https://doi.org/10.31649/1997-9266-2026-186-3-70-78

УДК 004.93

**В. В. Лукічов**[1]
**Д. О. Підчорний**[1]

# МЕТОД ДИНАМІЧНОЇ ВЕРИФІКАЦІЇ ПІДПИСУ НА ОСНОВІ XGBoost З ВИКОРИСТАННЯМ МІКРОМОТОРНИХ ОЗНАК ТА АДАПТИВНОГО ПОРОГУ ПРИЙНЯТТЯ РІШЕНЬ

[1]Вінницький національний технічний університет

*Актуальність дослідження зумовлена необхідністю створення високонадійних біометричних систем, стійких до спроб несанкціонованого доступу та якісних підробок підпису в умовах глобальної цифровізації бізнес-процесів. Традиційні методи статичної верифікації поступово втрачають ефективність через появу нових інструментів для відтворення графічного накреслення. У зв'язку з цим автором проведено комплексний порівняльний аналіз розробленого авторами ML-рішення з визнаним комерційним галузевим стандартом Wacom Ink SDK for Verification. Основна увага приділена здатності систем відрізнити справжній підпис від кваліфікованої підробки, виконаної зловмисником з візуальним доступом до оригіналу.*

*Експериментальне дослідження проведено з використанням професійного графічного планшета Wacom STU-540, що забезпечує високу частоту дискретизації (200 Гц) та 1024 рівні чутливості до тиску. Вибір такого обладнання дозволив зібрати деталізовані часові ряди, що включають координати пера (x, y), кути нахилу та азимут, а також динаміку зміни зусилля натискання. На основі аналізу реальних даних від шести користувачів, які надали як еталонні зразки, так і імітаційні спроби підробки, виконано багатокритеріальну оптимізацію порогу прийняття рішення. Встановлено, що з адаптивним значенням порогу розроблена система демонструє збалансовані показники ефективності: FAR (коефіцієнт помилкового допуску зловмисника) на рівні 1,33 % та FRR (коефіцієнт помилкового відхилення легітимного користувача) — 6,67 %.*

*Наукова новизна роботи полягає в обґрунтуванні та селекції набору найінформативніших динамічних параметрів для моделі градієнтного бустингу XGBoost. На відміну від стандартних підходів, запропонована модель враховує не лише геометрію підпису, а й похідні характеристики: миттєву швидкість, прискорення та швидкість зміни тиску (jittering). Використання механізму регуляризації в XGBoost дозволило уникнути перенавчання на малих вибірках, що характерно для біометричних даних одного користувача. Це дозволило досягти точності, яка є конкурентоспроможною відносно закритих комерційних алгоритмів (рівень рівної помилки EER ~4 %).*

*Особливості програмної реалізації включають етап попередньої обробки даних, де застосовується інтерполяція для вирівнювання часових кроків та нормалізація ознак для приведення їх до єдиного масштабу. Це критично важливо для стабільної роботи моделі XGBoost, оскільки мікромоторика руки кожного користувача має унікальні амплітудні характеристики. Розроблений конвеєр обробки дозволяє проводити верифікацію в режимі реального часу, витрачаючи менше 100 мс на один запит, що робить систему придатною для використання в умовах високої інтенсивності документообігу.*

*Практичне значення отриманих результатів полягає у можливості інтеграції запропонованого підходу в корпоративні системи електронного документообігу та автоматизовані системи ідентифікації персоналу (наприклад, для верифікації водіїв або фінансових менеджерів). Головною перевагою є відсутність залежності від дороговартісного пропрієтарного програмного забезпечення та ліцензійних обмежень, зі збереженням високого рівня безпеки.*

*Результати порівняння підтвердили, що використання градієнтного бустингу з урахуванням глибоких параметрів мікромоторики дозволяє ефективно виявляти зловмисників навіть у разі спроб ретельного копіювання візуального стилю підпису.*

**Ключові слова:** кібербезпека, загроза, біометрична ідентифікація, біометрична автентифікація, машинне навчання, системи контролю доступу, моделювання, штучний інтелект.

