

Експертна оцінка властивостей БХЛ: (+ + + – висока оцінка, + + – середня, + – низька)

Характеристика	Універсальність	Унікальність	Сталість	Вимірюваність
Відеообраз обличчя	+++	+	++	+++
Термограмма обличчя	+++	+++	+	+++
Відбиток пальця	++	+++	+++	++
Геометрія руки	++	++	++	+++
Райдужна оболонка ока	+++	+++	+++	++
Сітківка	+++	+++	++	+
Підпис	+	+	+	+++
Голос	++	+	+	++
Відбиток губ	+++	+++	++	+
Особливості вуха	++	++	++	++
Динаміка підпису	+++	+++	+	+++
Хода	+++	++	+	+

Протягом останніх десятиліть дорогі та складні біометричні системи використовуються в зонах підвищеної безпеки. Існує цілий ряд біометричних технологій, заснованих на біометричних характеристиках голови (зображення обличчя, райдужна оболонка ока, сітчаста оболонка ока, форма вуха), тіла (сканування відбитків пальців, геометрія руки, аналіз крові, ДНК) або поведінки (голос, рукописна підпис, хода, клавіатурний почерк). Тільки деякі з вище перерахованих технологій технічно доступні і готові до масового продажу за прийнятною ціною [6]. *Біометрична система* – це автоматизована система, що вирішує задачі реєстрації користувачів і їх ідентифікації. Ця система реалізує наступні функції: фіксація біометричних характеристик; вилучення біометричних даних з вибірки; порівняння біометричних даних з одним або великою кількістю еталонів; прийняття рішень про відповідність даних; формування результату про дійсність; прийняття рішень про повторення, закінчення або зміну процесу ідентифікації або автентифікації.

Біометричні технології – це методи отримання біометричних характеристик людини. При цьому використовуються як фізичні, так і поведінкові характеристики людини. У біометричних системах ідентифікаційними ознаками є особистість людини. В основі ідентифікації і автентифікації цього типу лежить процедура зчитування представленої біометричної ознаки користувача і її порівняння з попередньо отриманим шаблоном [6]. Біометричні системи ідентифікації особистості розрізняються ще по ряду показників: пропускна здатність; вартість; надійність з позиції ідентифікації; простота і зручність у використанні; ступінь психологічного комфорту; можливість обману системи; спосіб зчитування; точність встановлення автентичності; збільшена продуктивність; витрати на обслуговування; інтеграція; конфіденційність. Пропускна здатність системи в цьому випадку характеризується часом, необхідним для обслуговування одного користувача. Вона залежить, зокрема, від режиму роботи пристрою (проводиться ідентифікація або автентифікація). При ідентифікації користувача потрібно більше часу, ніж для автентифікації, оскільки необхідно порівняти зі зразком майже всі еталони з бази даних. У режимі автентифікації користувач повинен набрати на клавіатурі свій персональний код (номер еталона в базі даних), і системі досить порівняти пред'явлений зразок з одним еталоном. У багатьох системах ці режими може вибрати адміністратор. Вартість є одним з визначальних чинників широкого використання біометричних систем. Вартість цих систем досить висока в самих країнах-виробниках і значно зростає, коли системи доходять до кінцевих споживачів. Тут позначаються і митні тарифи, і прибуток, який закладається продавцями. Трохи краще в ціновому аспекті справи з вітчизняними розробками. Причому якість ідентифікації багатьох з них вище західних аналогів. Одна ж із серйозних проблем, що стримують поширення наших розробок, – рівень виробництва, що не дозволяє вийти на закордонний ринок. Говорячи про

надійність біометричної системи з позиції ідентифікації, ми маємо дві ймовірності. Йдеться про ймовірність «помилкових відмов» (система не визнала свого) і «помилкових допусків» (система прийняла «чужого» за «свого»). Це особливо важка і складна область біометрії, тому що система повинна пропускати менше число самозванців і в той же час відкидати менше число законних користувачів.

Простота і зручність у використанні багато в чому визначають споживчі властивості біометричних систем. Адже всі часто задають наступні питання. Наскільки легко встановити дану біометричну систему? Чи потребує система активної участі користувача або отримання характеристик надто обтяжливо? Чи потребує система тривалого навчання? Чи не станеться так, що обтяжлива або громіздка біометрична система автентифікації буде відкинута так само, як ми відмовляємося від використання систем, що вимагають введення довгих паролів? Ступінь психологічного комфорту визначає, наскільки ті чи інші системи та методи визначення біометричних характеристик здатні викликати у користувачів негативну реакцію, страх або сумнів. Наприклад, окремі люди побоюються, скажімо, дактилоскопії, а інші не бажають дивитися у об'єктив відеокамери з лазерною підсвіткою. Можливість обману системи пов'язана з використанням різних «дублікатів»: зліпків, магнітофонних записів і т.д. Найбільш «легковірними» вважаються системи ідентифікації по обличчю й голосу [5]. Спосіб зчитування визначає, чи потрібно користувачеві прикладати свій палець до зчитувача, притулятися обличчям до окуляра і т.д. або достатньо продемонструвати «електронному» пристрою атрибут, необхідний для ідентифікації, наприклад, вимовити умовну фразу або подивитися в об'єктив відеокамери. Виходячи з цього, розрізняють два способи зчитування – дистанційний і контактний. Технологія дистанційного зчитування дозволяє збільшити пропускну спроможність, уникнути регулярного очищення зчитувача і виключити його знос, збільшити вандалозахищеність і т.д. Точність автентифікації під час використання біометричних систем дещо відрізняється від точності систем, що використовують паролі. Надання коректного пароля в системі автентифікації за паролем завжди дає коректний результат про підтвердження автентичності. Але якщо в біометричну систему автентифікації представлені законні (справжні) біометричні характеристики, це, тим не менш, не гарантує коректної автентифікації. Таке може статися через «шум» давача, обмежень методів обробки і, що ще важливіше, мінливості біометричних характеристик. Є також ймовірність, що може бути підтверджена справжність людини, що видає себе за законного користувача. Більш того, точність даної біометричної реалізації має важливе значення для користувачів, на яких розрахована система. Для успішного застосування біометричної технології з метою ідентифікації особистості важливо розуміти і реально оцінювати цю технологію в контексті програми, для якого вона призначена, а також враховувати склад користувачів цієї програми. Продуктивність залежить від таких параметрів, як точність, вартість, інтеграція та зручність використання, інформації в цих системах. Іншими словами, чи не будуть біометричні дані використовуватися для стеження за людьми і порушення їх права на приватне життя. Щоб забезпечити соціально-правовий захист користувача, багато закордонних виробників зчитувачів зобов'язалися зберігати в базі даних не зображення відбитку, а деякий отриманий з нього ключ, за яким відновлення відбитку неможливо.

Розглянемо, як же працює будь-яка біометрична система, що використовує фізіологічні або поведінкові характеристики людини. Основа будь-якої біометричної системи розпізнавання особистості – давач, який видає сигнал, промодульований в залежності від фізичних особливостей конкретної людини. Далі відбувається перетворення аналогового сигналу в цифровий формат, видаляється вся непотрібна інформація і отримана матриця (шаблон) зберігається в пам'яті. Сучасні системи розпізнавання за відбитками пальців, наприклад, мають матрицю об'ємом менше 100 байт. Замість інформації про відбитки пальців може використовуватися інформація про всю долоню, венозний малюнок зап'ястя, райдужну оболонку очей. Дана інформація може поєднуватися з інформацією про голос, почерк, ходу.

