УДК 004.056

Г.Є. Ляшенко, А.А. Астраханцев

Харківський національний університет радіоелектроніки, Харків

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

В даній статті розглянуті основні існуючі статичні та динамічні методи біометричної аутентифікації; виконаний багатокритеріальний аналіз за найбільш розповсюдженими показниками біометричних систем; визначені оптимальні методи, які забезпечують найменше значення частот помилкових спрацьовувань та відмов в обслуговуванні; проаналізована ефективність роботи мультибіометричних систем, які використовують для підвищення надійності систем автентифікації.

Ключові слова: *автентифікація*, *біометричне* розпіз*навання*, *мультибіометричні системи*.

Вступ

У сучасному світі дуже важливими є володіння інформаційними ресурсами та контроль доступу до них. Тому, як ніколи, є актуальною проблема інформаційної безпеки, яка повинна забезпечувати конфіденційність інформації, доступність інформації для користувачів, які мають права доступу до неї, захищеність інформації від несанкціонованих модифікацій та руйнування.

Для забезпечення захисту інформації та контролю управління доступу до її ресурсів можуть бути використані біометричні технології, які дозволяють однозначно визначити суб'єкт доступу та його повноваження по відношенню до конкретного ресурсу. На відміну від традиційних методів автентифікації (паролі, картки, різноманітні електронні ключі), біометричні ознаки людині дуже важко підробити та неможливо втратити, вкрасти або передати в користування іншій особі. Біометричні зразки «знімаються» з об'єкта датчиками і відсилаються процесору, який витягує відмінні риси, відкидаючи всі інші компоненти. Оброблений біометричний зразок зберігається в базі даних як «шаблон», або порівнюється з певним шаблоном для визначення відповідності. Сучасні системи біологічного розпізнавання є якісними та надійними засобами автентифікації особистості.

В останній час у системах авторизації користувачів у платіжних системах зростає роль стеганографічних додатків. В якості інформації, яка передається за допомогою мережевої стеганографії, має сенс використовувати хеш-функцію біометричних даних користувача. Це дозволить використовувати прихований підпис інформації, що передається, та авторизовувати джерело пакетів.

Метою цієї статті є дослідження найбільш поширених видів динамічних і статичних методів біометричної ідентифікації та верифікації, визначення основних критеріїв оптимальності біометричних систем автентифікації, виконання багатокритеріального аналізу біометричних показників, а також порівняльний аналіз мультимодальних методів біометричної автентифікації для визначення методів, які забезпечують найменше значення частот помилкових спрацьовувань та відмов в обслуговуванні**.**

Аналіз однофакторних методів біометричної автентифікації

Існуючі алгоритми і методи біометричного розпізнавання можна поділити на дві основні групи: статичні та динамічні [1–2]. Статичні методи біометричної автентифікації ґрунтуються на фізіологічній характеристиці людини, яка є унікальною, бо була дана людині від народження, і невід'ємною від неї. До таких методів належать дактилоскопія, васкулярна автентифікація, розпізнавання за райдужною оболонкою ока, сітківкою ока, геометрією руки, геометрією обличчя, термограмою. Динамічні методи біометричної автентифікації ґрунтуються на поведінковій характеристиці людини в процесі відтворення певної дії. До таких методів належать розпізнавання голосу, динаміка підпису.

Для порівняння методів автентифікації були проаналізовані найбільш розповсюджені показники біометричних систем [3]: визнання користувачами (згода людей на збір даних, ступінь психологічного комфорту, час, який потрібен людині для взаємодії з пристроєм), стійкість до підробок та атак (можливість використання різних «дублікатів», таких як зліпки, магнітофонні записи тощо), вартість, простота використання, FRR (частота відмов в обслуговуванні), FAR (частота помилкових спрацьовувань), час розпізнавання об'єкту (час, який потрібен для обслуговування одного користувача), розмір шаблону (чим більше розмір образу, тим більше часу потребує розпізнавання), стабільність роботи методу при хворобах та старінні. Результат оцінювання біометричних ме-

тодів автентифікації за вище згаданими показниками після ранжування за шкалою важливості (від 1 до 9) зведений до табл. 1. Для оцінювання найбільш ефективного методу автентифікації був використаний метод власних векторів – метод Сааті. Були розраховані матриці попарних порівнянь Сааті для кожного критерію, коефіцієнти пріоритету альтернатив та визначені усереднені значення пріоритетності методів біометричної автентифікації з урахуванням усіх критеріїв, тобто визначено найкращий біометричний метод на основі багатокритеріального аналізу. Результати розрахунків приведені на рис. 1.