## Вступ

В умовах масштабної цифровізації корпоративного сектору та переходу до електронного документообігу, питання надійної верифікації співробітників набуває критичного значення. Традиційні методи автентифікації, такі як паролі або цифрові ключі, не можуть повною мірою гарантувати, що дію виконує саме авторизована особа, а не зловмисник, що заволодів її даними. Динамічна верифікація підпису, яка базується на аналізі унікальної мікромоторики руки (тиск, швидкість, нахил), є одним з найперспективніших методів біометричного контролю доступу.

Сьогодні ринок пропонує готові комерційні рішення, як Wacom Ink SDK for Verification, що демонструють високу точність, проте мають закритий вихідний код та високу вартість ліцензування. Як зазначають дослідники, використання ансамблевих методів машинного навчання, зокрема алгоритму градієнтного бустингу (XGBoost), дозволяє створювати гнучкі системи з високою роздільною здатністю, що не поступаються комерційним аналогам [1].

Незважаючи на ефективність пропрієтарних алгоритмів, для багатьох підприємств критично важливим є використання відкритих та адаптивних рішень, які дозволяють самостійно налаштовувати параметри безпеки відповідно до внутрішніх вимог організації. Важливим аспектом є пошук балансу між показниками помилкового допуску (FAR) та помилкового відхилення легітимного персоналу (FRR) [2].

*Метою роботи* є проведення порівняльного аналізу ефективності моделі на основі XGBoost та комерційного SDK від Wacom під час роботи з даними графічного планшета Wacom STU-540 для оптимізації процесів ідентифікації персоналу.

### Аналіз останніх досліджень і публікацій

Сучасний стан технологій біометричної верифікації підпису характеризується переходом від аналізу статичних зображень до дослідження динамічних параметрів мікромоторики. Як зазначається у технологічних специфікаціях Wacom SDK, системи автентифікації поділяються на два типи: статичні та динамічні. Статичні методи, що аналізують геометрію штриха, поступово втрачають актуальність через вразливість до візуального копіювання. Натомість динамічна верифікація, яка базується на аналізі швидкості, прискорення та сили натиску стилуса, забезпечує значно вищий рівень захисту від професійних підробок [3].

У наукових працях останніх років (2019—2024 рр.) виокремлюються декілька ключових напрямків розвитку інтелектуальних систем верифікації.

*Алгоритми порівняння часових послідовностей* (DTW). Класичний метод *Dynamic Time Warping* дозволяє порівнювати підписи різної тривалості, проте він критично чутливий до локальних аномалій та пауз. Вдосконалені підходи, зокрема алгоритм *Lost Box Recovery*, пропонують вирішення проблеми розривів у даних шляхом інтелектуального відновлення логічного зв'язку між сегментами підпису [4]. Це особливо важливо для стабільної роботи сенсорів у реальних умовах медичних оглядів чи офісного документообігу.

*Глибоке навчання та Сіамські нейронні мережі*. Дослідження Р. Толосани підтверджують перевагу архітектур на базі *LSTM (Long Short-Term Memory)* та сіамських мереж, які здатні обчислювати метрику схожості між еталоном та зразком без необхідності тривалого донавчання для кожного нового користувача [5]. Гібридні моделі *CNN-BiLSTM,* описані у роботах 2024 року, дозволяють одночасно враховувати і просторові (геометрію), і динамічні (кінематику) ознаки, досягаючи точності понад 99% [6].

*Механізми уваги та Трансформери*. Використання *Vision Transformers (ViT)* та моделей *CoAtNet* відкрило можливості для аналізу глобальних взаємозв'язків між штрихами за допомогою механізму *Multi-Head Attention* [7]. Хоча ці методи демонструють найвищу точність у розпізнаванні складних імітацій, їх впровадження обмежене високою обчислювальною складністю.

Більшість сучасних нейромережевих архітектур (CNN, ViT) орієнтовані на роботу з потужними графічними процесорами (GPU). В умовах пунктів контролю персоналу та медичних закладів, де використовуються стандартні офісні станції, застосування таких «важких» моделей призводить до затримок, що знижує пропускну здатність системи.