Біометрична система – це система розпізнавання шаблона, яка встановлює автентичність конкретних фізіологічних або поведінкових характеристик користувача. Логічно біометрична система може бути розділена на два модулі [5]: модуль реєстрації; модуль ідентифікації. Модуль реєстрації відповідає за «навчання» системи ідентифікувати конкретну людину. На етапі реєстрації біометричні давачі сканують зображення обличчя людини для того, щоб створити його цифрове представлення. Спеціальний модуль обробляє це подання, щоб виділити характерні особливості і згенерувати більш компактне і виразне представлення, що називається шаблоном. Для зображення обличчя такими характерними рисами можуть стати розмір і розміщення очей, носа і рота. Шаблон для кожного користувача зберігається в базі даних біометричної системи. Ця база даних може бути централізованою або розподіленою, коли шаблон кожного користувача залишається на смарт-картці і передається користувачеві. Модуль ідентифікації відповідає за розпізнавання користувача комп'ютера. На етапі ідентифікації біометричний давач знімає характеристики людини, ідентифікація якого проводиться, і перетворює ці характеристики в той же цифровий формат, в якому зберігається шаблон. Отриманий шаблон порівнюється з тим, що зберігається, щоб визначити, чи відповідають ці шаблони один одному. Ідентифікація може виконуватися у вигляді верифікації, автентифікації (перевірка затвердження типу «Я – Сергій Петров») або розпізнавання, визначаючи особистість людини з бази даних про людей, відомих системі (визначення того, хто я, не

знаючи мого імені). У верифікаційній системі, коли отримані характеристики і збережений шаблон користувача, за якого себе видає людина, збігаються, система підтверджує ідентичність. Коли отримані характеристики і один з збережених шаблонів виявляються однаковими, система розпізнавання ідентифікує людину з відповідним шаблоном.

Наведемо основні характеристики біометричних технологій [4]: FTE (failure to enroll) – помилка зняття характеристики (помилка реєстрації в системі); час розпізнавання; стійкість до навколишнього середовища (експлуатаційні якості можуть втрачати стабільність в залежності від оточуючих умов); стійкість до підробки (несанкціонованого доступу); соціальна прийнятність – згода людей на збір даних; точність – будь-яку біометричну систему можна налаштувати на різну пильність; вартість. Крім того, у кожній з реалізацій технології можна виділити також наступні характеристики: FRR (false rejection rate) – частота помилок «першого роду» – помилкова відмова; FAR (false acceptance rate) – частота помилок «другого роду» – помилковий допуск. Для користувачів також важливі такі характеристики: можливість ідентифікації і автентифікації; складність реалізації систем ідентифікації; досягнута точність (рівень FRR і FAR); можливість безконтактного зчитування; розміри файла-еталона (чим більше розмір образу, тим повільніше йде розпізнавання).

Переваги біометричних систем безпеки очевидні [4,5]: унікальні людські якості добрі тим, що їх важко підробити, важко залишити фальшивий відбиток пальця за допомогою свого власного або зробити райдужну оболонку свого ока схожою на чиюсь іншу. На відміну від паперових ідентифікаторів (паспорт, водійські права, посвідчення особи), від пароля або персонального ідентифікаційного номера (ПІН), біометричні характеристики не можуть бути забуті або втрачені, в силу своєї унікальності вони використовуються для запобігання крадіжки або шахрайства. Деякі люди вміють імітувати голоси, а в Голлівуді навчилися гримувати людей так, що вони стають вражаюче схожі на інших, але, погодьтеся, це вимагає особливих навичок, які не часто зустрінеш в повсякденному житті. Основна ж *слабкість біометрії,* на думку фахівців [3-5], полягає в тому, що біометричні дані можна викрасти після того, як вони отримані. Розглянемо, наприклад, біометричну систему перевірки відбитків пальців для одержання віддаленого доступу до сервера. Ви кладете палець на зчитувач, вбудований в мишу або клавіатуру, комп'ютер надсилає цифрований відбиток пальця на сервер. Сервер порівнює його з збереженим зразком і при збігу дозволяє вам доступ. Але ця схема недостатньо ефективна просто тому, що «вкрасти» цифрований відбиток пальця не складе труднощів для досвідченого хакера, і як тільки йому це вдасться, він зможе обманювати сервер знову і знову. Висновок полягає в тому, що біометричні характеристики добре працюють тільки тоді, коли оператор може перевірити дві речі: по-перше, що біометричні дані отримані від конкретної особи саме під час перевірки; по-друге, що ці дані збігаються із зразком, який зберігається в картотеці. Якщо система не в змозі цього зробити, вона не буде працювати. Біометричні характеристики є унікальними ідентифікаторами, але питання їх надійного зберігання і захисту від перехоплення, як і раніше залишається відкритим [4].

Класифікація біометричних методів ідентифікації. Людині властиво розвиватися, міняти свої звички, зовнішність і поведінку, однак у неї є й ознаки, що залишаються незмінними протягом всього життя, наприклад, малюнок відбитка пальця або кровоносних судин очного дна. І ті й інші властивості можуть використовуватися біометричними системами як критерій ідентифікації. І залежно від цього методи біометричної ідентифікації діляться на дві великі групи – статистичні й динамічні.

Статичні – велика група біометричних продуктів, побудованих на аналізі відкритих статичних (незмінних) образів особистості, даних їй від народження і на які оточуючі звертають свою увагу без особливих зусиль. Статичні методи ідентифікації засновані на аналізі незмінних фізіологічних характеристик людини. До числа цих характеристик входять [6]: відбитки пальців (на використанні цих ідентифікаторів будується найпоширеніша, зручна і ефективна біометрична технологія); форма і геометрія обличчя (з цими ідентифікаторами працюють технології розпізнавання двовимірних зображень облич); форма і будова черепа (для більшої благозвучності компанії, що діють в даній сфері, вважають за краще говорити про технології розпізнавання людини за тривимірною моделлю обличчя); сітківка ока (практично не використовується в якості ідентифікатора); райдужна оболонка ока (розповсюдження технології, в якій застосовується цей ідентифікатор, стримується патентними обмеженнями); геометрія долоні, кисті руки або пальця (використовується в декількох вузьких сегментах ринку); термографія особи, термографія руки (засновані на використанні цих ідентифікаторів технології не набули поширення); малюнок вен на долоні або пальці руки (відповідна технологія стає популярною, але з огляду на ціну сканерів поки не використовується широко); ДНК (в основному в сфері спеціалізованих експертиз); запах тіла (автоматичних систем розпізнавання людини, що використовують даний ідентифікатор, ще не створено); форма вуха (автоматичних систем розпізнавання людини, що використовують даний ідентифікатор, ще не створено).

Динамічні – пристрої і біометричні програми, побудовані на аналізі динамічних образів особистості. Динамічні образи відображають особливості характерних особистості швидких підсвідомих рухів у процесі відтворення контрольного слова рукописним почерком або при проголошенні контрольного слова голосом. Параметри, що контролюються «динамічною біометрією» можуть бути легко змінені автором

шляхом зміни контрольного слова-пароля. Динамічні методи істотно поступаються статичним в точності та ефективності і, як правило, використовуються як допоміжні [6]. Застосовувані ідентифікатори: динаміка підпису; динаміка клавіатурного набору; голос; рух губ; хода; особливості накреслення рукописного тексту. На рис 1. наведено сегментацію сучасного біометричного ринку за використовуваними ідентифікаторами [3]. Статична і динамічна біометрії – це дві взаємодоповнюючі одна одну ланки. Основна перевага статичної біометрії – відносна незалежність від психологічного стану користувачів, малі витрати їхніх зусиль і, отже, можливість організації біометричної ідентифікації великих потоків людей.

