УДК 004.93

І. В. Калініна, О. І. Лісовиченко

КОМБІНОВАНІ МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ В ЗАДАЧАХ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Анотація: У роботі запропоновано комбіновані методи біометричної ідентифікації для ефективності біометричних систем, які дозволять підвищити захист від несанкціонованого доступу.

Ключові слова: несанкціонований доступ; захист інформації; біометричні системи захисту; розпізнавання за відбитком пальця; розпізнаванняза зображенням; розпізнавання за райдужною оболонкою ока; комбіновані методи біометричної ідентифікації.

Вступ

У повсякденному житті з давніх часів використовувались біометричні характеристики для забезпечення безпеки та контролю.

Незважаючи на широкі технологічні можливості забезпечення захисту, на сьогоднішній день, кількість злочинів та шахрайства зростає з кожною хвилиною.

Однією з поширених технологій захисту є біометричні засоби захисту захисту інформації (рис. 1). Ці системи є зручними, оскільки не потребують зберігання у пам’яті складних паролів чи носіння з собою спеціальних ідентифікаторів (ключів, карток, і т. ін.), а достатньо буде тільки сказати кодове слово, прикласти палець чи кисть руки, або підставити лице для сканування, щоб отримати доступ.

Слід зазначити, що теоретичному різноманітті можливих біометричних методів багато, що застосовуються на практиці серед них небагато. Основні засоби три – розпізнавання за відбитком пальця, за зображенням особи (двовимірне або тривимірне) та за райдужною оболонкою ока.

Спробуємо розглянути в кожному засобі та виділити недоліки та переваги. Недоліки та переваги основних засобів представлено в таблиці [2].

Переваги біометричних систем: унікальні людські якості тим, що їх складно підробити, залишити фальшивий відбиток пальця за допомогою власного, або зробити райдужну оболонку свого ока схожою на чиюсь. 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.

