УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.105

МЕТОДИ ТА МОДЕЛІ БАГАТОДЖЕРЕЛЬНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Кайдалов В.Д.
Науковий керівник – к.т.н., доцент Голян В.В.
Харківський національний університет радіоелектроніки, каф. ПІ,
м. Харків, Україна
e-mail: vadym.kaidalov@nure.ua

Authentication can be achieved using one or more of three fundamental factors: knowledge-based, possession-based, and biometric features. The latter has gained popularity as a reliable alternative solution. Biometric features are categorized into physiological features, behavioral features, and “soft” features. Each of them has its advantages and disadvantages, including the financial cost of installing appropriate sensors and the amount of time spent by users to interact with these sensors. Multimodal biometric authentication utilizes several independent features (such as face and voice) and does not rely on a single characteristic. As a result, it is much more resistant to spoofing attacks and mitigates the negative impact of noise and low-quality data.

Автентифікація користувача широко використовується як засіб захисту будь-якої інформаційної системи (ІС) від дій зловмисників. Інформаційній системі необхідно перевірити ідентичність користувача, зазвичай використовуючи такі облікові дані, як ім’я користувача та пароль, щоб потім наділити користувача певними привілеями (авторизувати) для доступу до ресурсів системи. Оскільки ІС тісно пов’язані з нашим повсякденним життям, надійна автентифікація є надзвичайно важливою для забезпечення безпеки в будь-якій ІС. Більше 40 років проводиться інтенсивне дослідження методів автентифікації – це підтверджує важливість процесу автентифікації для створення безпечних середовищ, які захищають ІС від підробки ідентичності користувача, а також намагаються полегшити або спростити сам процес взаємодії користувача з системою автентифікації.

Автентифікація користувача може бути здійснена за допомогою одного або декількох з трьох фундаментальних факторів:

- на основі знання (щось, що користувач знає),
- на основі володіння (щось, чим користувач володіє),
- на основі біометричних ознак (щось, чим користувач є).

Останній фактор, біометричні ознаки, набув популярності як надійне альтернативне рішення [1].

Біометричні ознаки, за походженням, діляться на наступні групи:

– фізіологічні ознаки базуються на унікальних фізичних рисах особи (відбитки пальців, райдужна оболонка ока, форма та риси обличчя тощо);

– поведінкові ознаки відносяться до поведінки особи (аналіз ходи, динаміка натискання клавіш на клавіатурі, рух комп'ютерної миші, рух пальців на сенсорному екрані, голос тощо);

– «м'які» ознаки не надають можливості унікально ідентифікувати особу, але надають корисну додаткову інформацію (стать, зріст, колір волосся тощо).

Використання тих чи інших ознак має свої переваги та недоліки, включаючи фінансову вартість встановлення відповідних сенсорів та час, який користувачу необхідно витрачати на взаємодію з цими сенсорами. Наприклад, збір даних про взаємодію з клавіатурою під час роботи користувача не вимагає ні додаткових фінансових витрат, ні додаткового часу на надання користувачем біометричних даних на відміну від сканування райдужки очей, яке, з іншого боку, надає більшу постійність даних і призводить до вищої точності автентифікації [2].

Задачу проведення автентифікації можна представити у вигляді задачі однокласової класифікації, в якій за зразком вхідних даних необхідно встановити, чи належить наданий зразок до визначеного класу, чи ні. Зразок вхідних даних – це зразок даних біометричної ознаки користувача, наприклад, двовимірне зображення райдужки ока чи двовимірна таблиця, що зберігає ідентифікатори клавіш клавіатури та моменти часу, в які вони були натиснуті. Відношення зразку вхідних даних до визначеного класу означає, що зразок був згенерований в результаті взаємодії справжнього користувача з ІС, що підтверджує ідентичність. Якщо зразок вхідних даних не відноситься до цього єдиного класу, то ідентичність не підтверджується, і тоді ІС перериває сесію користувача і припиняє надання доступу до себе, поки ідентичність не буде підтверджена тим чи іншим шляхом знову.

Залежно від кількості біометричних джерел, які використовуються, біометричну систему автентифікації можна класифікувати на два типи: одноджерельну (одномодальну, унімодальну) або багатоджерельну (багатомодальну, мультимодальну). Одноджерельні біометричні системи ґрунтуються на одному джерелі для автентифікації і тому їх легше розробляти, оскільки вони базуються на одному ідентифікаторі. Однак, одноджерельна система стикається з такими викликами, як шумні дані, погана продуктивність розпізнавання, нижча точність та атаки підробки, оскільки для успішної атаки достатньо підробити усього одну біометричну ознаку. Багатоджерельна біометрична автентифікація, навпаки, використовує кілька незалежних ознак (наприклад, обличчя та голос), не ґрунтується на одній ознаці і тому набагато

більш стійка до атаки підробки та зменшує негативний вплив шумів і низької якості даних [3].

У випадку з багатоджерельною біометричною аутентифікацією, виникає потреба обчислити єдину оцінку схожості на основі обробки даних, отриманих з декількох джерел – здійснити так зване «злиття» (англ. «fusion»). В залежності від етапу, на якому відбувається злиття, існують наступні найуживаніші методи:

– злиття на рівні оцінок (англ. «score level fusion») – метод, що об'єднує оцінки схожості, незалежно отримані від декількох класифікаторів, кожен з яких працює зі своїм джерелом біометричних даних. Незалежність роботи класифікаторів надає можливість приєднувати додаткові класифікатори, які будуть впливати на загальну оцінку тільки на етапі злиття, не впливаючи на роботу інших компонентів;

– злиття на рівні ознак (англ. «feature level fusion») – є другим за популярністю методом злиття, що поєднує різні ознаки, витягнуті з сирої біометричної інформації, в один єдиний масив даних, що надалі обробляється єдиним класифікатором. Цей процес може усунути шум в сирій біометричній інформації, що потенційно покращує точність автентифікації. Об'єднання на рівні ознак дозволяє анонімізувати зображення та набори ознак, створюючи новий "непрозорий" масив даних для автентифікації, що також може сприяти підвищенню конфіденційності зберігання біометричних даних у системах віддаленого доступу. Однак через високу розмірність даних, об'єднання на рівні ознак генерує вище обчислювальне навантаження.

Неперервна багатоджерельна біометрична автентифікація (англ. «continuous multimodal biometric authentication») з'явилася для покращення точності перевірки ідентичності та усунення вразливостей статичної автентифікації [1]. Однак, виникають проблеми з використанням та масштабованістю, оскільки CMBA вимагає неперервної перевірки заявленої ідентичності впродовж сесії користувача, що веде до підвищення споживання обчислювальних ресурсів, розміру збережених даних тощо.

Список використаних джерел

1. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review / R. Ryu et al. *IEEE Access*. 2021. Vol. 9. P. 34541–34557. URL: https://doi.org/10.1109/access.2021.3061589 (date of access: 12.03.2024).

3. Dee T., Richardson I., Tyagi A. Continuous Nonintrusive Mobile Device Soft Keyboard Biometric Authentication. *Cryptography*. 2022. Vol. 6, no. 2. P. 14. URL: https://doi.org/10.3390/cryptography6020014 (date of access: 12.03.2024).

3. Continuous and transparent multimodal authentication: reviewing the state of the art / A. Al Abdulwahid et al. *Cluster Computing*. 2015. Vol. 19, no. 1. P. 455–474. URL: https://doi.org/10.1007/s10586-015-0510-4 (date of access: 12.03.2024).