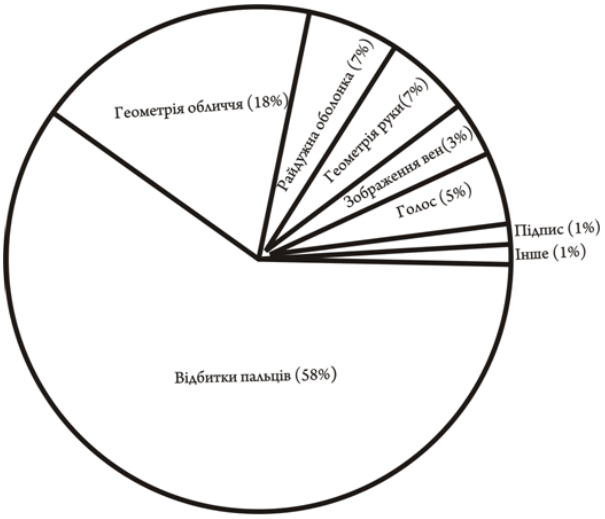

Рис. 1. Сегментація біометричного ринку по застосовуваним ідентифікаторам (за даними компанії Acuity Market Intelligence)

Аналітичне дослідження сучасних методів біометричної аутентифікації. Ідентифікація людини за допомогою відбитків пальців. Розпізнавання відбитків пальців це одна з найпростіших і добре відомих біометричних технологій. Комерційні ідентифікаційні системи автоматичного розпізнавання відбитків пальців з'явилися ще в 60-х роках XIX століття [6]. Але і до недавнього часу ці системи в основному використовувалися правоохоронними органами при розслідуванні злочинів.

Ідея ідентифікації особистості на основі папілярних малюнків пальців рук була запропонована двома авторами - Г. Фулдсом і В. Гершелем - у статті авторитетного англійського журналу «Nature» в 1880 році. У 1864 році доктор Нейман Гроу опублікував перші роботи з пропозицією ідентифікації особи за відбитками пальців. ФБР наприкінці минулого століття зробив перші кроки в цьому напрямку. У 1895 році дактилоскопія як метод реєстрації злочинців введена в Англії. А вже в 1905 році в Лондонському суді був юридичний прецедент, коли підсудний був засуджений до смертної кари на підставі ідентифікації відбитків його пальців. У Росії дактилоскопія як метод реєстрації злочинців стала використовуватися з 1907 року.

Розпізнавання відбитків пальців – це один з найпростіших і добре відомих біометричних методів ідентифікації особи. Саме він виявився найбільш практичним щодо реалізації та сприйняття його людьми і саме він використовується вже тривалий час. Відбитки пальців у всіх людей абсолютно різні. Всі люди, що населяють в наш час Землю, мають, притаманні тільки їм одним, певні відбитки пальців. І навіть відбитки пальців всіх попередніх поколінь людей також відмінні від всіх наступних. Правоохоронні органи в усьому світі використовують ідентифікацію за відбитками пальців вже більше ста років, причому до сьогодні не виявлено жодного випадку збігу відбитків пальців у різних людей, включаючи навіть однояйцевих близнят. У силу цього саме відбитки пальців руки однієї людини вважаються специфічною, притаманною тільки цій людині «особистою карткою», і саме в такій якості ця властивість застосовується в усьому світі. Але така особливість пальців руки людини була виявлена лише до кінця XIX століття. До того часу вони представлялися людям просто набором ліній, нічого не позначають і не володіли якимись особливостями.

Шкіра людини складається з двох шарів, при цьому нижній шар утворює безліч виступів – сосочків (від лат. Papillae – сосочок), у вершині яких є отвори вихідних проток потових залоз. На основній частині шкіри сосочки (потові залози) розташовуються хаотично і їх важко побачити. У кожному відбитку пальця можна визначити два типи ознак: глобальні; локальні. Глобальні ознаки – це ті ознаки, які можна побачити неозброєним оком. На окремих ділянках шкіри кінцівок папілляри строго впорядковані в лінії (гребені) і утворюють так звані унікальні папілярні візерунки. Ці візерунки і відображають всю людську індивідуальність. На рис. 2 наведено типи папілярних візерунків.

Рис. 2. Типи папілярних візерунків (1 … 4 – візерунки типу «петля» (ліва, права, центральна, подвійна), 5 і 6 – візерунки типу «дельта» або «дуга» (проста і гостра), 7 і 8 – візерунки типу «спіраль» (центральна та змішана))

Інший тип ознак – локальні [4]. Їх називають минуціями - унікальні для кожного відбитка ознаки, що визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розрив і т.д.), орієнтацію папілярних ліній і координати в цих пунктах. Кожен відбиток містить до 70 минуцій. Область образу – виділений фрагмент відбитку, в якому локалізовані всі ознаки. Ядро – пункт,

локалізований в середині відбитку або деякої виділеної області. Пункт «дельта» – початкова точка. Місце, в якому відбувається розділення або підключення борозенок папілярних ліній, або дуже коротка борідка (може доходити до точки). Тип лінії – дві найбільші лінії, які починаються як паралельні, а потім розходяться і огинають всю область образу. Лічильник ліній – число ліній на області образу або між ядром і пунктом «дельта».

Рис. 3. Локальні типи ознак – минуції

На рис 3. відзначені такі ознаки: дві лінії – «тип лінії»; те, що між ними – може виступати в якості області образу, але зазвичай береться вся площа відбитка; червоне коло ліворуч – пункт «дельта»; червоне коло нижче – ядро; жовті кола показують деякі минуції; папілярний візерунок – ліва петля. Практика показує, що відбитки пальців різних людей можуть мати однакові глобальні ознаки, але зовсім неможливо наявність однакових мікровізерунків минуцій. Тому глобальні ознаки використовують для розділення бази даних на класи і на етапі автентифікації. На другому етапі розпізнавання використовують вже локальні ознаки. Зараз в основному для розпізнавання відбитків пальців використовуються стандарти ANSI і ФБР США [7], у державах СНД – також і російські [8-11]. У них визначено наступні вимоги до образу відбитка: кожен образ представляється у форматі не стисненого TIF; образ повинен мати розширення не нижче 500 dpi; образ повинен бути напів тоновим з 256 рівнями яскравості; максимальний кут повороту відбитка від вертикалі не більше 15 градусів; основні типи минуцій – закінчення і роздвоєння.