 ISSN 1560-8956

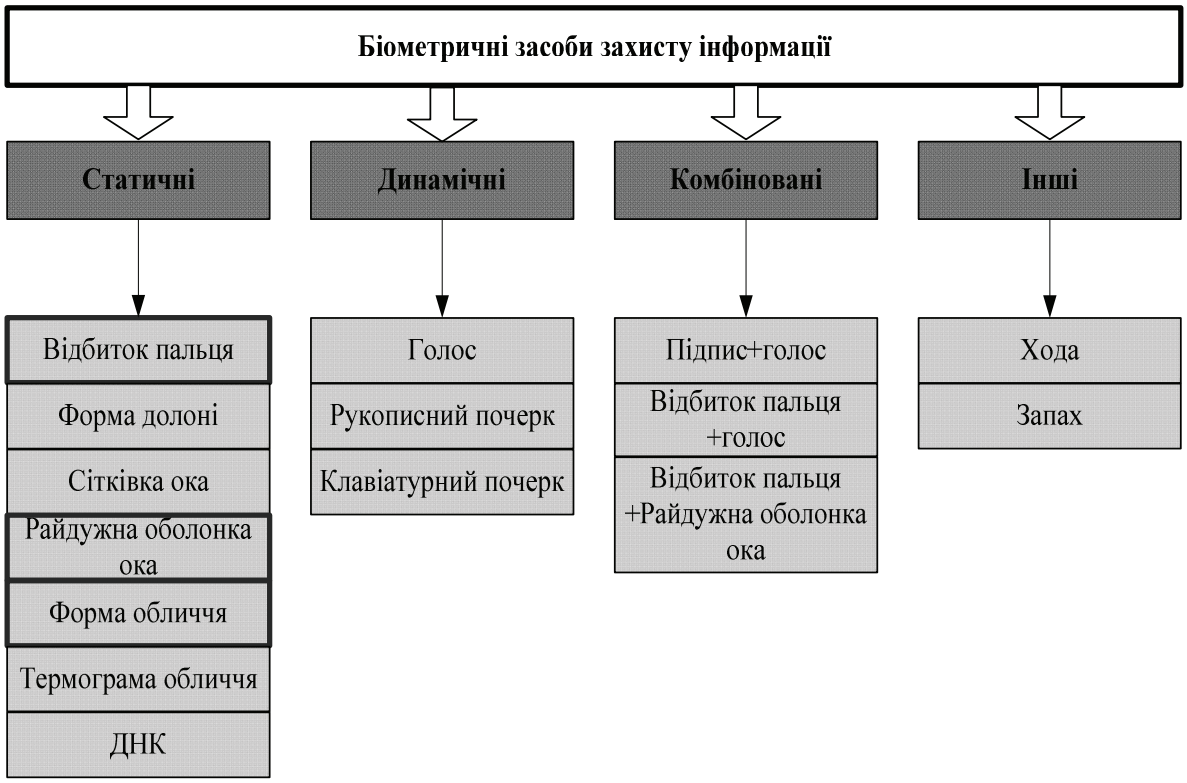

Рис. 1. Біометричні засоби захисту інформації

Таблиця.

Метод	Переваги методу	Недоліки методу
Відбиток пальця	• висока достовірність; • низька вартість обладнання; • достатньо проста процедура сканування відбитка.	• папілярний узор відбитка пальця дуже легко можна пошкодити дрібними подряпинами, порізами; • недостатня захищеність від підробки, викликана широким поширенням методу; • залежність від чистоти пальця; • для сухої шкіри якість розпізнавання нижче.
2D – розпізнавання особи	• не потрібне дороге обладнання; • при відповідному обладнанні можливість розпізнавання на значних відстанях від камери.	• низька статична достовірність; • пред'являються вимоги до освітлення; • неприйнятність будь-яких зовнішніх перешкод; • не враховують можливі зміни міміки обличчя, вираз повинен бути нейтральним.

Закінчення таблиці

3D – розпізнавання особи	• висока достовірність розпізнавання – більше інформації, чим має звичайний знімок; • стійкість розпізнавання до відхилення ракурсу особи від фронтального; • стійкість розпізнавання до неоднорідності освітлення; • відсутність необхідності контактувати з пристроєм; • низька чутливість до зовнішніх факторів.	• має обмежену сферу застосування із-за поганих статичних показників; • зміна міміки обличчя і перешкоди на обличчі погіршують статичну надійність методу.
Райдужна оболонка ока	• захоплення зображення проводиться на відстані від декількох см до декількох метрів, фізичний контакт людини з пристроєм не відбувається; • райдужна оболонка захищена від пошкоджень, тому не змінюється в часі.	• погана якість зображення райдужної оболонки – розмиття, викликане поганим фокусуванням, часом та іншими факторами; • низька доступність готових технічних рішень.

Доцільно зауважити, що умови при кожному скануванні різні, а частини тіла, які підлягають скануванню, та поведінкові рефлекси особи також не зовсім постійні, тому можна говорити про неточне збігання зі зразком, а лише про ступінь подібності з еталоном. Тому біометричні системи характеризуються параметрами «можливість невизнання свого» (тобто вірогідність невпізнання зареєстрованої особи), та «можливістю визнання своїм чужого» (тобто є вірогідність, що проникне несанкціонований користувач).

Постановка задачі

Розглянути та проаналізувати комбіновані методи ідентифікації, необхідно знайти шляхи підвищення ефективності засобів біометричних систем захисту від несанкціонованого доступу. Розглянути розвиток технологій, щодо удосконалення вище вказаних засобів.

Аналіз методів

Основними характеристиками ефективності біометричних систем є точність розпізнавання, стійкість до зміни навколишнього середовища,

 ISSN 1560-8956

криптостійкість – захист від підробки та надійність роботи безпосередньо системи. Спробуємо дати кількісну характеристику засобів за вищенаведеним критеріям за 10-ти бальною шкалою. В табл. 2 наведені якісні характеристики основних біометричних засобів [3].

Таблиця 2

Критерій / Засіб	Точність	Стійкість до зміни навколишнього середовища	Стійкість до підробки	Вартість
Відбиток пальця	8	10	6	10
Зображення особи (2D)	4	6	4	10
Зображення особи (3D)	6	8	9	5
Райдужна оболонка ока	10	9	10	7

Розглянемо детальніше кожний із критеріїв.

