

ПРИНЦИПИ ФУНКЦІОНУВАННЯ ТА ПЕРЕВАГИ ТЕХНОЛОГІЇ FACE ID

Матвеев Є.Є.

e-mail: yevhen.matvieiev@nure.ua

Науковий керівник – канд. техн. наук, ст. викл. Кобилін І.О.
Харківський національний університет радіоелектроніки, каф. ІНФ
м. Харків, Україна

In the modern era of rapid digitalization, traditional authentication methods like passwords are losing their effectiveness against sophisticated cyber threats. This paper explores the necessary transition to advanced biometric security systems, specifically focusing on the 3D facial recognition technology known as Face ID. The study analyzes the complex hardware and software mechanisms underlying this technology, including the TrueDepth camera sensors and machine learning algorithms. Furthermore, it provides an objective evaluation of Face ID's reliability, cryptographic strength, and potential privacy vulnerabilities. Finally, the research highlights the current applications of 3D facial authentication across various sectors and predicts its future integration into zero-trust security architectures.

У сучасних умовах стрімкої цифровізації суспільства проблема надійного захисту персональних даних набуває безпрецедентного значення. Традиційні методи автентифікації (паролі, PIN-коди) втрачають ефективність через вразливість до кібератак, фішингу та соціальної інженерії. Це зумовило активний перехід індустрії інформаційної безпеки до біометричних систем захисту. Однією з найбільш передових технологій у цій сфері є система просторового 3D-розпізнавання обличчя – Face ID. Актуальність дослідження зумовлена необхідністю розуміння механізмів роботи цієї технології, об'єктивної оцінки її надійності та прогнозування перспектив подальшого впровадження у різні сфери життєдіяльності.

Face ID кардинально відрізняється від систем двовимірного (2D) розпізнавання обличчя, які легко обдурити за допомогою фотографії. Система базується на складному апаратно-програмному комплексі. Апаратна частина, відома як камера TrueDepth, включає інфрачервону (ІЧ) камеру, ІЧ-випромінювач (Flood Illuminator) та проектор точок (Dot Projector). Процес автентифікації починається з того, що ІЧ-випромінювач визначає наявність обличчя у кадрі навіть у повній темряві. Далі проектор точок проектує понад 30 000 невидимих інфрачервоних точок на обличчя користувача. Інфрачервона камера зчитує цей точковий патерн та формує точну структурну 3D-мапу обличчя. Після цього вступає в дію програмна складова: отримані дані передаються до співпроцесора Secure Enclave, де за допомогою алгоритмів машинного навчання, що обробляються модулем Neural Engine, зліпок порівнюється із зареєстрованим математичним еталоном. Нейромережі дозволяють системі адаптуватися до змін у зовнішності: відрощування бороди, носіння окулярів, головних уборів чи макіяжу.