Розглянемо наступні принципи порівняння відбитків за локальними ознаками: 1) Етап 1. Поліпшення якості початкового зображення відбитка. Збільшується різкість кордонів папілярних ліній. 2) Етап 2. Обчислення поля орієнтації папілярних ліній відбитка. Зображення розбивається на квадратні блоки, зі стороною більше 4 пікселів і за градієнтами яскравості обчислюється кут t орієнтації ліній для фрагмента відбитка. 3) Етап 3. Бінаризація зображення відбитка. Приведення до чорно-білого зображення (1 bit) пороговою обробкою. 4) Етап 4. Стоншення ліній зображення відбитка. Потоншення проводиться до тих пір, поки лінії не будуть шириною 1 піксель. 5) Етап 5. Виділення минуцій. Зображення розбивається на блоки 9x9 пікселів. Після цього підраховується число чорних (ненульових) пікселів, що знаходяться навколо центру. Піксель в центрі вважається минуцією, якщо він сам ненульовий, і сусідніх ненульових пікселів один (минуція «закінчення») або два (минуція «роздвоєння»). Координати виявлених минуцій та їх кути орієнтації записуються у вектор: W (p) = [(x1, y1, t1), (x2, y2, t2)...(xp, yp, tp)] (p – число минуцій). При реєстрації користувачів цей вектор вважається еталоном і записується в базу даних. При розпізнаванні вектор визначає поточний відбиток (що цілком логічно). 6) Етап 6. Зіставлення минуцій. Два відбитки одного пальця будуть відрізнятися один від одного поворотом, зсувом, зміною масштабу та / або площею дотику в залежності від того, як користувач прикладає палець до сканера. Тому не можна сказати, чи належить відбиток людині чи ні на підставі простого їхнього порівняння (вектори еталона і поточного відбитка можуть відрізнятися по довжині, містити невідповідні минуції і т.д.). Через це процес зіставлення повинен бути реалізований для кожної минуції окремо. Етапи порівняння: реєстрація даних; пошук пар відповідних минуцій; оцінка відповідності відбитків; при реєстрації визначаються параметри афінних перетворень (кут повороту, масштаб і зрушення), за яких деяка минуція з одного вектора є певною минуції з другого. Під час пошуку для кожної минуції потрібно перебрати до 30 значень повороту (від -15 градусів до +15), 500 значень зсуву (від -250 пкс до 250 пкс - хоча, звісно, межі вибирають і трохи менше ...) і 10 значень масштабу (від 0,5 до 1,5 з кроком 0,1). Разом до 150000 кроків для кожної з 70 можливих минуцій. Оцінка відповідності відбитків виконується за такою формулою:

$$K = \left(D \cdot D \cdot 100\ \%\right) / \left(p \cdot q\right),$$

де D – кількість минуцій, що збігалися; p – кількість минуцій еталона; q – кількість минуцій ідентифікованого відбитка).

У випадку, якщо результат перевищує 65 %, відбитки вважаються ідентичними (поріг може бути знижений виставлянням іншого рівня пильності). Якщо виконувалася автентифікація, то на цьому все і закінчується. Для ідентифікації необхідно повторити цей процес для всіх відбитків в базі даних (потім вибирається користувач, у якого найбільший рівень відповідності (зрозуміло, його результат повинен бути вище за поріг 65 %)). Незважаючи на те, що описаний вище принцип порівняння відбитків забезпечує високий рівень надійності, тривають пошуки більш досконалих (і швидкісних) методів порівняння. Розглянемо метод на основі глобальних ознак. При цьому виконується виявлення глобальних ознак (ядро, дельта). Кількість цих ознак і їх взаємне розташування дозволяє класифікувати тип візерунка. Остаточне розпізнавання виконується на основі локальних ознак (число порівнянь виходить на кілька порядків нижче для великої бази даних). Вважається, що тип візерунка може визначати характер, темперамент і здібності людини, тому цей метод можна використовувати і в цілях, відмінних від ідентифікації / автентифікації. Розглянемо метод порівняння відбитків на основі графів (рис 4).

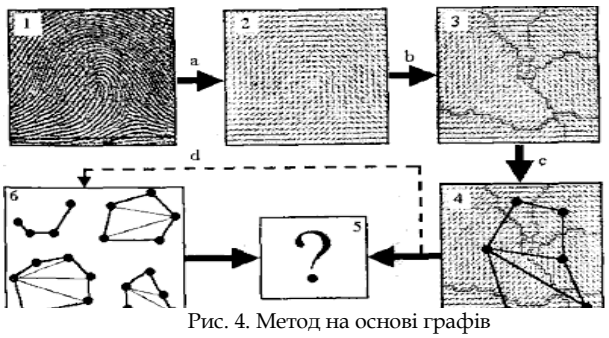

Рис. 4. Метод на основі графів

Початкове зображення відбитка (1) перетворюється на зображення поля орієнтації папілярних ліній (2). На ньому (2) помітні області з однаковою орієнтацією ліній, тому можна провести межі між цими областями (3). Потім визначаються центри цих областей і виходить граф (4). Стрілкою «d» відзначений запис в базу даних при реєстрації користувача. Визначення подібності відбитків реалізовано в квадраті 5. (Подальші дії аналогічні попередньому методу - порівняння за локальними ознаками). Розпізнавання відбитків пальців здійснюється за допомогою сучасних сенсорів відбитків пальців. Вони точніше й ефективніше в обробці необхідної інформації, ніж їх більш ранні аналоги. Крім того, ціни на них значно нижчі, ніж на інші біометричні пристрої [6]. Незважаючи на зовнішні відмінності, всі сканери можна розділити на кілька видів: 1) Оптичні: FTIR-сканери; оптоволоконні; оптичні протяжні; роликові; безконтактні. 2) Напівпровідникові (напівпровідники змінюють властивості в місцях контакту): ємнісні; чутливі до тиску; термосканери; радіочастотні; протяжні термосканери; ємнісні протяжні; радіочастотні протяжні. 3) Ультразвукові (ультразвук повертається через різні проміжки часу, відбиваючись від борозенок або ліній).

Перевагою ультразвукового сканування є можливість визначити необхідні характеристики на брудних пальцях і навіть через тонкі гумові рукавички. Крім того, всі прилади зчитування розрізняються за видом, як, наприклад, зовнішні сканери для робочих станцій, ноутбуків і портативних комп'ютерів. Вбудовані сканери відбитків пальців для цих типів систем також починають з'являтися, як і сканери відбитків для стільникових телефонів. Переваги доступу за відбитком пальця – це простота використання, зручність та надійність. Весь процес ідентифікації займає мало часу і не вимагає зусиль від тих, хто використовує дану систему доступу. У будь-якій такій системі клієнтові спочатку пропонують прикласти свій палець (будь-який) до віконця розпізнавального пристрою. На першому етапі інформація, отримана від зображення пальця, використовується для формування так званого шаблону. Ця операція займає 10-15 с. Потім система пропонує людині пред'явити палець ще кілька разів, щоб перевірити придатність занесеної в пам'ять інформації. Процес реєстрації займає кілька хвилин. Основним елементом пристрою є сканер, що зчитує папілярний візерунок, який потім обробляється за допомогою спеціального алгоритму, і отриманий код порівнюється із шаблоном, що зберігається в пам'яті.