Точність біометричної системи характеризується:

- FAR (False Acceptance Rate) – відсоток помилкових допусків, коли доступ до системи помилково надано неавторизованому користувачеві.
- FRR (False Rejection Rate) – відсоток помилкових відмов, коли система відмовила в доступі авторизованому користувачеві;

Значення точності в режимі операційного тестування для основних біометричних методів після проведення певних тестів наведені в табл. 3 [3].

Таблиця 3

Засіб	FAR	FRR
Відбиток пальця	0,01%	10%
Зображення особи (2D)	0,0047%	0,103%
Зображення особи (3D)	0,0047%	0,103%
Райдужна оболонка ока	0,01%	0,05%

За показником FAR найбільш надійним буде засіб зображення особи (2D і 3D), тому що ймовірність хибного співпадання біометричних характеристик двох осіб найменша в порівняні з останніми двома мето-

дами. За показником FRR найбільш надійним буде метод по райдужній оболонці ока, тому що ймовірність відмови в доступі особи, що має право доступу найменша, а найбільш гіршим по цьому показнику являється метод за відбитком пальця.

Стійкість до зміни навколишнього середовища є важливою характеристикою біометричних методів. Експлуатаційні якості різних методів у значній мірі залежать від навколишніх умов і можуть втрачати стабільність при їх зміні. Наприклад, сканери відбитків пальців, коли достатньо швидко забруднюються, і якість роботи значно падає.

Для розпізнавання особи двовимірними методами та за райдужною оболонкою дуже велике значення має розподіл зовнішньої освітленості. Найкращою дана характеристика виявилася у розпізнаванні відбитку пальця [4].

Стійкість до підробки є головним критерієм запобігання несанкціонованому доступу. Фотографічне зображення райдужної оболонки ока або двовимірного зображенню особи, запропоноване системі, може призвести до помилкового розпізнавання. Для одержання несанкціонованого доступу за відбитком пальця часто буває досить просто подихати на залишений на сканері відбиток пальця попереднього користувача, що приведе до аутентифікації. Найбільш стійкою до підробки на даний момент є технологія розпізнавання за тривимірним зображенням особи. Щоб увести в оману таку систему, необхідно було б виготовити точну маску обличчя особи, яка повторювала всі деталі даної біометричної характеристики. При цьому система тривимірного розпізнавання, за умов функціонування в реальному часі, може містити у собі перевірку на природні мімічні мікрорухи обличчя особи, що імітувати за допомогою маски дуже складно [4].

Вартість на обладнання варіюється від 4000 до 50000 грн. взалежності від сфери використання. Наприклад, мульти біометричний термінал D-Station здатний з високою швидкістю розпізнавати відбитки пальців і риси обличчя людини, яка проходить перевірку. Ціна такого терміналу коштує 50 000 грн.

Співвідношення ціна/якість систем біометричної ідентифікації можна оцінити за графіком на рис. 2.

 ISSN 1560-8956

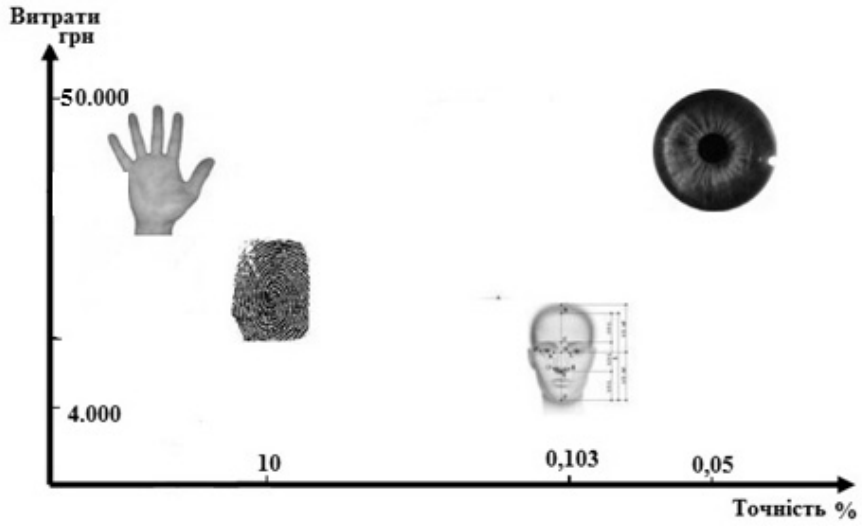

Рис. 2. Співвідношення ціна/якість систем
біометричної ідентифікації

Комбінування біометричних методів

Комбінована біометрична система аутентифікації застосовує різні доповнення для використання декількох методів біометричних характеристик, що дозволяє з'єднати типи біометричних технологій в системах аутентифікації в одній (рис. 3). Це дозволяє задовольнити найсуворіші вимоги до ефективності системи аутентифікації.