Таблиця 1

Порівняльний аналіз показників біометричних методів автентифікації

Біометрична технологія / Показник	Визнання користувачами	Стійкість до підробок та атак	Вартість	Простота використання	FRR	FAR	Час розпізнавання об'єкту	Розмір шаблону	Стабільність роботи при хворобах
Відбиток пальця	5	5	7	8	5	5	6	5	9
Геометрія руки	5	6	4	8	5	5	8	9	4
Геометрія обличчя	9	3	7	9	1	6	8	5	3
Райдужна оболонка	4	6	5	6	7	7	7	7	8
Динаміка підпису	7	4	6	8	8	7	9	7	6
Голос	9	1	9	9	3	5	6	2	3

Результати оцінки показали, що найбільш високий коефіцієнт пріоритету має біометрична технологія розпізнавання підпису, близькими за значеннями виявилися методи розпізнавання особистості за райдужною оболонкою ока та відбитком пальцю, а найгіршим – розпізнавання за голосом.

Оскільки різні характеристики методів мають різну вагу і по-різному сприймаються користувачами, були введені вагові коефіцієнти на критерії і було визначено оптимальний метод автентифікації з урахуванням ваг критеріїв.

Результати досліджень (рис. 2) показують, що оптимальним за сукупністю критеріїв з їх важливості є метод динамічного підпису. Також близькі значення до оптимального мають методи автентифікації за райдужною оболонкою ока та за відбитком пальця.

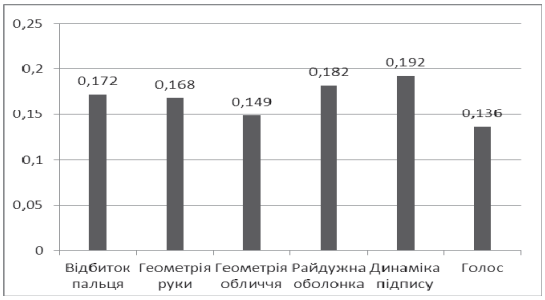

Рис. 1. Порівняння методів автентифікації на основі багатокритеріального аналізу

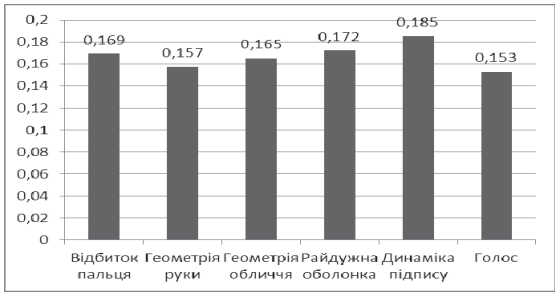

Рис. 2. Порівняння методів автентифікації на основі багатокритеріального аналізу

Аналіз мультимодальних біометричних систем

Для підвищення надійності захисту інформації використовують мультимодальні системи. В таких системах застосовується більше одного датчика, одного екземпляру та/або алгоритму в тій чи іншій комбінації для прийняття певного рішення щодо біометричної ідентифікації або верифікації.

Мультимодальні біометричні системи приймають вхідний сигнал з одного або безлічі датчиків, які, в свою чергу, отримують біометричні характеристики двох або більше модальностей.

Вибір та кількість біометричних ознак, що використовуються при проектуванні мультибіометричної системи, є змінними та повинні обиратися перед розгортанням системи.

Сутність багатокритеріального аналізу ефективності систем біометричної ідентифікації та автентифікації полягає в раціональному виборі системи з урахуванням її відповідності та адаптації до чинників, які можуть грати ключову роль в сфері захисту інформації для того чи іншого сценарію.

В роботах [4–5] були проведені дослідження з точки зору практичної реалізації мультимодальних біометричних технологій, заснованих на об'єднанні біометричних систем на рівні ступенів схожості. На основі даних експериментів проведено власне дослідження, його результати відображені на графіках зале-

жності частоти помилкових спрацьовувань від частоти відмов в обслуговуванні для мультибіометрічних систем на основі геометрії обличчя (рис. 3) та відбитку пальця (рис. 4).