Існує два основних алгоритми порівняння: за характером точок; за рельєфом всієї поверхні пальця. Перший алгоритм виявляє характерні ділянки і запам'ятовує їх розташування. У другому випадку аналізується усе «зображення» в цілому. При розпізнаванні за характерними точками виникає шум високого рівня, якщо палець у поганому стані. При розпізнаванні за всією поверхнею цього недоліку немає, але є інший: потрібно дуже акуратно розміщувати палець на скануючому елементі. У сучасних системах використовується також комбінація обох алгоритмів, за рахунок чого підвищується рівень надійності системи. Сформований шаблон заноситься в базу даних системи, в пам'ять головного комп'ютера або мікропроцесорної картки, або в інший пристрій зберігання цифрових даних і виходить такий собі цифровий індекс. Обсяг збереженої еталонної інформації може бути істотно зменшений, якщо зробити класифікацію за характерними типами папілярних малюнків і виділити на відбитку мікроособливості, що являють собою початок (закінчення) папілярних ліній або їх злиття (розгалуження). У пропонованих на ринку засобах ідентифікації за відбитком пальця інформація про відбитки, що зберігається в базі даних оператора системи, як правило, недостатня для повної реконструкції відбитка. Це важливо, оскільки виключається використання такої інформації в будь-яких інших цілях, наприклад, при розслідуванні злочину. У деяких системах можна зареєструвати відбитки декількох пальців однієї людини, повторивши процес реєстрації для кожного пальця, який ви захочете використовувати для ідентифікації, але кожен палець можна зареєструвати тільки один раз. Ще один аспект безпеки розглянутих систем пов'язаний з використанням різних фальшивок. Замовники часто вимагають від постачальників, щоб система розпізнавала випадки представлення зліпків пальців, виконаних, наприклад, із силікону. Жодна з систем ідентифікації за відбитком пальця не забезпечує надійного захисту від підробок. Можна лише розраховувати на те, що зробити гарний зліпок зовсім не так просто, і в більшості випадків для цього необхідно співучасть зареєстрованої людини. Тим не менше, для захисту від пред'явлення фальшивого пальця вживаються різні заходи (типу аналізу колірного спектру чи оцінки коефіцієнта відбиття).

Ідентифікація людини за допомогою її очей. Існує багато систем ідентифікації, де як ключ використовуються очі людини. Ці системи можна розділити на два різновиди, що використовують різні ідентифікатори: у першому випадку як «носій» ідентифікаційного коду застосовується малюнок капілярів (кровоносних судин) на сітківці (дні) ока; у другому – візерунок райдужної оболонки ока (рис. 5).

Ідентифікація за допомогою сітківки ока. Розглянемо спосіб ідентифікації за візерунком кровоносних судин, розташованих на поверхні

очного дна (сітківці). Сітківка розташована глибоко всередині ока, але це не зупиняє сучасні технології. Більше того, саме завдяки цій властивості, сітківка – одна з найбільш стабільних фізіологічних ознак організму.

Рис. 5. Райдужна оболонка ока

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. Для цих цілей використовується лазерний промінь м'якого випромінювання. Вени і артерії, що постачають кров'ю очі, добре видно при підсвічуванні очного дна зовнішнім джерелом світла. Ще в 1935 році Саймон і Голдштейн довели унікальність дерева кровоносних судин очного дна для кожного конкретного індивідуума [2]. Сканери для сітківки ока набули значного поширення в надсекретних системах контролю доступу, оскільки у них один з найнижчих відсотків відмови доступу зареєстрованих користувачів. Крім того, у системах передбачений захист від муляжу. У даний час широкому поширенню цього методу перешкоджає ряд причин: висока вартість зчитувача; невисока пропускна здатність; психологічний фактор. Невисока пропускна здатність пов'язана з тим, що користувач повинен протягом декількох секунд дивитися в окуляр на зелену крапку. І тим не менше, ці системи удосконалюються і знаходять своє застосування. У США, наприклад, розроблено нову систему перевірки пасажирів, яка заснована на скануванні сітківки ока. Фахівці стверджують, що тепер для перевірки не треба діставати з кишені гаманець з документами, що достатньо лише пройти перед камерою. Дослідження сітківки ґрунтуються на аналізі більш як 500 характеристик. Після сканування код буде зберігатися в базі даних разом з іншою інформацією про пасажира, і в подальшому ідентифікація особи займатиме лише кілька секунд. Використання подібної системи буде абсолютно добровільною процедурою для пасажирів. Англійська Національна фізична лабораторія (National Physical Laboratory, NPL), за замовленням організації Communications Electronics Security Group, що спеціалізується на електронних засобах захисту систем зв'язку, провела дослідження різних біометричних технологій ідентифікації користувачів. В ході випробувань система розпізнавання користувачів за сітківкою ока не дозволила допуск жодному з більш ніж 2,7 млн. «сторонніх», а серед тих, хто мав права доступу, лише 1,8% були помилково відкинуті системою (проводилися три спроби доступу). Як повідомляється, це був наднизький коефіцієнт помилкових рішень серед перевіряючих систем біометричної ідентифікації. А найбільший відсоток помилок був у системи розпізнавання обличчя - в різних серіях випробувань вона відкинула від 10 до 25 % законних користувачів.

Ідентифікація на основі параметрів райдужної оболонки ока. Унікальним для кожної особистості статичним ідентифікатором також є райдужна оболонка ока. Унікальність малюнка райдужної оболонки обумовлена генотипом особистості, і суттєві відмінності райдужної оболонки спостерігаються навіть у близнюків. Лікарі використовують малюнок і колір райдужної оболонки для діагностики захворювань та виявлення генетичної схильності до деяких захворювань. Виявлено, що при ряді захворювань на райдужній оболонці з'являються характерні пігментні плями і зміни кольору. Для ослаблення впливу стану здоров'я на результати ідентифікації людини в технічних системах розпізнавання використовуються тільки чорно-білі зображення високої роздільної здатності [4]. Ідея розпізнавання на основі параметрів райдужної оболонки ока з'явилася ще в 1950-х роках [5]. Джон Даугман, професор Кембриджського університету, винайшов технологію, до складу якої входила система розпізнавання за райдужною оболонкою, що використовується зараз в Nationwide ATM. У той час вчені довели, що не існує двох людей з однаковою райдужною оболонкою ока (більше того, навіть у однієї людини райдужні оболонки очей відрізняються), але програмного забезпечення, здатного виконувати пошук і встановлювати відповідність зразків відсканованого зображення, тоді ще не було. У 1991 році Даугман почав роботу над алгоритмом розпізнавання параметрів райдужної оболонки ока і в 1994 році отримав патент на цю технологію. З цього моменту її ліцензували вже 22 компанії, в тому числі Sensar, British Telecom і японська OKI. Отримане при скануванні райдужної оболонки ока зображення зазвичай виявляється більш інформативним, ніж оцифроване у випадку сканування відбитків пальців. Унікальність малюнка райдужної оболонки ока дозволяє випускати фірмам цілий клас досить надійних систем для біометричної ідентифікації особи. Для зчитування візерунка райдужної оболонки ока застосовується дистанційний спосіб зняття біометричної характеристики. Зараз використовуються *два основні підходи розпізнавання райдужної оболонки ока,* що відрізняються способами представлення образів. У першому підході райдужна оболонка ока виділяється з зображення очей, у другому - образом є матриця штрих-кодів, відповідна радужці. У першому підході є два своїх способи подання: у вигляді кілець, що відносяться до області райдужної оболонки; у вигляді прямокутника, отриманого шляхом перетворення декартової системи координат в полярну. Спочатку визначається центр зіниці і два радіуси щодо нього – радіус зіниці і радіус зовнішнього краю райдужної оболонки (межі визначаються пороговою обробкою). Межі зіниці та