Одним з найпоширеніших комбінованих рішень є розпізнавання за відбитками декількох пальців. Так, в програмі US-visit в даний час застосовується розпізнавання за двома пальцями, і сьогодні вже обговорюється перехід до розпізнавання за трьома або навіть п'ятьма пальцями. Точність, що досягається в разі п'яти пальців, поки недосяжна для комбінацій інших методів. Незважаючи на це, практичне використання таких систем обмежене за рядом технічних можливостей.

Рис. 3. Комбінація засобів за видбитком пальця і
райдужною оболонкою ока

Методи одержання 3D-зображення особи, як правило, дозволяють одночасно одержувати й 2D-зображення, тому природним є одночасне використання обох джерел інформації. Наприклад, зручність звичайних двовимірних фотографій для візуального порівняння робить раціональним збереження тривимірного знімку разом із двовимірним. Комбіновані системи збільшують точність розпізнавання. В таблиці 4 наведені різні варіанти комбінацій засобів біометричної ідентифікації.

Таблиця 4.

Методи	Відбиток пальця	Зображення особи(2D)	Зображення особи (3D)	Райдужна оболонка ока
Відбиток пальця		–	+	+
Зображення особи (2D)	–		+	–
Зображення особи (3D)	+	+		+
Райдужна оболонка ока	+	+	+	

Область використання комбінованих засобів біометричної ідентифікації

Методи сканування райдужної оболонки і відбитку пальців почали застосовувати і в аеропортах для таких різноманітних функцій, як ідентифікація/верифікація працівників для проходження через зони обмеженого доступу, а також для ідентифікації пасажирів, які найбільш часто користуються послугами авіакомпанії для швидкого проходження паспортного контролю.

Ще однією областю використання комбінованих біометричних засобів є паспорта, перевірка громадян, що в'їжджають в країну. Наприклад, США розширюють застосування програми оцінки автоматизованих процедур біометричної перевірки від'їжджаючих «US-VISIT» щодо іноземних громадян.

Іноземці, які повертаються з США, повинні пройти реєстрацію в якості відїзджаючих в спеціальних реєстраційних кабінках. Як і при проходженні процедури реєстрації при в'їзді, при проходженні процедури перевірки буде проводитися контроль їх проїзних документів, електронне сканування двох відбитків вказівних пальців в реєстраційній кабінці і виготовлення цифрового фотографічного знімка, після цього в'їжджаючі отримають друковану квитанцію про

 ISSN 1560-8956

проходження реєстрації. Міністерство внутрішньої безпеки США повідомило, що сформована в рамках програми US-VISIT база відбитків пальців претендентів американських віз включає відомості про 70 млн. чоловік.

Україна також не стоїть осторонь від застосування біометричних даних при вирішенні певних завдань.

Постановою Кабінету Міністрів України від 9 листопада 2004 року № 1500 на виконання Указу Президента України від 30 квітня 2004 року № 500 «Про створення Єдиного державного реєстру фізичних осіб» (в даний момент зазначені Постанова Кабінету Міністрів України та Указу Президента України недійсні) було затверджено Концепцію створення Єдиного державного реєстру фізичних осіб, яка передбачала, в якості основи побудови інформаційного забезпечення цього Реєстру, використання даних біометричної ідентифікації та машинозчитуваної інформації.

Концепція створення Єдиного державного реєстру фізичних осіб дала визначення терміну «біометрична ідентифікація», як способу підтвердження особи, приналежності паспорта його власнику шляхом розпізнавання і зіставлення, зафіксованих носіями біометричної інформації біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, а також малюнка особи).