Це зумовлює необхідність пошуку альтернативних методів, які забезпечують баланс між точністю нейромереж та обчислювальною легкістю. Саме тому в цій роботі пропонується використання алгоритму градієнтного бустингу XGBoost, який дозволяє ефективно обробляти структуровані

біометричні дані з мінімальними вимогами до апаратного забезпечення, зберігаючи при цьому рівень безпеки, порівнюваний із комерційними SDK.

### Запропонований метод автентифікації на основі XGBoost

Для розробки засобу автентифікації працівників вибрано алгоритм машинного навчання XGBoost (Extreme Gradient Boosting), який базується на принципі градієнтного бустингу [8]. Вибір цієї моделі зумовлений її високою ефективністю у роботі зі структурованими даними, які можна представити у вигляді векторів ознак. На відміну від нейронних мереж, XGBoost демонструє кращі результати на малих наборах даних, що є критично важливим в умовах «холодного старту», коли для нового водія в базі наявні лише 5...10 еталонних підписів. До того ж алгоритм є менш вимогливим до апаратного забезпечення, що дозволяє виконувати обчислення безпосередньо на центральному процесорі (CPU) офісної станції без потреби у потужних графічних прискорювачах.


Рис. 1. Вигляд планшета Wacom STU-540

Основним джерелом даних для моделі є параметри, що надходять від планшета Wacom STU-540 через спеціалізований мікроконтролер (рис. 1). До вектора ознак включаються просторові координати кінчика стилуса ($x$, $y$), рівень тиску ($p$), який має 1024 рівні чутливості, та часові мітки ($t$) з частотою опитування 200 Гц [3]. Унікальною особливістю методу є інтеграція «повітряних штрихів» (In-air), які фіксують траєкторію стилуса на відстані до 15 мм над екраном. Ці дані відображають приховану моторику водія, яку неможливо підробити візуально, оскільки ці штрихи не відображаються на моніторі пристрою.

Принцип роботи запропонованого алгоритму полягає в ітераційній побудові ансамблю «слабких» дерев рішень, що у сукупності формують точну модель. Процес починається з першого дерева (D_1), яке робить грубе припущення щодо справжності підпису, після чого вираховується математична похибка — «залишок» (рис. 2).

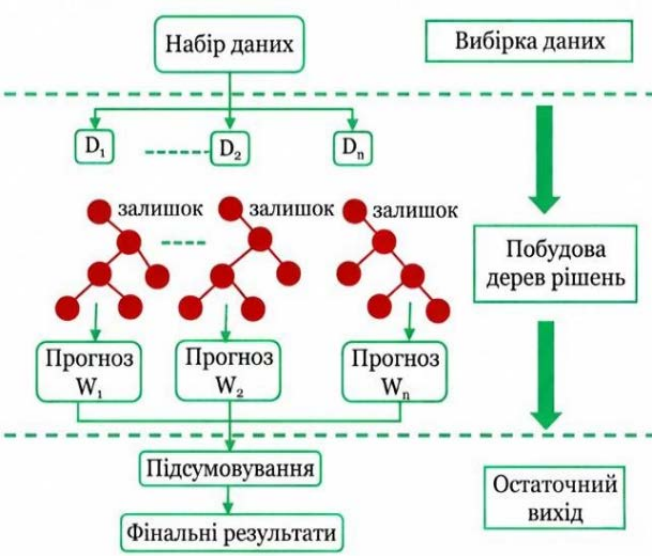



Рис. 2. Принцип роботи алгоритму градієнтного бустингу

Кожне наступне дерево D_2, ..., D_$n$ вчиться виправляти саме ці похибки, аналізуючи все дрібніші деталі: мікро-тремор руки, стабільність сили натискання в певних зонах або ритм рухів. На фінальному етапі результати всіх дерев підсумовуються, і система видає ймовірність того, що підпис належить конкретному працівнику. Такий підхід пропонується доповнити алгоритмом адаптивного порогу, який замінює жорстку логіку оцінювання. Система автоматично аналізує «стабільні зони» та «зони шуму» в підписі конкретного працівника.

