УДК 004.93

Б. М. Куцик

Сучасна аутентифікація “Optic ID” та її порівняння з “Touch ID”

Вінницький національний технічний університет

Анотація

У роботі порівняно середовища Optic ID та Touch ID, розглянуто їхні переваги та недоліки.

Ключові слова: аутентифікація, Optic ID, Touch ID, оптична аутентифікація, розпізнавання райдужної оболонки.

Abstract

This study compares environments of Optic ID and Touch ID, considered their advantages and disadvantages.

Keywords: authentication, Optic ID, Touch ID, optic authentication, iris recognition, multi-factor authentication.

Вступ

У дослідженні розглянуто сучасну інтеграцію середовища Optic ID в Apple Vision Pro та використання двох різних методів біометричної ідентифікації: Optic ID і Touch ID. Optic ID характеризується здатністю працювати за допомогою оптичної ідентифікації та розпізнавання райдужної оболонки, тоді як Touch ID характеризується простотою та швидкістю розпізнавання відбитків пальців. Обидва методи мають свої переваги і вибір залежить від бажань користувача. У майбутньому можливо буде необхідно поєднати їхні переваги, щоб створити більш ефективні системи ідентифікації.

Існує ймовірність того, що такий підхід до поєднання різних методів біометричної ідентифікації може бути дуже перспективним. Узгодження технологій Optic ID і Touch ID може підвищити безпеку та зручність для користувачів. Наприклад, існує потенціал для впровадження системи, яка спочатку перевіряє відбиток пальця за допомогою Touch ID, а потім використовує Optic ID для додаткової перевірки. Це підвищить рівень безпеки та запобігатиме потенційним шахрайствам. Майбутні інновації в галузі біометричних систем ідентифікації можуть залежати від цієї стратегії.

Результати дослідження

У досліджені розглянуто, що ефективність розпізнавання обличчя та об’єктів значно покращилася після додавання системи автентифікації «Optic ID» до технологій Apple Vision Pro.

Багатофакторна автентифікація, яка включає розпізнавання райдужної оболонки та оптичну автентифікацію, дозволяє системі точно та швидко ідентифікувати користувачів і об’єкти в різних умовах[2].

Крім того, багатофакторна автентифікація, яка включає розпізнавання райдужної оболонки та оптичну ідентифікацію, дозволяє уникати однобічного підходу до безпеки. Це означає, що необхідні додаткові процедури перевірки, щоб запобігти несанкціонованому доступу. Такий метод особливо важливий, оскільки багатофакторна автентифікація робить систему менш чутливою до атак і імітацій.

Розпізнавання райдужної оболонки та оптичної ідентифікації можуть забезпечити комплексний захист ідентичності, що стає важливим аспектом сучасного цифрового середовища.

Цей тип технологій дозволяє підвищити безпеку в цифрових середовищах, ідентифікуючи користувача за допомогою біометричних даних, таких як райдужна оболонка. Оскільки біометричні дані є унікальними для кожної людини, підробка чи використання без дозволу значно складніше. Такий метод захисту ідентичності стає все більш важливим у світі, де діджиталізація проникає в усі сфери життя.

На рисунку 1 зображено принцип роботи ідентифікації завдяки визначенню райдужної оболонки та зіниці. Такий метод ідентифікації базується на дослідженні особливостей зіниці та райдужної оболонки, що є однією з найнадійніших методів ідентифікації. За допомогою спеціалізованих камер або сканерів можна отримати зображення райдужної оболонки та зіниці, які фіксують особливості цих частин ока.

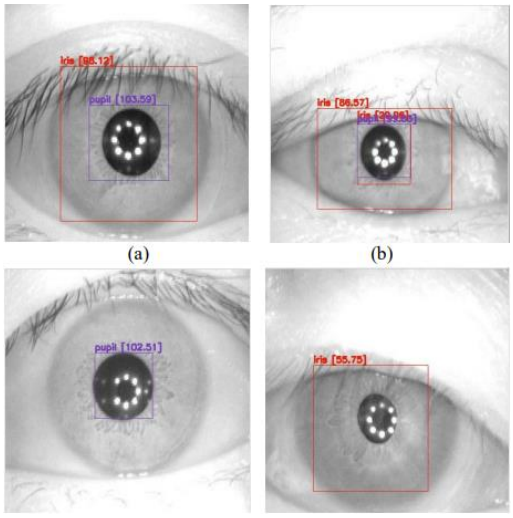

Рисунок 1 – Визначення райдужки та зіниці [3]

Особлива увага була приділена впливу освітлення на точність автентифікації. Результати показали, що «Оптичний ідентифікатор» добре адаптується до різних умов освітлення[3]. Система досить добре пристосована до змін яскравості та кутів падіння світла, що робить її досить надійною в різних умовах.

Було також виявлено, що багатофакторна автентифікація “Optic ID” підвищує загальну безпеку системи, забезпечуючи високу відповідність і запобігаючи несанкціонованому доступу.

