УДК 004.056.5

В. О. Пальчик
К. В. Безпалий

МЕТОД АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА ЖЕСТОВИМ ПАРОЛЕМ НА ОСНОВІ АНАЛІЗУ КЛЮЧОВИХ ТОЧОК РУКИ

Вінницький національний технічний університет

Анотація

У роботі запропоновано метод автентифікації користувача за жестовим паролем, що ґрунтується на аналізі ключових точок руки, отриманих зі стандартної веб-камери. Описано підхід до формування ознакового вектора на основі landmark-представлення кисті, що включає нормалізовані координати 21 ключової точки, кути нахилу пальців та евклідові відстані від кінчиків пальців до центру долоні. Розглянуто алгоритм послідовної перевірки чотирьох жестів із використанням евклідової відстані, порогової оцінки подібності та часової стабілізації за кількістю послідовних кадрів. Запропонований метод дає змогу реалізувати природну взаємодію користувача із системою та підвищити стійкість автентифікації порівняно з перевіркою одного жесту.

Ключові слова: автентифікація, жестовий пароль, MediaPipe, ключові точки руки, біометрія, комп'ютерний зір.

Abstract

The paper proposes a user authentication method based on a gesture password and the analysis of hand keypoints captured by a standard webcam. The approach to feature vector construction is described using a landmark-based hand representation that includes normalized coordinates of 21 keypoints, finger inclination angles, and Euclidean distances from fingertips to the palm center. The algorithm of sequential verification of four gestures is considered using Euclidean distance, threshold-based similarity estimation, and temporal stabilization by the number of consecutive frames. The proposed method enables natural user interaction with the system and improves authentication robustness compared with single-gesture verification.

Keywords: authentication, gesture password, MediaPipe, hand keypoints, biometrics, computer vision.

Вступ

У сучасних інформаційних системах автентифікація є одним із ключових механізмів захисту доступу до даних і сервісів. Традиційні парольні методи залишаються поширеними, однак вони мають низку практичних недоліків: користувачі часто обирають прості паролі, повторно використовують їх у різних системах або зберігають у небезпечний спосіб. Біометричні та поведінкові методи автентифікації частково вирішують ці проблеми, оскільки використовують індивідуальні характеристики користувача або особливості його взаємодії з системою [1, 2].

Одним із перспективних напрямів є автентифікація за жестами руки. У такому підході секретом виступає не текстова комбінація символів, а визначена користувачем послідовність жестів. Це робить взаємодію більш природною, а також дозволяє застосувати методи комп'ютерного зору для формального опису положення кисті. Розвиток фреймворків на зразок MediaPipe створює технічні передумови для реалізації таких систем у режимі реального часу без використання спеціалізованого обладнання [3, 4].

Метою роботи є розроблення методу автентифікації користувача за жестовим паролем на основі аналізу ключових точок руки. Для досягнення цієї мети необхідно сформувати числове представлення жесту, забезпечити його стійкість до незначних змін положення руки у кадрі та визначити алгоритм прийняття рішення про успішність автентифікації.

Результати дослідження

Запропонований метод передбачає використання стандартної веб-камери для отримання відеопотоку та подальшого виділення ключових точок руки. На етапі попередньої обробки кадр може дзеркально відображатися для зручності користувача та перетворюватися у формат, придатний для подальшої обробки моделлю розпізнавання. Основним компонентом виділення ознак є модель MediaPipe HandLandmarker, яка визначає 21 ключову точку кисті та повертає їхні тривимірні координати [5].

Ознаковий вектор одного жесту формується з трьох груп характеристик. Перша група містить нормалізовані координати 21 ключової точки руки, що дає 63 числові ознаки. Друга група включає кути нахилу пальців, які обчислюються для п’яти кінчиків пальців і характеризують їхню орієнтацію у площині зображення. Третя група складається з евклідових відстаней від кінчиків пальців до центру долоні, що відображає ступінь розкриття пальців і загальну форму кисті. У результаті для однієї руки формується 73-вимірний вектор ознак, а в режимі двох рук - 146-вимірний вектор шляхом конкатенації двох окремих представлень.

Важливою складовою методу є часове усереднення ознак. Оскільки окремий кадр може містити шум детекції, незначне тремтіння руки або неточності розпізнавання, еталонний жест доцільно формувати не за одним зображенням, а за серією послідовних кадрів. У матеріалі системи передбачено накопичення 60 кадрів, після чого обчислюється середній вектор ознак. Такий підхід зменшує вплив випадкових відхилень і підвищує стабільність еталонного представлення жесту.

Автентифікація користувача реалізується як перевірка жестового пароля - послідовності з чотирьох жестів, визначених під час реєстрації. На відміну від перевірки одного жесту, послідовна модель ускладнює несанкціонований доступ, оскільки зловмисник повинен відтворити не лише форму кожного жесту, а й правильний порядок їх виконання. Для кожного кроку автентифікації поточний вектор ознак порівнюється з відповідним еталонним вектором користувача.