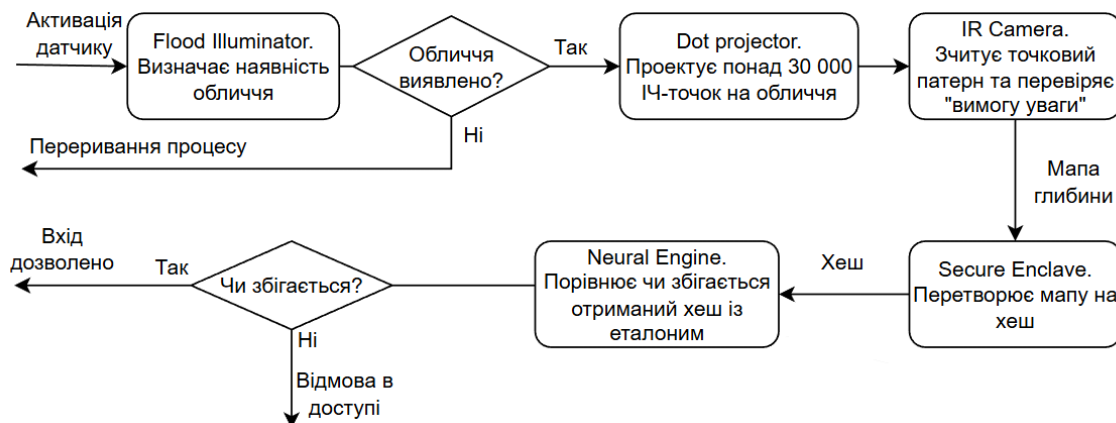


Рисунок 1 – Приклад потоку обробки обличчя Face ID

Головною перевагою Face ID є безпрецедентно високий рівень безпеки серед споживчих біометричних систем. За заявами розробників, імовірність випадкового збігу для Face ID становить 1 до 1 000 000 (порівняно з 1 до 50 000 для дактилоскопічних сканерів Touch ID). Крім того, система використовує функцію "вимоги уваги" (Attention Aware): пристрій розблокується лише тоді, коли користувач дивиться безпосередньо на екран з розплющеними очима. Це унеможливує розблокування пристрою сплячої людини або використання масок високої якості.

Іншою важливою перевагою є ергономічність та швидкість роботи. Безконтактний спосіб автентифікації є гігієнічнішим та зручнішим, особливо в умовах, коли руки користувача зайняті, мокрі або знаходяться в рукавичках, що робить використання сканерів відбитків пальців неможливим.

Таблиця 1 – Переваги FaceID порівняно з іншими методами

Характеристика	Face ID (3D розпізнавання)	Touch ID (Відбиток пальця)	2D розпізнавання обличчя	Пароль / PIN-код
Ймовірність хибного збігу (FAR)	1 до 1 000 000	1 до 50 000	Висока	Залежить від складності
Стійкість до підробки (спуфінгу)	Дуже висока (перевірка об'єму та уваги)	Висока	Низька (обдурюється фотографією)	Вразливий до підглядання
Безконтактність	Так	Ні	Так	Ні
Залежність від умов (рукавички, волога)	Не залежить	Сильно залежить	Не залежить	Не залежить

Технологія має певні обмеження, зокрема труднощі з розрізненням ідентичних близнюків та дітей до 13 років через ще несформовані риси

обличчя. Викликом також стало масове носіння медичних масок під час пандемії, що потребувало компромісних програмних рішень для розпізнавання лише за зоною очей. Крім того, наявність детальних біометричних даних на пристрої викликає постійні дискусії щодо приватності та ризику апаратних вразливостей.

Технологія активно використовується у фінансовому секторі для підтвердження транзакцій (Apple Pay) та безпечного входу в застосунки інтернет-банкінгу, що радикально знижує рівень шахрайства. Також вона масово впроваджується в корпоративні системи контролю та управління доступом (СКУД) на підприємствах, де біометричний ідентифікатор неможливо загубити або передати іншій особі.

Впровадження технології Face ID стало фундаментальним кроком в еволюції систем інформаційної безпеки, досягнувши оптимального балансу між криптографічною стійкістю та зручністю для користувача. У перспективі очікується розвиток систем "безперервної автентифікації" та інтеграція 3D-розпізнавання обличчя з іншими біометричними показниками для створення мультимодальних систем захисту.

Список використаних джерел:

1. Agu, E. (2024). Enhancing mobile biometric authentication: A new model for addressing security vulnerabilities in Face ID technology. *IRE Journals*, 7(9), 355–360. <https://www.irejournals.com/formatedpaper/1705591.pdf>
2. Doe, J. (2024). Are biometrics truly better? *International Journal of Engineering Research & Technology*, 14(5). <https://www.ijert.org/research/are-biometrics-truly-better-IJERTV14IS050252.pdf>
3. Schlett, T., Rathgeb, C., & Busch, C. (2023). *Considerations on the evaluation of biometric quality assessment algorithms*. ResearchGate. https://www.researchgate.net/publication/376025400_Considerations_on_the_Evaluation_of_Biometric_Quality_Assessment_Algorithms