райдужної оболонки не є при цьому круглими. Вони стають такими після додаткового оброблення. Після чого виконується збільшення чіткості образу. Другий спосіб можна подати у вигляді такого алгоритму: визначення місця розташування, центру і контурів зіниці; визначення радіусів зіниці і зовнішнього краю райдужної оболонки; формування полярної системи координат; перетворення кожного пікселя з декартової системи в полярну. На останньому етапі може знадобитися інтерполяція зображення, тому що цілочисельні декартові координати не завжди відповідають цілочисельним полярним. У результаті по осі X відкладені кути полярної системи координат, а по осі Y – значення радіуса (радіус зовнішнього кола радужки мінус радіус внутрішнього). Другий підхід, хоч і вимагає великих обчислень на етапі реєстрації, але зручніший тому, що поворот зображення, перетвореного з декартової системи координат в полярну, замінюється циклічним зсувом. Другий підхід розпізнавання райдужної оболонки ока (одержання матриці штрих-кодів) можна подати наступним чином. Зображення ока виділяється з зображення обличчя, потім на райдужну оболонку накладається спеціальна маска штрих-кодів. У результаті виходить матриця, отримана шляхом логічного множення маски на райдужну оболонку. Образ-еталон виходить розміром 512 байт. Системи цього класу, використовуючи звичайні відеокамери, захоплюють відео зображення очей на відстані до одного метра від відеокамери, здійснюють автоматичне виділення зіниці та райдужної оболонки. Пропускна здатність таких систем дуже висока. Ймовірність же помилкових спрацьовувань невелика. Крім цього, передбачений захист від муляжу. Вони сприймають лише око живої людини. Ще одна перевага цього методу ідентифікації – висока стійкість. На працездатність системи не впливають окуляри, контактні лінзи та сонячні відблиски. Перевага сканерів для райдужної оболонки полягає в тому, що вони не вимагають, щоб користувач зосередився на цілі, тому що зразок плям на райдужній оболонці знаходиться на поверхні ока. Навіть у людей з ослабленим зором, але з неушкодженою райдужною оболонкою, все одно можуть скануватися і кодуватися ідентифікуючі параметри. Навіть якщо є катаракта (ушкодження кришталика ока, яке знаходиться позаду райдужної оболонки), то і вона ніяк не впливає на процес сканування райдужної оболонки. Однак погане фокусування камери, сонячний відблиск та інші труднощі при розпізнаванні приводять до помилок в 1 % випадків. Перспективи поширення цього способу біометричної ідентифікації для організації доступу в комп'ютерних системах дуже великі. Тим більше, що зараз вже існують мультимедійні монітори з вбудованими в корпус відеокамерами. Тому на такий комп'ютер досить встановити необхідне програмне забезпечення і система контролю доступу готова до роботи. Зрозуміло, що і її вартість при цьому буде не дуже високою.

Голосова ідентифікація особи людини. У сучасному світі все більше проявляється інтерес до мовних технологій, зокрема, до ідентифікації людини за голосом [6]. Це пояснюється, з одного боку, появою високопродуктивних обчислювальних систем на базі персональних комп'ютерів і апаратних засобів, що дозволяють виробляти введення сигналу в комп'ютер, а, з іншого боку, високою потребою систем автентифікації в різних галузях життєдіяльності людини. Метод ідентифікації людини за голосом існує з того часу, як людина навчилася говорити. Тому переваги і недоліки цього методу відомі всім. Не завжди з відповіді на питання «Хто там?» Ми можемо визначити, що за дверима стоїть знайома людина, і доводиться розвіювати свої сумніви, заглянувши у дверне вічко, так і технічна система ідентифікації може помилятися в силу зміни голосу окремої людини. Привабливість даного методу – зручність у застосуванні. Метод перевірки голосу має дві позитивні відмінності від інших біометричних методів: по-перше, це ідеальний спосіб для телекомунікаційних програм; по-друге, більшість сучасних комп'ютерів вже мають необхідне апаратне забезпечення. Основна проблема, пов'язана з цим біометричним підходом – точність ідентифікації. Однак це не є серйозною проблемою з того моменту, як пристрої ідентифікації людини за голосом розрізняють характеристики людської мови. Голос формується з комбінації фізіологічних і поведінкових чинників. В даний час ідентифікація за голосом використовується для керування доступом до приміщення середнього ступеня безпеки, наприклад, лабораторії та комп'ютерних класів. Ідентифікація за голосом зручний, але в той же час не такий надійний, як інші біометричні методи. Наприклад, людина з застудою або ларингітом може відчувати труднощі при використанні даних систем. Існує також можливість відтворення звукозапису з магнітофона. Технологія розпізнавання голосу – ймовірно, найбільш практичне рішення для більшості мережевих додатків, у всякому разі, на даний момент. Системи розпізнавання голосу аналізують характеристики цифрованої мови, в тому числі її тон, висоту і ритм. Незважаючи на те, що залишаються технічні питання, зокрема, на зниження надійності розпізнавання за наявності шумів, це досить економічне рішення, так як мікрофони і звукові карти вже давно отримали прописку в мережі. Як відомо, джерелом мовного сигналу служить мовоутворюючий тракт, який збуджує звукові хвилі в пружному повітряному середовищі. Сформований мовний сигнал і передається у просторі у вигляді звукових хвиль. Приймач сигналу – це давач звукових коливань. Зазвичай для цих цілей використовують мікрофон - пристрій для перетворення звукових коливань в електричні. Існує велика кількість типів мікрофонів (вугільні, електродинамічні, електростатичні, п'єзоелектричні та ін.). Але в мікрофонах будь-якого типу чутливим елементом є пружна мембрана, за допомогою якої передається коливальний процес під впливом звукових хвиль. Мембрана пов'язана з

елементом, який перетворює коливання мембрани в електричний сигнал. З виходу мікрофона сигнал подається на вхід звукової карти персонального комп'ютера. Під час запису звукова карта є аналого-цифровим перетворювачем з широкими можливостями настроювання параметрів оцифрування. Основними параметрами є частота дискретизації та розрядність кодування. Ці параметри визначають якість і розмір вибірки, що отримується в результаті запису. Причому розмір запису і її якість прямо пропорційні, тобто чим вище якість запису, тим більше її розмір. Щоб забезпечити компроміс між якістю і розміром, скористаємося знаннями про властивості людського голосу при виборі параметрів аналого-цифрового перетворення. На цей момент у нас і за кордоном реалізовані системи автоматичної ідентифікації за голосом, більшість з яких будуються за єдиною концептуальною схемою: здійснюється реєстрація користувача та обчислюється шаблон; вибираються ділянки мовного потоку для подальшого аналізу; здійснюється первинне оброблення сигналу; обчислюються первинні параметри; будується «відбиток» (шаблон) голосу; проводиться порівняння «відбитків» голосів і формується рішення щодо ідентичності голосів або «близькості» голосу до групи голосів.

Ідентифікація людини за допомогою геометрії обличчя. Система розпізнавання облич – найбільш давній і поширений спосіб ідентифікації [6]. Саме такій процедурі піддається кожен, хто перетинає кордон. При цьому прикордонник звіряє фото на паспорті з особою власника паспорта і приймає рішення, його це паспорт чи ні. Приблизно таку ж процедуру виконує комп'ютер, але з тією лише різницею, що фото вже знаходиться в його пам'яті. Привабливість даного методу заснована на тому, що він найбільш близький до того, як ми ідентифікуємо одне одного. Розвиток даного напряму обумовлено швидким зростанням мультимедійних відеотехнологій, завдяки яким можна побачити все більше відеокамер, встановлених вдома і на робочих місцях. Істотний імпульс цей напрямок одержав через значне поширення технології відеоконференцій Internet / Intranet. Орієнтація на стандартні відеокамери персональних комп'ютерів робить цей клас біометричних систем порівняно дешевим. Тим не менш, ідентифікація людини за геометрією обличчя являє собою досить складне (з математичної точки зору) завдання. Хоча обличчя людини - унікальний параметр, але досить динамічний; людина може посміхатися, відпускати бороду і вуса, надягати окуляри – все це додає труднощів у процедуру ідентифікації і вимагає досить потужної й дорогої апаратури, що відповідно впливає на ступінь поширення даного методу.