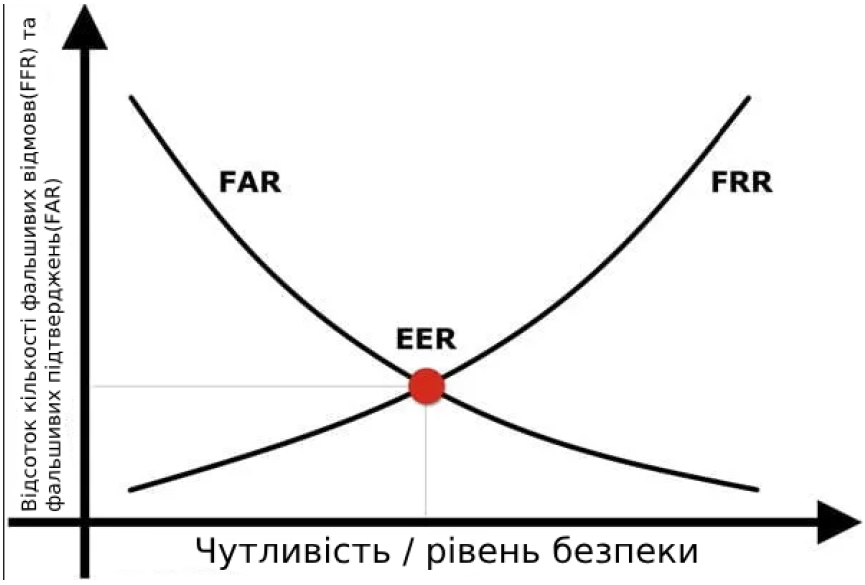

Рисунок 2 – Графік залежності між чутливістю та безпекою в автентифікації [4]

З одного боку, висока чутливість гарантує точне та швидке розпізнавання райдужної оболонки, забезпечуючи користувачеві безперервний та зручний доступ. З іншого боку, важливо розробляти механізми для ефективного контролю та управління доступом, щоб уникнути небажаних вторгнень або несанкціонованого використання біометричних даних.

Для порівняння майбутньої автентифікації, варто порівняти Optic та Touch ID. Touch ID має деякі переваги, на відміну від Optic ID. Touch ID використовує сканування відбитків пальців для швидкої та простої біометричної ідентифікації[5]. Основною перевагою Touch ID є те, що він простий у використанні, дозволяючи швидко отримати доступ до пристрою без використання паролю чи PIN-коду.

Крім того, варто відзначити, що Touch ID добре сприймається користувачами завдяки відмінній швидкості та надійності процесу розпізнавання відбитків пальців. Це робить його популярним вибором для автентифікації комп’ютерів і мобільних пристроїв.

Здібність оптичної ідентифікації та розпізнавання райдужної оболонки відрізняє Optic ID. Це підвищує адаптивність і дозволяє працювати в різних умовах освітлення.

Висновки

У досліджені було порівняно технології авторизації Touch ID та Optic ID. Обидві технології мають на меті допомогти ідентифікувати особистість, проте їх способи реалізації кардинально відрізняються один від одного.

Середовище Optic ID є новітнім різновидом розпізнавання особистості, яка застосовується лише у Apple Vision Pro, на відмінну від Touch ID. Ця автентифікація дозволяє підтвердити особистість, безпосередньо не контактуючи з пристроєм завдяки райдужній оболонці. Через унікальність та новітність даної технології ще невідомо більшість вразливостей та дефектів.

Аутентифікація Touch ID є більш перевіреною та поширеною технологією серед користувачів. Це середовище інтегроване у різних операційних системах, таких як: Android, iOS, MacOS, Windows. Через простоту та розповсюдженість, відомо багато поширених вразливостей та недоліків, проте важливо зазначити, що інші методи аутентифікації, такі як розпізнавання обличчя або коди доступу, також мають свої власні переваги та недоліки.

Наприклад, розпізнавання обличчя може бути зручним, але воно може стати менш ефективним у певних умовах освітлення або при зміні зовнішнього вигляду користувача. Коди доступу можуть бути надійними, але їх легше вкрасти чи вгадати. Тож вибір методу аутентифікації повинен бути зроблений з урахуванням конкретних потреб і загроз безпеці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Apple, about Optic ID [Електронний ресурс]. Режим доступу до ресурсу: https://support.apple.com/en-us/118483 (дата звернення 14.04.2024)
2. E. Perez-Cabre; B. Javidi, scale and rotation Invariant optical ID tags for automatic vehicle identification and authentication [Електронний ресурс]. Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/1492682 (дата звернення 1.05.2024).
3. National Laboratory of Pattern Recognition (NLPR), зображення з CASIAv3 райдужки ока та зіниці. Iris Image Database [Електронний ресурс]. Режим доступу до ресурсу: http://biometrics.idealtest.org/#/ (дата звернення 16.04.2024)
4. RecogTech, зображення балансу між чутливістю та безпекою. Everything about FAR and FRR [Електронний ресурс]. Режим доступу до ресурсу: https://recogtech.com/en/insights/far-and-frr-security-level-versus-ease-of-use/ (дата звернення 20.04.2024)
5. Apple, використання Touch ID [Електронний ресурс]. Режим доступу до ресурсу: https://support.apple.com/uk-ua/102528 (дата звернення 14.04.2024)

Куцик Богдан Михайлович — студент групи КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: mkkbodya@gmail.com

Kutsyk Bohdan M. — student of group KITS-22b, Faculty of Management and information security, Vinnytsia National Technical University, Vinnytsia, email: mkkbodya@gmail.com

Науковий керівник: ***Шелепало Галина Василівна*** – к. фіз.-мат. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Supervisor: ***Shelepalo Halyna V.***—PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.