Серед інших сфер застосування можна назвати такі проекти, як верифікація при онлайн-покупках, онлайн-користування банківськими послугами, онлайн-голосування і онлайн-торгівля акціями [6]. Наприклад, компанія Brown Investments оголосила про випуск нового платіжного кіоску серії Pinnacle, однією з ключових функцій якого є ідентифікація користувача за відбитками пальців. Крім відбитків пальців, кіоск може впізнавати клієнтів і за іншими ідентифікаторами, приймати чеки, встановлювати їх справжність та навіть за невелику комісію випускати платіжну дебетову карту, рахунок якої буде дорівнює сумі чека [7].

Стандарти

BioAPI є стандартом BioAPI Consortium, розробленим спеціально для уніфікації програмних інтерфейсів програмного забезпечення розробників біометричних пристроїв.

AAMVA Fingerprint Minutiae Format / National Standard for the Driver License / Identification Card DL/ID-2000 – американський ста-

ндарт на формат представлення, зберігання та передачі відбитків пальців для водійських прав. Сумісний із специфікаціями BioAPI і стандартом CBEFF.

CBEFF (Common Biometric Exchange File Format) – єдиний формат подання біометричних даних, який пропонується для заміни біометричних форматів, використовуваних виробниками різних сегментів ринку біометричних систем, в своєму обладнанні і програмному забезпеченні. При створенні CBEFF були враховані всі можливі аспекти його застосування, в тому числі криптографія, багатофакторна біометрична ідентифікація та інтеграція з картковими системами ідентифікації.

CDSA / HRS (Human Recognition Services) – біометричний модуль в архітектурі Common Data Security Architecture, розробленої Intel Architecture Labs і схваленого консорціумом Open Group. CDSA визначає набір API, що представляють собою логічно пов'язане безліч функцій, що охоплюють такі компоненти захисту, як шифрування, цифрові сертифікати, різні способи аутентифікації користувачів, в список яких завдяки HRS додана і біометрія. CDSA / HRS сумісний зі специфікаціями BioAPI і стандартом CBEFF.

ANSI / NIST — ITL 1-2000 Fingerprint Standard Revision – американський стандарт, що визначає загальний формат подання та передачі даних за відбитками пальців, особі, натільним шрамам й тату для використання в правоохоронних органах США [8].

Висновок

Розглянуті та проаналізовані комбіновані методи біометричної ідентифікації дозволять підвищити захист від несанкціонованого доступу. Найбільш вдалі комбінації: відбиток пальця + райдужна оболонка ока; відбиток пальця + зображення особи (2D і 3D); зображення особи (2D) + зображення особи (3D). Крім того, існує комбінування за відбитками декількох пальців. Точність, що досягається в разі п'яти пальців, поки недосяжна для комбінацій інших методів, так як знайти людей з однаковими відбитками п'яти пальців неможливо.

Комбіновані біометричні системи в основному є більш надійними з точки зору можливості фальсифікації, тому що важче підробити цілий ряд біометричних характеристик, ніж фальсифікувати одну біометричну ознаку.

 ISSN 1560-8956

Список використаних джерел

1. Мельник Л. С. Засіб автентифікації за клавіатурним почерком на основі нейромережевої моделі. /Л. С. Мельник – Вінниця: ВНТУ, 2015 – 76 с.
2. Бугаєнко Х. А., Горбенко І. Д. Аналіз трьох біометричних методів автентифікації особи. / Х. А. Бугаєнко, І. Д. Горбенко: Прикладная радиоэлектроника, 2012, Том 11, № 2.
3. ВакуленкоА., Юхин А. Биометрические методы идентификации личности: обоснованный выбор. – http://www.bytemag.ru/articles/detail.php?ID=9077
4. Мелешко О. О., Лебединська І. О., Наконечна Г. В., Ткачук А. І. Захист інформації з використанням біометричних систем. – http://www.rusnauka.com/35_OINBG_2010/Informatica/76206.doc.htm
5. Системи контролю доступу. – http://www.npblog.com.ua/index.php/tehnika/sistemi-kontrolju-dostupu.html
6. House Control – http://house-control.org.ua/category/ biometricheskie_sistemy/1/order/price/
7. Д.В. Ландэ, В.Н. Фурашев. О цифровой идентификации личности.
8. Біометричні системи розпізнання людини. – http://itzo-book.at.ua/load/disciplina/lekcijni_zanjattja/tema_9_biometrichni_sistemi_rozpiznannja_ljudini/2-1-0-12.