Алгоритм функціонування системи розпізнавання досить простий [5]. Зображення особи зчитується звичайною відеокамерою та аналізується. Програмне забезпечення порівнює введений портрет з тим, що зберігається в пам'яті в якості еталона. Деякі системи додатково архівують зображення, які вводяться для можливого в майбутньому вирішення конфліктних ситуацій. Вельми важливо також те, що біометричні системи цього класу потенційно здатні виконувати безперервну ідентифікацію (автентифікацію) користувача комп'ютера протягом всього сеансу його роботи. Більшість алгоритмів дозволяє компенсувати наявність окулярів, капелюха і бороди у піддослідного. Було б наївно припускати, що за допомогою подібних систем можна отримати дуже точний результат. Незважаючи на це, в деяких країнах вони досить успішно використовуються для верифікації касирів і користувачів депозитних сейфів. Основними проблемами, з якими стикаються розробники даного класу біометричних систем, є зміна освітленості, варіації положення голови користувача, виділення інформативної частини портрета (гасіння фону) [2]. З цими проблемами вдається впоратися, автоматично виділяючи на обличчі особливі точки і потім вимірюючи відстані між ними. На обличчі виділяють контури очей, брів, носа, підборіддя. Відстані між характерними точками цих контурів утворюють вельми компактний еталон конкретного обличчя, що легко піддається масштабуванню. Завдання оконтурювання характерних деталей обличчя легко може бути вирішене для плоских двомірних зображень з фронтальним підсвічуванням, але такі біометричні системи можна обдурити плоскими зображеннями обличчя оригіналу.

Ідентифікація за «тепловим портретом» обличчя. Більш надійним різновидом систем розпізнавання облич є ідентифікація за «тепловим портретом» особи або тіла людини в інфрачервоному діапазоні. Цей метод, на відміну від звичайного, оптичного, не залежить від змін обличчя людини (наприклад, появи бороди), тому що теплова картина обличчя змінюється дуже рідко. Дана технологія заснована на тому, що термограми обличчя людини (теплова картинка, створена випромінюванням тепла кровоносними судинами обличчя) унікальна для кожної людини і, отже, може бути використана в якості біокоду для систем контролю допуску. Дана термограма є більш стабільним кодом, ніж геометрія обличчя, оскільки не залежить від часу і змін зовнішності людини. У процесі термографічної ідентифікації обличчя індивідуальний малюнок розподілу теплових областей на обличчі людини вводиться в комп'ютер за допомогою інфрачервоної камери та плати захоплення зображення. Монохромне зображення, що надходить від інфрачервоної відеокамери, вводиться в комп'ютер за допомогою спеціального кабелю. В цей же час до зображення додається спеціально створена переглядова таблиця (look up table). Зображення піддається обробці спеціальною утилітою, розробленою на C++. У цей час і відбувається ідентифікація за індивідуальним малюнком теплових областей на обличчі. Проблеми ідентифікації людини за допомогою обличчя істотно спрощуються при переході спостережень у дальній інфрачервоний діапазон світлових хвиль. Запропоновано здійснювати термографію ідентифікуючого обличчя, яка виявляє унікальність

розподілу артерій на обличчі, що забезпечують шкіру теплою кров'ю. Проблема підсвічування для цього класу біометричних пристроїв не існує, так як вони сприймають лише температурні перепади обличчя і можуть працювати в повній темноті. На результати ідентифікації не впливають перегрів особи, його переохолодження, природне старіння обличчя, пластичні операції, тому що вони не змінюють внутрішнє розташування судин. Методом лицьової термографії можливо розрізнити однояйцевих близнят, кровоносні судини на їхніх обличчях мають досить істотні відмінності. Дистанційне зчитування з будь-якої відстані незалежно від освітленості забезпечує високу пропускну здатність. Метод розрахований на використання спеціалізованої відеокамери далекого інфрачервоного діапазону, що й визначає його високу вартість [4].

Ідентифікація людини за допомогою кисті руки. Практично все про людину можливо прочитати за його рукою. Проте, в біометриці з метою ідентифікації (або автентифікації) використовується зараз тільки проста геометрія руки – розміри і форма, а також деякі інформаційні знаки на тильній стороні руки (образи на згинах між фалангами пальців, візерунки розташування кровоносних судин). Взагалі з руки можна зібрати до 90 інформаційних знаків, частина з яких не використовується в біометриці [2-4]. Наприклад, унікальний візерунок на долоні. Існує два підходи до використання геометрії руки: перший (існує з 1976 року) заснований на геометричних характеристиках кисті; другий (сучасний) використовує крім геометричних ще й образові характеристики руки (образи на згинах між фалангами пальців і візерунки кровоносних судин).

Метод розпізнавання геометрії кисті руки заснований на аналізі тривимірного зображення кисті руки і отримав розвиток у зв'язку з тим, що математична модель ідентифікації за даним параметром вимагає досить малого обсягу інформації – всього 9 байт, що дозволяє зберігати великий обсяг записів, і, отже, швидко здійснювати пошук. Однак форма кисті руки також є параметром, який досить сильно зазнає змін у часі, а крім того, вимагає сканерів великого розміру, що веде до подорожчання системи. У даний час, метод ідентифікації користувачів за геометрією руки використовується багатьма організаціями і компаніями. У деяких випадках працювати з відбитком руки набагато зручніше, ніж з відбитком пальця. Перший комерційний біометричний пристрій, що визначає геометрію пальців, з'явився більше 400 років тому. Перші моделі зчитувачів, у яких в якості ідентифікатора використовувалося об'ємне зображення долоні, з'явилися в 1972 році в США. Долоня підсвічувалась безліччю лампочок, розташованих у вигляді матриці, і аналізувалася тінь – двовимірне зображення кисті руки. У сучасних моделях зчитувачів враховується і товщина долоні. Більш складними є системи, які додатково вимірюють профіль руки (обсяг пальців, обсяг кисті, нерівності долоні, розташування складок шкіри на згинах). Дані про тривимірну геометрію руки отримують шляхом використання однієї телевізійної камери та інфрачервоної підсвітки руки під різними кутами. Послідовне включення декількох підсвічуючих світлодіодів дають тіньові варіанти проекцій тривимірної геометрії кисті руки, що містять інформацію про її об'єм. Пристрої, в яких реалізовано подібне технічне рішення, не будуть малогабаритними, тому що потрібно виносити джерела підсвічування на відстань 10-15 см. Широкому поширенню таких систем перешкоджає кілька чинників [4]: висока ціна самого зчитувача; невисока пропускна здатність – долоню потрібно правильно розташувати у зчитувальному пристрої; відсутність технологій захисту від фальсифікації; замість кисті руки в зчитувач можна засунути її муляж. Також у цієї системи біометричної ідентифікації є і свої переваги [3]. На відміну від дактилоскопічних зчитувачів, вони не пред'являють підвищених вимог до вологості, температури, кольору, забрудненості та інших параметрів. Системи такого типу доцільно застосовувати в студентських містечках, на складах і т. п., тобто там, де неможливо забезпечити чистоту рук і відносно невисокі вимоги до безпеки.