Якщо водій зазвичай підписується недбало, математичний допуск у цих місцях розширюється, а в стабільних частинах траєкторії — посилюється. Це дозволяє системі відрізняти навмисну спробу підробки від природної варіативності почерку, викликаної втомою чи стресом, що забезпечує оптимальний баланс між безпекою та зручністю використання.

Основні переваги використання XGBoost :

– алгоритм оптимізований для роботи на стандартних центральних процесорах, що забезпечує низькі апаратні вимоги та виключає необхідність дорогого оновлення комп’ютерної техніки в медичних пунктах;

– модель демонструє високу ефективність на малих даних, показуючи високу точність вже за

наявності 5...10 еталонних зразків підпису, що ефективно вирішує проблему «холодного старту» для нових працівників. Підтвердженням цього є порівняльний аналіз метрик точності (рис. 4), де XGBoost випереджає нейронні мережі саме на вибірках малого розміру, зберігаючи при цьому стабільність результатів [9];

– завдяки аналізу невидимих рухів In-air досягається висока стійкість до підробок, оскільки система блокує зловмисників, які імітують лише візуальну форму підпису;

– використання динамічного порогу забезпечує адаптивність до стану суб'єкта, дозволяючи суттєво знизити кількість помилкових відмов для реальних водіїв з урахуванням їхнього психофізіологічного стану;

– ансамбль дерев рішень гарантує високу швидкість обробки та миттєву перевірку з мінімальною затримкою, що є критично важливим для пунктів із великим потоком людей;

– на відміну від «чорної скриньки» нейромереж, структура дерев забезпечує прозорість прийняття рішень, дозволяючи чітко визначити, на основі яких саме ознак, як-от швидкість, тиск чи координати, підтверджено або відхилено підпис.

Для забезпечення високої роздільної здатності моделі розроблено систему з 18 ознак, що охоплюють чотири ключові аспекти підпису: геометричну структуру, динаміку руху, розподіл тиску та часові характеристики [10]. До геометричного блоку включено параметри площі охоплюючого прямокутника, загальну довжину траєкторії та компактність підпису. Динамічні властивості описуються через середню швидкість, прискорення та кутову складність, яка обчислюється як сума поворотів стилуса відносно часової осі, аналіз тиску: крім середнього значення та стандартного відхилення, розраховується відношення тиску до швидкості (pressure-velocity ratio), що дозволяє ідентифікувати унікальні зусилля під час виконання складних елементів почерку. Просторова щільність підпису оцінюється через заповненість квадрантів та статистику напрямків руху стилуса (співвідношення підйомів і зміщень).

### Алгоритм навчання моделі XGBoost

Процес навчання розробленої системи базувався на використанні комбінованого датасету, що дозволило моделі ефективно розрізняти як грубі, так і майстерні спроби імітації. Навчальна вибірка включала дані від десяти різних користувачів: для першої групи з п'яти осіб зібрано по 20 оригінальних зразків та 20 цілеспрямованих підробок, що дозволило алгоритму вивчити межі варіативності конкретного почерку. Для другої групи з п'яти користувачів використано по 10 реальних оригінальних підписів, отриманих за допомогою пристроїв Wacom. Процедура тренування ітераційно оптимізувала ансамбль дерев рішень, мінімізуючи функцію логістичних втрат (logloss). Завдяки використанню алгоритму XGBoost, модель пройшла 600 циклів навчання з низьким коефіцієнтом швидкості (learning_rate=0.01), що забезпечило глибоке вивчення мікромоторики без ризику перенавчання. Процес ініціалізації моделі з оптимальними параметрами виглядає так:

```
model = xgb.XGBClassifier(
    n_estimators=600,
    max_depth=3,
    learning_rate=0.01,
    colsample_bytree=0.25,
    subsample=0.8,
    reg_alpha=8,
    reg_lambda=8,
    scale_pos_weight=len(neg_data) / len(pos_data),
    eval_metric='logloss',
    random_state=42)
```

Вибір саме такої конфігурації зумовлений необхідністю «змусити» модель звертати увагу на дрібні деталі мікромоторики. Обмеження кількості ознак для кожного окремого дерева (colsample_bytree=0.25) гарантує, що алгоритм буде будувати рішення на основі різних комбінацій параметрів тиску, швидкості та повітряних штрихів, а не фокусуватися на одній випадковій ознаці.

