

СТВОРЕННЯ ІНТЕЛЕКТУАЛЬНОЇ ПІДСИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ДЛЯ СИСТЕМИ РОЗУМНИЙ БУДИНОК

Сучасний етап розвитку технологій характеризується стрімкою інтеграцією штучного інтелекту та методів комп'ютерного зору в системи типу «Розумний будинок» [1]. Це відкриває нові горизонти для автоматизації побутових процесів, управління приладами та налаштування індивідуальних сценаріїв у житлових і комерційних приміщеннях.

Проте більшість наявних рішень виконують задачі базової автоматизації, реагуючи виключно на факт присутності фізичного об'єкта в зоні дії сенсорів руху. В таких умовах усі сценарії стають універсальними, а система працює без урахування індивідуальних потреб конкретного користувача. Стандартна інфраструктура не здатна ідентифікувати особу без активної взаємодії, наприклад, використання смартфонів, фізичних ключів, RFID-міток або голосових команд. Відсутність точної біометричної ідентифікації унеможливорює гнучку видачу прав доступу до певних приміщень власникам, гостям або стороннім особам.

Метою даної роботи є підвищення ефективності персоналізованого керування доступом та рівеня безпеки в системах домашньої автоматизації на основі інтелектуальної підсистеми біометричної ідентифікації.

Архітектура подібних систем базується на трьох класичних рівнях: рівні сприйняття (IP-камери та сенсори), рівні керування (центральный хаб) та рівні виконання (виконавчі пристрої та мультимедіа). На відміну від комерційних екосистем (Apple HomeKit, Google Home), які залежать від хмарних обчислень і створюють ризики перехоплення відеопотоку, локальна підсистема може гарантувати вищу конфіденційність і захист даних, не передаючи дані у відкриту мережу [2]-[3].

Застосування парадигми граничних обчислень дозволяє виконувати всі ресурсомісткі процеси пошуку та виявлення об'єктів алгоритмами комп'ютерного зору безпосередньо на локальному сервері. До контролера розумного будинку через протокол MQTT передається лише фінальний текстовий результат у форматі JSON, що містить ідентифікатор особи та рівень збігу, мінімізуючи мережеві затримки.

Програма реалізація підсистеми базується на бібліотеках OpenCV і FaceRecognitionDotNet. Ключовим викликом при розпізнаванні облич у побутових умовах є динамічне та нерівномірне освітлення. Звичайні каскади Хаара вкрай чутливі до глибоких тіней, хибно ідентифікуючи їх як перенісся

або очниці, а світло від вікон часто перетворює об'єкт на темний силует, що призводить до збою глибоких нейронних мереж [4]. Для розв'язання цієї проблеми можуть використовуватися алгоритми нормалізації зображень, які вирівнюють контраст перед подачею кадру на вхід алгоритмів розпізнавання.

Окрему увагу варто приділити захисту від атак типу «спуфінг» - обману камери [5]. Апаратні методи суттєво підвищують вартість системи, тому акцент робиться на програмних методах аналізу стандартного 2D RGB-відеопотоку. Система виявляє підробки (паперові фото або відео з екрана смартфона) шляхом аналізу мікротекстур, фіксуючи появу муару, відблисків скла та пікселізації. Крім того, алгоритм відстежує фонове моргання очей, що унеможливує злам системи за допомогою статичного зображення. Додатково для збільшення якості ідентифікації подібних зламів застосовується спеціалізована антиспуфінг-нейромережева модель (наприклад, MobileNet), яка працює як швидкий бінарний класифікатор для підтвердження «живого» обличчя.

Результатом роботи є підсистема, яка у режимі реального часу проводить відстеження й аналіз відеопотоку, ідентифікує особу, перевіряє її на предмет підробок та передає верифіковані дані для запуску відповідного персоналізованого сценарію.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kanimozhi V. The Role of Artificial Intelligence in Smart Homes *International Advanced Research Journal in Science, Engineering and Technology*. 2024. Vol. 11, № 6. P. 349-353.
2. Salama M. MQTT in Action: Building Reliable and Scalable Home Automation Systems. *Sakarya University Journal of Computer and Information Sciences*. 2024. Vol. 7, № 3. P. 494–509.
3. Comparison of Open-Source Home Automation Systems / B. Setz et al. *IEEE Access*. 2021. Vol. 9. P. 167332-167352.
4. The masked villain: the effects of facial masking, distance, lighting, and eyewitness age on eyewitness identification accuracy / T. J. Nyman et al. *Psychology, Crime & Law*. 2025. Vol. 31, № 3. P. 332–370.
5. Keresh A., Shamo P. Liveness Detection in Computer Vision: Transformer-based Self-Supervised Learning for Face Anti-Spoofing *IEEE Access*. 2024. Vol. 12. P. 185673-185685.