Мірою відмінності між поточним і еталонним жестом є евклідова відстань у просторі ознак. Для зручності інтерпретації ця відстань перетворюється на відсоткову оцінку подібності у діапазоні від 0 до 100 %. Рішення про збіг приймається у разі перевищення встановленого порогу подібності. У спроєктованому методі використовується поріг 75 %, що є компромісом між зручністю для легітимного користувача та стійкістю до випадкового або навмисного відтворення жесту.

Для зменшення кількості хибних спрацьовувань використовується механізм часової стабілізації. Жест зараховується лише тоді, коли умова перевищення порогу подібності виконується протягом 15 послідовних кадрів. За частоти відеопотоку близько 30 кадрів за секунду це відповідає приблизно половині секунди стабільного утримання жесту. Така вимога відсіює випадкові короткочасні збіги та робить процес автентифікації більш надійним.

Логіку роботи методу можна подати як детермінований скінченний автомат із послідовними станами перевірки жестів. Початковий стан відповідає очікуванню запуску автентифікації, проміжні стани - перевірці першого, другого, третього та четвертого жестів, а термінальний стан - успішному або відхиленому завершенню перевірки. Перехід до наступного стану відбувається лише після стабільного підтвердження поточного жесту. Така модель є формально зрозумілою, передбачуваною та придатною для програмної реалізації.

Перевагою запропонованого підходу є те, що система не потребує збереження відеозаписів користувача. У профілі можуть зберігатися лише компактні числові вектори ознак та службові метадані, зокрема режим використання однієї або двох рук і дата реєстрації. Це зменшує обсяг збережуваних даних і підвищує конфіденційність, оскільки з числового вектора значно складніше відновити початковий відеофрагмент.

Запропонований метод може бути реалізований у вигляді локальної інтелектуальної системи автентифікації з графічним інтерфейсом користувача. На рівні архітектури доцільно розділити систему на модулі захоплення відеопотоку, виділення ознак, порівняння з еталонами та взаємодії з користувачем. Такий поділ відповідає принципу розподілу відповідальності та дозволяє окремо вдосконалювати модуль розпізнавання, алгоритм порівняння або інтерфейс без повної перебудови системи.

Висновки

У роботі запропоновано метод автентифікації користувача за жестовим паролем на основі аналізу ключових точок руки. Метод поєднує landmark-представлення кисті, формування багатовимірного вектора ознак, порівняння за евклідовою відстанню та послідовну перевірку чотирьох жестів.

Сформований вектор ознак містить координатні, кутові та відстанні характеристики, що дозволяє описати як просторове положення ключових точок, так і відносну геометрію кисті. Використання часового усереднення під час реєстрації та стабілізації за 15 послідовними кадрами під час входу підвищує надійність розпізнавання і зменшує вплив короткочасних шумів відеопотоку.

Запропонований підхід є придатним для побудови локальної системи автентифікації, що працює зі стандартною веб-камерою та не потребує збереження відеозаписів користувача. Подальший розвиток методу може передбачати експериментальне уточнення порогів подібності, розширення алфавіту

жестів, аналіз стійкості до атак повторення та оцінювання показників хибного прийняття і хибної відмови.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке автентифікація? Визначення й способи | Захисний комплекс Microsoft. Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-authentication (дата звернення: 10.02.2026).
2. Maslova N. O., Polunina D. O. Biometric authentication methods for personal identification. Naukovyi visnyk Donetskoho natsionalnoho tekhnichnoho universytetu. 2019. Т. 1(2), № 2(3). С. 12-20. URL: https://doi.org/10.31474/2415-7902-2019-1(2)-2(3)-12-20 (дата звернення: 10.02.2026).
3. Yasen M., Jusoh S. A systematic review on hand gesture recognition techniques, challenges and applications. PeerJ Computer Science. 2019. Т. 5. С. e218. URL: https://doi.org/10.7717/peerj-cs.218 (дата звернення: 10.03.2026).
4. Lugaresi C. та ін. MediaPipe: A Framework for Building Perception Pipelines. arXiv.org. URL: https://arxiv.org/pdf/1906.08172 (дата звернення: 10.03.2026).
5. Zhang F. та ін. MediaPipe Hands: On-device Real-time Hand Tracking. arXiv.org. URL: https://arxiv.org/pdf/2006.10214 (дата звернення: 10.03.2026).
6. Hand landmarks detection guide | Google AI Edge | Google AI for Developers. Google AI for Developers. URL: https://ai.google.dev/edge/mediapipe/solutions/vision/hand_landmarker (дата звернення: 10.03.2026).
7. Dynamic Hand Gesture Recognition Using MediaPipe and Transformer. MDPI. URL: https://doi.org/10.3390/engproc2025108022 (дата звернення: 10.03.2026).

Пальчик Владислав Олександрович - студент групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: vladthefinger@gmail.com

Науковий керівник: ***Безпалий Кирило Валерійович*** - асистент кафедри МБІС, Вінницький національний технічний університет, м. Вінниця, e-mail: kyrylo.bezpalyi@vntu.edu.ua

Palchyk Vladyslav O. - student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: vladthefinger@gmail.com

Scientific adviser: ***Bezpalyi Kyrylo V.*** - Assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: kyrylo.bezpalyi@vntu.edu.ua