Результатом тренування є персоналізований файл у форматі JSON, який є компактним «цифровим зліпком» індивідуальної манери підпису. У цій структурі зафіксовано ієрархію дерев рішень, ваги кожної з 18 ознак та оптимізовану межу прийняття рішення. У цій структурі зафіксовано ієрархію дерев рішень, математичні ваги кожної з 18 ознак та оптимізовану межу прийняття рішення. На відміну від методів глибокого навчання, використання XGBoost дозволяє чітко інтерпрету-

вати логіку роботи системи, визначивши внесок кожного біометричного параметра у фінальний результат. Для оцінки адекватності моделі проведено розрахунок важливості ознак (Feature Importance) за показником Gain (внесок у приріст точності). Результати аналізу для цільового профілю користувача подані у табл. 1.

Таблиця 1

**Розподіл важливості біометричних ознак у навченій моделі**

| № | Назва ознаки (Feature) | Опис параметра | Важливість, % |
|---|---|---|---|
| 1 | mean_pressure | середній тиск стилуса на поверхню | 15,22 |
| 2 | rel_center_x | відносна позиція центру підпису по горизонталі | 11,07 |
| 3 | q1_density | щільність точок у верхньому лівому квадранті | 10,87 |
| 4 | mean_velocity | середня швидкість руху стилуса | 9,14 |
| 5 | complexity_score | кутова складність (ритмічність поворотів) | 7,96 |
| 6 | aspect_ratio | співвідношення ширини до висоти підпису | 5,97 |
| 7 | total_time | загальна тривалість процесу підписання | 5,78 |
| 8 | pressure_std | варіативність сили натиску (стандартне відхилення) | 5,07 |
| 9 | velocity_std | стабільність швидкості (варіативність темпу) | 4,75 |
| 10 | pressure_diff | диференціал зміни тиску між точками | 4,32 |
| 11 | p_v_ratio | співвідношення тиску до швидкості (P/V) | 4,11 |
| 12 | bbox_area | площа прямокутника, що описує підпис | 3,48 |
| 13 | up_moves_ratio | частка рухів стилуса вгору | 2,85 |
| 14 | total_dist | загальна довжина траєкторії підпису | 2,57 |
| 15 | compactness | компактність (відношення шляху до діагоналі) | 2,46 |
| 16 | right_moves_ratio | частка рухів стилуса праворуч | 2,33 |
| 17 | q4_density | щільність точок у нижньому правому квадранті | 2,05 |
| 18 | integrity | цілісність (наявність даних у початковій/фінальній фазах) | 0,00 |

Зауважимо, що поданий у табл. 1 розподіл важливості ознак є індивідуальним для конкретного користувача. В цьому й полягає ключова особливість запропонованого алгоритму: для одного працівника вирішальним фактором може бути ритм зміни швидкості, тоді як для іншого — унікальна динаміка тиску або просторове розташування штрихів.

### Алгоритм розрахунку адаптивного порогу прийняття рішень

Для забезпечення математичної точності адаптивної моделі система проводить детальний статистичний аналіз результатів розпізнавання еталонної вибірки. На основі масиву ймовірностей $P(s_i)$, отриманих від моделі XGBoost для кожного з $n$ еталонних підписів, обчислюється середнє значення μ, яке визначає математичне очікування впевненості системи для конкретного користувача

$$\mu = \frac{1}{n} \sum_{(i=1)}^{n} P(s_i), \tag{1}$$

де μ — математичне очікування (середнє арифметичне) впевненості моделі; $n$ — загальна кількість еталонних підписів у вибірці; $p_i$ — ймовірність автентичності, отримана від моделі XGBoost для $i$-го зразка.