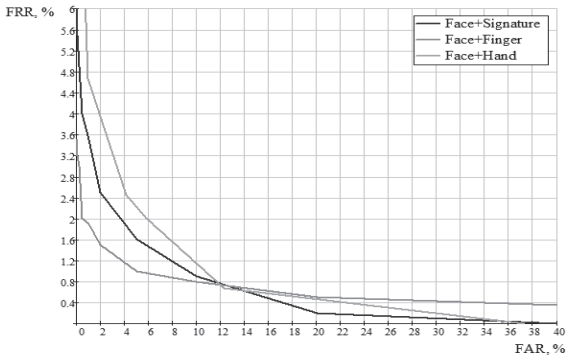

Рис. 3. Графік залежності FAR від FRR для мультибіометрічних систем на основі геометрії обличчя

На графіках видно, що при низьких значеннях FAR та FRR з мультимодальних систем на основі геометрії обличчя (рис. 3) можна виділити технологію, яка комбінує у собі технології розпізнавання людини за обличчям та відбитком пальця.

У свою чергу, в результаті порівняльного аналізу мультибіометрічних систем на основі відбитку пальця (рис. 4) кращим вибором двомодальної системи є та, що заснована на методах біометричної автентифікації особистості за відбитком пальця та динамікою підпису. Саме ця система має найнижче значення «помилок другого роду» (FAR) до 6,6% включно при 0,5% значення «помилок першого роду» (FRR).

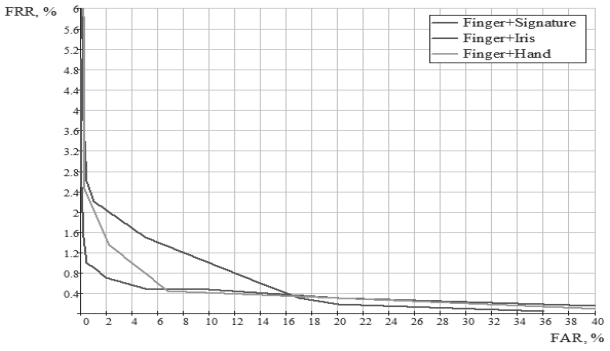

Рис. 4. Графік залежності FAR від FRR для мультибіометрічних систем на основі відбитку пальця

Таким чином, для оцінювання ефективності мультибіометричних систем необхідно порівняти ці методи між собою. Після отримання залежності значень FAR та FRR для цих мультимодальних технологій (табл. 2 та рис. 5) можна прийти до остаточного висновку, що кращою багатофакторною біометричною системою є система розпізнавання за відбитками пальців, підписом та за геометрією обличчя.

Таблиця 2

Відповідність значень FAR та FRR для мультимодальних біометричних систем

	FAR, %		
FRR, %	Обличчя + Відбиток	Відбиток + Підпис	Обличчя + Відбиток + Підпис
4	1,17	0,58	0,44
8	0,88	0,48	0,29
12	0,74	0,45	0,19
16	0,63	0,38	0,18
20	0,51	0,32	0,16

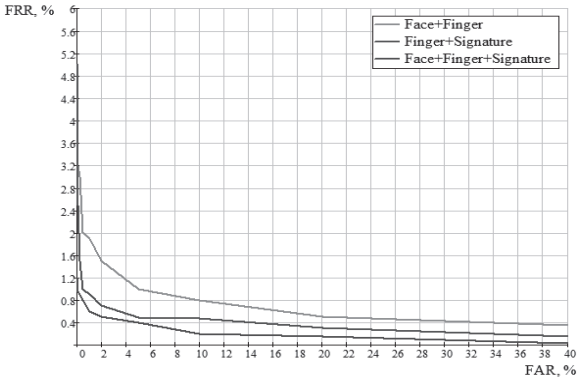

Рис. 5. Графік залежності FAR від FRR для вибору кращої мультибіометрічної системи

Втім, якщо взяти до уваги, що ця система має незначний виграш у точності та надійності і є більш складною у реалізації, досить дорогою та вимогливою до користувачів (потребує великих зусиль для отримання біометричних зразків апаратурою, що реєструє, за достатньо великий час, який потрібен людині для взаємодії з цими пристроями), то кращим варіантом слід вважати систему біометричної автентифікації та ідентифікації за відбитком пальця та підписом.

