УДК 004.056.523:57.087.1

МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ОСОБИ ТА ЇХ ПОРІВНЯННЯ

Коломієць Є.Д.
e-mail: yehor.kolomiiets@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна

The article explores the development of biometric authentication as a modern security mechanism in response to the growing need for reliable and accurate identity verification. It shows different biometric methods, including fingerprint, palm, vein, facial, and iris recognition, as well as dynamic techniques like voice and handwriting analysis. The article highlights the advantages of biometric authentication, such as accuracy and resistance to fake, while also addressing challenges like cost and vulnerability to fake. The article provides a comparative analysis of different methods, evaluating their reliability, uniqueness, and practicality in contemporary security systems.

З розвитком людства та технологій збільшувалася кількість інформації та необхідність її захисту від несанкціонованого доступу. Якщо раніше для підтвердження особи, прав на володіння інформацією або доступу до неї вистачало підпису чи документу, то зараз, у часи стрімкого розвитку інформаційних технологій, такі методи, через свою легкість в підробці та недостатню надійність, швидкими темпами поступаються місцем більш сучасним. Методи біометричної авторизації є однією з течій сучасної системи захисту інформації.

Умовно, їх можна розділяти за методом взаємодії на тактильні та нетактильні, за методом використання на статичні та динамічні чи за особливостями зчитування, але усі групи об’єднує їх надійність та зручність у використанні для звичайної особи. Надійність методу включає в себе точність та стійкість до зламу. Точність розраховується за допомогою двох показників: ймовірності помилкового підтвердження та ймовірності помилкової відмови. Ці показники залежать від методу та типу сканеру. Стійкість відображає, наскільки багато у методу вразливостей і наскільки легко пройти перевірку з фальшивими даними.

Серед основних методів біометричної авторизації можна виділити:

- розпізнавання за відбитком пальців;
- розпізнавання за відбитком долоні;
- розпізнавання за формою долоні;
- розпізнавання за будовою кровоносної системи;
- розпізнавання за формою та мімікою обличчя;
- розпізнавання за візерунком райдужної оболонки ока;
- розпізнавання за динамічними ознаками (почерк, голос та інше).

Розпізнавання за відбитками пальців є найпоширенішим та найпростішим у використанні та перевірці серед тактильних методів біометричної авторизації. З розвитком мобільних пристроїв цей метод став частиною повсякденного життя та стандартом простої системи захисту. Серед його основних плюсів можна виділити гарну точність та малу вартість, але, через свою простоту цей метод є вразливим для підробки [1].

Схожим до відбитків пальців є метод розпізнавання за відбитком долоні. На відміну від попереднього, він є менш поширеним, компактним та дешевим, але має кращі показники точності та набагато стійкіший.

Останнім серед тактильних методів є розпізнавання за геометрією долоні. Для розпізнавання використовуються данні про розміри долоні, довжину та ширину пальців та інше. В порівнянні з іншими, цей метод є застарілим, більш громіздкі та менш точним, але він і досі має великий попит та використовуються для доступу у режимні приміщення.

Розпізнавання за будовою кровоносної системи є унікальним методом біометричної автентифікації. Для зняття та перевіри біометричних даних використовується низькочастотне (для сітківки) та високочастотне (для пальців та долоні) світло, за допомогою якого отримують зображення структури вен та капілярів, яке є унікальним для кожної людини [2]. Цей метод має дуже високу стійкість та точність, однак є менш поширеним та більш дорогим.

Розпізнавання за райдужною оболонкою ока також використовує унікальні параметри для автентифікації, але він майже повністю втрачає свою стійкість у випадку, коли зловмиснику вдалося підробити необхідні для автентифікації данні. Такий механізм розпізнавання є гарним методом автентифікації але через високу вартість та розвиток інших методів, він стає менш привабливим для вибору.

Останнім серед статичних є метод розпізнавання за обличчям, який поділяють на два типи за методом сканування: 3D та 2D. На першому етапі розвитку цього методу використовувалося 2D сканування, яке мало погані показники точності та стійкості, але в подальшому розвитку, на основі нього, були розроблені метод 3D сканування, які не тільки не програє в точності іншим способам розпізнавання, але й іноді випереджає їх. Серед інших методів, розпізнавання за формою та мімікою обличчя має найшвидший розвиток та поширення у сучасному світі, чому сприяє стрімкий розвиток штучного інтелекту, мала вартість сканерів та соціальна політика деяких країн.

Окремою галуззю є динамічні методи розпізнавання. До них відносять розпізнавання за голосом, рукописним почерком, методом натискання клавіш на клавіатурі, манерою ходження, рухами миші або натисканням на екран телефону. Усі вони мають доволі низьку стійкість та точність, оскільки фактори, які використовуються для розпізнавання можна легко змінити або підробити.

Розглянувши усі методи можна сформувати загальну порівняльну таблицю, в якій будуть враховані такі фактори: точність, стійкість, унікальність (відмінність), ціна та частота використання (поширеність) [3]. Оцінку цих факторів будуть зображені за допомогою умовних позначень В, С та Н, де В – високий показник, С – середній і Н – низький. Порівняння методів розпізнавання зображено в таблиці 1.

Таблиця 1 – Порівняння методів біометричної автентифікації.

Метод	Точність	Стійкість	Унікальність	Ціна	Частота
Відбитки пальців	В	Н	С	Н	В
Відбитки долоні	В	С	С	С	С
Форма долоні	С	С	С	С	В
Кровоносна система	В	В	В	В	Н
Райдужна оболонка	В	С	В	В	С
Форма обличчя	В	С	С	Н	В
Динамічні	Н	Н	С	В	Н

Роблячи висновок з порівняння різних методів, можна сказати, що найбільш точним та надійним є метод розпізнавання за кровоносною системою, але через високу вартість та габаритність його використання не завжди є доцільним. Натомість, метод розпізнавання за формою та мімікою обличчя за останні роки значно підвищив свої показники точності та стійкості. Цей метод є перспективним для розвитку й поширення, а також надає можливість інтегрувати в алгоритми перевірки новітні технології, такі як штучний інтелект або сучасні камери.

Список використаних джерел:

1. Paul Rascagneres. Fingerprint cloning: Myth or reality?. Cisco Talos: вебсайт. URL: https://blog.talosintelligence.com/fingerprint-research/ (дата звернення 02.03.2025).
2. What is Biometrics? Definition, Data Types, Trends (2024). Aratek: вебсайт. URL: https://www.aratek.co/news/what-is-biometrics-definition-data-types-trends (дата звернення 03.03.2025).
3. Mohammad Al Rousan. A Comparative Analysis of Biometrics Types: Literature Review. Journal of Computer Science 16(12): с 1778-1788. DOI: 10.3844/jcssp.2020.1778.1788. електронний збірник. URL: https://www.researchgate.net/publication/347971656_A_Comparative_Analysis_of_Biometrics_Types_Literature_Review (дата звернення 03.03.2025).