Цей показник є базовим рівнем автентичності, на який орієнтується алгоритм у подальшій перевірці нових зразків. Паралельно з цим проводиться розрахунок середньоквадратичного відхилення (σ), яке дозволяє оцінити ступінь розсіювання значень навколо середнього арифметичного

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^{n} \left( P(s_i) - \mu \right)^2}, \tag{2}$$

де σ — середньоквадратичне відхилення (сигма), що визначає розсіювання даних; $p_i$ — значення ймовірності для конкретного $i$-го зразка; μ — розраховане раніше середнє значення впевненості; $n$ — кількість зразків у вибірці.

Розраховане значення σ виступає кількісною мірою індивідуальної варіативності почерку. Чим меншим є це відхилення, тим стабільнішою вважається моторика користувача, що дозволяє системі встановити суворіші межі для вхідного контролю. Отримані значення μ та σ безпосередньо використовуються для формування індивідуального адаптивного порогу верифікації визначається за правилом «трьох сигм», що дозволяє створити індивідуальний коридор допуску для кожного суб'єкта

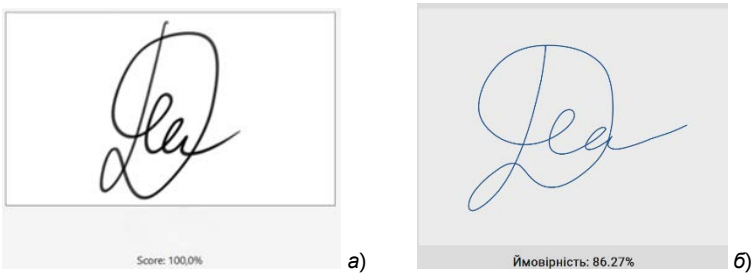
$$T_{adapt} = \mu - (3 \cdot \sigma), \tag{3}$$

де $T_{adapt}$ — підсумковий індивідуальний поріг верифікації; μ — базовий рівень впевненості користувача; σ — показник індивідуальної варіативності (стабільності) підпису; 3 — коефіцієнт суворості згідно з правилом «трьох сигм».

Фінальний результат розрахунку проходить через програмний фільтр, що обмежує значення $T_{adapt}$ у діапазоні [0,70; 0,95]. Це запобігає критичному зниженню рівня безпеки у випадках аномально високої варіативності еталонів та забезпечує стабільну роботу системи в реальних умовах експлуатації.

### Порівняльний аналіз ефективності та тестування алгоритму

Завершальним етапом дослідження стало проведення порівняльного аналізу розробленої моделі на основі XGBoost з комерційним галузевим стандартом — Wacom Ink SDK for Verification. Для наочної демонстрації відмінностей у роботі проведено серію тестів. Під час експерименту підпис (спочатку оригінальний, а потім — якісна імітація) одночасно аналізувався обома системами. У першому тесті власник підпису виконав свій еталонний автограф. На рис. 3 продемонстровано результати аналізу.



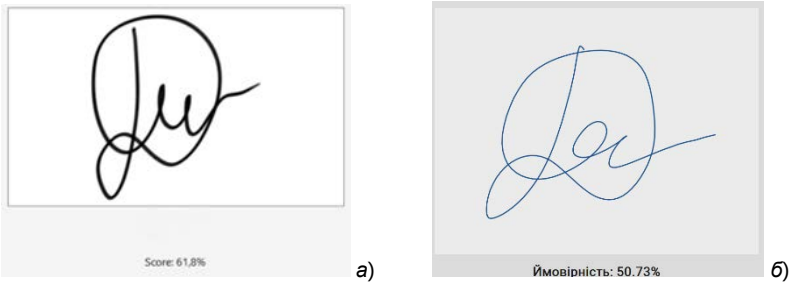

*а*) *б*)

Рис. 3. Результати верифікації оригінального підпису:
*а* — Wacom Ink SDK (оцінка схожості: 100,0 %); *б* — розроблений XGBoost (ймовірність: 86,27 %)

Як випливає з рис. 3, *Wacom Ink SDK* (рис. 3*а*) видає максимальну оцінку схожості— 100,0 %, що є логічним для оригінального підпису. Проте, комерційний алгоритм зазвичай орієнтований на універсальність, тому його оцінка часто базується на «глобальніших» геометричних ознаках.