Висновки

В роботі були розглянуті основні види динамічних і статичних методів біометричної ідентифікації та верифікації. Виконано багатокритеріальний аналіз біометричних систем за їх показниками для того, щоб обрати оптимальний метод, який дозволить отримувати дані для прихованої передачі інформації в системах авторизації користувачів. Результати цього дослідження показали, що кращим за всіх традиційних методів біометричної автентифікації та ідентифікації особистості є метод динамічного підпису. Цей метод має цілком прийнятні рівні ймовірності помилок першого та другого роду – 0,05%. Перевагами цього методу є те, що характеристики, які використовуються для розпізнавання динамічного підпису, майже неможливо скопіювати, верифікація підпису проходить досить швидко, а для збері-

гання шаблонів потрібно небагато місця. Цей метод є звичним для людини, так як він є найпоширенішим і загальновизнаним способом підтвердження своєї особистості. Для дактилоскопії помилки першого роду складають 2%, а час розпізнавання одного користувача є досить великим, хоча за вартістю та стабільністю роботи при старінні та хворобах він є кращім ніж динамічний підпис. Система розпізнавання за райдужною оболонкою ока є також кращою за показником «стабільність роботи при старінні та хворобах», ніж технологія розпізнавання за підписом, так як вона практично не змінюється протягом життя. Біометрична система розпізнавання за голосом за значеннями критеріїв «визнання користувачами», «простота використання» та «вартість» має найкращі значення, ніж інші системи, однак вона має найнижче значення показника «стійкість до підробок та атак».

При застосуванні однофакторної біометричної автентифікації більш доцільно використовувати динамічний метод розпізнавання за підписом, а при багатофакторній – кращою є система, яка поєднує технології розпізнавання користувача за відбитками пальців, підписом та за геометрією обличчя.

Результати дослідження можуть бути використані при виконанні автентифікації користувачів мобільних пристроїв, де кількість використаних факторів автентифікації залежить від вимог додатка (наприклад, камера чи платіжна система).

Список літератури

1. *Jain A.K. 50 Years of Biometric Research: Accomplishments, Challenges and Opportunities [Text] / Jain A.K., Nandakumar K., Ross A.// Pattern Recognition Letters. – 2016. – №79. – P. 80-105.*
2. *Колешко В.М. Традиционные методы биометрической аутентификации и идентификации [Текст] : учеб. пособие / В.М. Колешко, Е.А. Воробей, П.М. Азизов и др. – М.: БНТУ, 2009. – 107 с.*
3. *Jain A.K. An Introduction to Biometric Recognition [Text] / A.K. Jain, A. Ross, S. Prabhakar // IEEE Transactions on Circuits and Systems for Video Technology –2004. – № 14. – 4 –20p.*
4. *Kaur G. Comparative Analysis of Biometric Modalities [Electronic resource] / G. Kaur, Ch. K. Verma // International Journal of Advanced Research in Computer Science and Software Engineering – Mode of access: https://www.ijarcsse.com/docs/papers/Volume_4/4_April2014/V4I4-0407.pdf – 2014. – Title from the screen.*
5. *Fierrez-Aguilar J. A Comparative Evaluation of Fusion Strategies for Multimodal Biometric Verification [Text] / J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, J. Gonzalez-Rodriguez // Audio- and Video-Based Biometric Person Authentication. – 2003. – №2688. – P.830-837.*

Надійшла до редколегії 9.03.2017

Рецензент: д-р техн. наук, проф., С.Г. Удовенко, Харківський національний економічний університет ім. Семена Кузнеця, Харків.

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Г.Є. Ляшенко, А.А. Астраханцев

В данной статье рассмотрены основные существующие статические и динамические методы биометрической аутентификации; выполнен многокритериальный анализ по наиболее распространенным показателям биометрических систем; определены оптимальные методы, которые обеспечивают наименьшее значение частот ложных срабатываний и отказов в обслуживании; проанализирована эффективность работы мультибиометрических систем, которые используют для повышения надежности систем аутентификации.

Ключевые слова: *аутентификация, биометрическое распознавание, мультибиометрические системы.*

ANALYSIS OF BIOMETRIC AUTHENTICATION TECHNIQUES

G. Liashenko, A. Astrakhantsev

This article describes the main existing static and dynamic methods of biometric authentication. The multi-criteria analysis of the most common biometric systems indicators is made. The optimal methods for authenticate mobile users based on FAR and FRR are defined. Multifactor biometric system is analyzed. The best for mobile users scenario case is determined.

Keywords: *authentication, biometric recognition, multi-biometric system.*