Ідентифікація за зображенням кровоносних судин на зворотному боці долоні. Ще один варіант застосування кисті руки в якості ідентифікатора – це використання малюнка кровоносних судин на зворотному боці долоні. Такий візерунок унікальний, його можна зчитувати на відстані і складно відтворити штучно [5]. Ця новітня технологія розпізнавання лежить в основі багатьох пристроїв ідентифікації. Особливість приладів полягає в тому, що вони сканують не поверхню пальця, а склад внутрішніх органів людини (структуру мережі кровоносних судин руки) за допомогою спеціального інфрачервоного давача. У цьому випадку деформація поверхні, сухість, вологість або забрудненість рук ніяк не впливають на результати розпізнавання. Після сканування система розпізнавання обробляє отримане зображення. Такі пристрої можуть працювати як самостійно, так і в мережі під управлінням сервера. Крім розглянутих пристроїв, існують такі, які використовують для ідентифікації людини малюнок вен, розташованих на тильній стороні кисті руки, стиснутої в кулак. Спостереження малюнка вен здійснюється телевізійною камерою за інфрачервоного підсвічування, після чого обчислюється шаблон.

Ідентифікація людини за її підписом. Підпис – один з класичних способів ідентифікації, що застосовується вже кілька століть в юридичній практиці, банківській справі та торгівлі. Існує два незалежних способи ідентифікації за підписом [6]: ідентифікація за зображенням підпису на документі; ідентифікація за динамікою підпису, що вводиться в комп'ютер. У першому способі потрібно порівняти два зображення. З цим краще впорається людина. У другому способі є дані про коливання пера при відтворенні підпису в тривимірному просторі (X, Y –

координати і Z – тиск на планшет). З цим може впоратися тільки комп'ютер.

Додаткові біометричні параметри. Раніше були розглянуті основні біометричні параметри, які в цей час широко використовуються для аутентифікації людини. Ріст ринку біометричних систем стимулює розвиток нових технологій ідентифікації, у кожної з яких є свої достоїнства й недоліки та своя область застосування. До таких біометричних параметрів відносяться [6]:

1. ДНК – часто називають майже самим ідеальним параметром, тому що код ДНК є ідентифікаційною інформацією в цифровій формі, що є в будь-якій клітині людини. Недолік цього параметра в тому, що із практичної точки зору порівняння людей на основі двох зразків ДНК – повільний, дорогий й складний процес.

2. Сітківка ока – ідентифікація людини за сітківкою ока відбувається шляхом порівняння зображень кровоносних судин очного дна. У цей час сенсори, використовувані для ідентифікації за сітківкою, усе ще занадто дорогі в порівнянні із сенсорами для зчитування інших біометричних параметрів. Більшою перевагою ідентифікації за сітківкою є сталість параметра: на сітківку не впливає нічого, крім сильних травм, її не можливо підробити.

3. Термограми – це зображення, отримані в різних областях інфрачервоного спектра, іноді з додатковим використанням видимого спектра. Термограми в біометрії – це зображення частин тіла в короткохвильовому, середньому й довгохвильовому діапазонах інфрачервоного спектра. Велика перевага термограм перед звичайними зображеннями - це їхня незалежність від зміни освітлення. На термограми також не впливає зміна зовнішності, принаймні, вони не чутливі до деяких видів маскування. Одним з недоліків цього методу аутентифікації є висока вартість сенсорів.

4. Хода – ставиться до поведінкових біометричних параметрів. Достоїнство цього методу – можливість розпізнавання людей на відстані, використовуючи відеозапис. Недолік – процедура розпізнавання дуже сильно залежить від умов, у яких перебуває об'єкт.

5. Клавіатурний почерк – ідентифікація за клавіатурним почерком - це ідентифікація людини за власним стилем друкування. Система ідентифікації за клавіатурним почерком заснована на фіксованому паролі, але приблизно можуть бути й незалежними від тексту, що набирається, як системи розпізнавання голосу.

6. Відбиття шкіри – один з нових біометричних параметрів, що з'явилися завдяки розробці сенсорів. Перевагою даної технології є те, що для зразка маленького розміру потрібно й маленький чіп – за розміром й обсягом пам'яті й продуктивності. Також потрібно відзначити відсутність проблем з реєстрацією, які характерні для методу ідентифікації за відбитками пальців; 7 рухів губ – ставиться до поведінкових біометричних параметрів, він може використовуватися як візуальне доповнення до системи розпізнавання мовця; технологія аутентифікації за рухом губ такий же різновид, що й методика розпізнавання мовця: з фіксованим текстом, залежна від тексту й незалежна від тексту. Одне з найбільших достоїнств цього методу – можливість легко поєднати його з ідентифікацією мовця й розпізнаванням за геометрією особи. У такий спосіб можна створити дуже точну систему, яку буде складно обдурити.

Висновки. Отже, у цій статті досліджено біометричні характеристики людини, за допомогою яких здійснюється їх ідентифікація, а саме: відбитки пальців; форма і геометрія обличчя; форма і будова черепа; сітківка ока; райдужна оболонка ока; геометрія долоні, кисті руки або пальця; термографія особи, термографія руки; малюнок вен на долоні або пальці руки; ДНК; запах тіла; форма вуха; динаміка підпису; динаміка клавіатурного набору; голос; рух губ; хода; особливості накреслення рукописного тексту. Наведено основні характеристики сучасних біометричних технологій, а також класифікацію біометричних методів ідентифікації. Крім того, проведено аналітичне дослідження сучасних методів біометричної аутентифікації, виділено їх переваги та недоліки. Ця робота буде корисною для вибору певних біометричних методів і засобів з метою організації систем захисту інформації чи їх удосконалення.

Література

[1] Jain A., Hong L. & Pankanti S. (2000). Biometric Identification. Communications of the ACM, 43(2), p. 91-98. DOI 10.1145/328236.328110.

[2] Jain Anil K. & Ross, Arun (2008). Introduction to Biometrics. In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22.

[3] Горлицин И. Контроль и управление доступом - просто и надежно КТЦ «Охранные системы», 2002.

[4] Гинце А. Новые технологии в СКУД // Системы безопасности, 2005.

[5] Крахмалев А. К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ «Охрана» ГУВО МВД России. 2003.

[6] Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. 2002.

[7] NISTIR 6529-A, ANSI INCITS 377-2009, ANSI INCITS 381, ANSI INCITS 378, ANSI INCITS 379, ANSI INCITS 396, ANSI INCITS 385, ANSI INCITS 442-2010, ANSI INCITS 429, ANSI/NIST-ITL 1-2007.

[8] ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца»

[9] ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальцев»

[10] ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация

биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица».

[11] ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза».

УДК 004.056.52 (045)

Швец В.А., Фесенко А.А. Основные биометрические характеристики, современные системы и технологии биометрической аутентификации

Аннотация. *В данной статье исследованы биометрические характеристики человека, с помощью которых осуществляется их идентификация. Приведены основные характеристики современных биометрических технологий, а также классификацию биометрических методов идентификации. Кроме того, проведено аналитическое исследование современных методов биометрической аутентификации, выделены их преимущества и недостатки.*

Ключевые слова: *защита информации, биометрия, биометрическая характеристика, биометрическая технология, идентификация, аутентификация, характеристики биометрических технологий.*

Shvets V.A., Fesenko A.O. Basic biometric characteristics, modern systems & technologies of biometric authentication

Abstract. *This article explores the biometric characteristics of a person, by means of which their identification. The basic characteristics of modern biometric technologies, as well as classification of biometric identification methods were presented. Also an analytical study of modern methods of biometric authentication was carried out, highlighted their advantages and disadvantages.*

Key words: *information security, biometrics, biometric characteristic, biometric technology, identification, authentication, characteristics of biometric technology.*

Отримано *3 червня 2013 року*, затверджено редколегією *18 червня 2013 року*