Розроблений алгоритм *XGBoost* (рис. 3*б*) оцінив цей же підпис у 86,27 %. Такий результат, що є нижчим за максимальний, зумовлений жорсткішою конфігурацією моделі, яка враховує не лише форму, а й мікромоторику, варіативність тиску та повітряні переходи. Оскільки встановлений поріг прийняття рішення в системі для певного користувача становить 0,832 (або 83,2 %), цей підпис успішно проходить верифікацію як оригінальний, але з меншим «запасом», ніж у Wacom.

Для другого тесту залучено іншу особу, яка намагалася візуально скопіювати форму підпису власника. Зловмисник мав можливість бачити оригінал, тому геометрія підробки була дуже схожою. Результати цього тесту показані на рис. 4.




*а*) *б*)

Рис. 4. Результати верифікації підробленого підпису:
*а* — Wacom Ink SDK (оцінка схожості: 61,0 %); *б* — розроблений XGBoost (ймовірність: 50,73 %)

За результатами проведених випробувань обидві системи — як комерційний засіб Wacom Ink SDK, так і розроблений алгоритм на основі XGBoost — продемонстрували високу ефективність та успішно ідентифікували підроблені зразки. У кожному з тестових випадків системи видали вердикт про відхилення верифікації, що підтверджує надійність обох підходів у виявленні спроб імітації.

Різниця в отриманих числових показниках (61,8 % та 50,73 %) зумовлена специфікою внутрішньої математичної логіки алгоритмів, а також різницею самих підроблених підписів, проте кінцевий результат був ідентичним: доступ для зловмисника заблоковано.

Для об'єктивного оцінювання ефективності розробленого методу проведено серію випробувань, що базуються на стандартних критеріях аналізу точності біометричних систем. Основними метриками, що використовуються у світовій практиці для визначення якості розпізнавання, є коефіцієнт помилкового допуску (FAR) та коефіцієнт помилкового відхилення (FRR). Процес оцінювання полягав у проведенні масової перехресної валідації, де кожна навчена модель почергово проходила через масив оригінальних підписів інших осіб для симуляції спроб несанкціонованого доступу, а також через контрольні зразки реальних власників, що не брали участі у навчанні.

Результати проведеного тестування продемонстрували високу здатність алгоритму до диференціації біометричних ознак. За встановленого порогу прийняття рішення система показала стабільне розмежування між ймовірністю для легітимного користувача та сторонніх осіб. Підсумкові показники, отримані в ході глобальної валідації, подано у табл. 2.

Таблиця 2

**Стандартні показники точності біометричної системи**

| Назва метрики | Результат випробувань, % | Кількість випадків |
|---|---|---|
| FAR (False Acceptance Rate) | 1,33 | 4 помилкові допуски на 300 спроб |
| FRR (False Rejection Rate) | 6,67 | 4 помилкові відхилення на 60 спроб |

Зокрема у більшості випадків ймовірність підтвердження для власника значно перевищувала встановлений ліміт, тоді як спроби доступу за допомогою випадкових підписів інших людей оцінювалися моделлю як малоймовірні, що підтверджує ефективність індивідуального налаштування ваг ознак.

Проведене оцінювання за загальноприйнятими критеріями підтверджує високу роздільну здатність розробленого підходу. Отриманий показник FAR на рівні 1,33 % вказує на надійний захист від несанкціонованого входу, а рівень FRR у 6,67 % є допустимим для систем динамічної верифікації, що працюють у реальному часі.

## Висновки

Проведене дослідження підтвердило доцільність використання алгоритму градієнтного бустингу XGBoost для задач динамічної верифікації підпису в системах ідентифікації персоналу. На відміну від комерційних рішень, запропонований підхід забезпечує прозорість прийняття рішень через аналіз вагомості біометричних ознак, що дозволяє адаптувати систему під індивідуальну моторику кожного працівника.

Встановлено, що інтеграція 18 параметрів, зокрема координати, швидкість та динаміку тиску стилуса, дозволяє моделі виявляти складні закономірності почерку, які неможливо відтворити у разі візуального копіювання форми підпису. Особливу роль у забезпеченні стійкості до підробок відіграє аналіз «повітряних штрихів» та варіативності натиску, що становлять понад 15 % загальної ваги у структурі навченого ансамблю дерев рішень.

Результати тестування на базі 360 верифікаційних спроб продемонстрували показник FAR на рівні 1,33 % та FRR — 6,67 % з адаптивним порогом прийняття рішення. Ці значення відповідають галузевим стандартам біометричного захисту і свідчать про високу роздільну здатність алгоритму.

Практична значущість роботи полягає у можливості розгортання надійної системи біометричної верифікації на наявній IT-інфраструктурі підприємств без залучення спеціалізованих обчислювальних потужностей (GPU). Використання компактних моделей у форматі JSON забезпечує миттєву перевірку особи в режимі реального часу, що є критично важливим для пунктів контролю з високою інтенсивністю руху персоналу. Перспективним напрямом подальших досліджень є впровадження механізмів адаптивного порогу для автоматичного коригування чутливості системи залежно від стабільності почерку конкретного суб'єкта.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] T. Chen, and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785-794, 2016. https://doi.org/10.1145/2939672.2939785 .

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, no. 1, pp. 4-20, 2004. https://doi.org/10.1109/TCSVT.2003.818349 .

[3] "Signature Verification SDK Documentation," Wacom Technology Corporation. [Electronic resource]. Available: https://developer-docs.wacom.com/ . Accessed: 13.04.2026.

[4] Jaini, et al., "Improved Dynamic Time Warping for Online Signature Verification," *arXiv preprint arXiv:1904.00786*, 2019. https://doi.org/10.48550/arXiv.1904.00786 .

[5] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "DeepSign: Deep On-Line Signature Verification," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, no. 2, pp. 229-239, 2021. https://doi.org/10.1109/TBIOM.2021.3053996 .

[6] A. Rahim, et al., "An Enhanced Hybrid Model Based on CNN and BiLSTM for Identifying Individuals via Handwriting Analysis," *Multimedia Tools and Applications*, 2024. https://doi.org/10.1007/978-3-031-49529-8_23 .

[7] "Attention-Driven CNN-LSTM Hybrid Models for Secure Dynamic Signature Verification," in *2024 IEEE Conference Proceedings*, pp. 1-6, 2024. https://doi.org/10.1109/ICAC360840.2024.10609324 .

[8] "Довідник по Machine Learning – XgBoost," База знань IT технологій. [Електронний ресурс]. Режим доступу: https://itwiki.dev/data-science/ml-reference/ml-glossary/xgboost . Дата звернення 13.04.2026.

[9] "XGBoost Vs Neural Networks: Which Is Best for Your Project?" AICompetence.org. [Electronic resource]. Available: https://aicompetence.org/xgboost-vs-neural-networks/ . Accessed: 13.04.2026.

[10] J. Fierrez-Aguilar, et al., "An On-line Signature Verification System Based on Fusion of Local and Global Information," in *International Conference on Biometric Authentication*, Springer, pp. 523-529, 2004. https://doi.org/10.1007/978-3-540-25948-0_71 .

Рекомендована кафедрою захисту інформації ВНТУ

Дата надходження 24.04.2026
Дата прийняття до друку після рецензування 29.04.2026
Дата публікації 7.07.2026



***Лукічов Віталій Володимирович*** — канд. техн. наук, доцент кафедри захисту інформації, e-mail: lukichov.vitalyi@vntu.edu.ua , https://orcid.org/0000-0002-3423-5436 ;

***Підчорний Данило Олександрович*** — студент факультету інформаційних технологій та комп'ютерної інженерії, e-mail: danyadenpod@gmail.com , https://orcid.org/0009-0008-8348-4106 .

Вінницький національний технічний університет, Вінниця

**V. V. Lukichov**[1]
**D. O. Pidchorniy**[1]

# Dynamic Signature Verification Method Based on XGBoost Using Micromotor Features and Adaptive Decision-Making Threshold

[1]Vinnytsia National Technical University

*The relevance of the study is driven by the need to create highly reliable biometric systems resistant to unauthorized access and high-quality signature forgeries in the context of global business process digitalization. Traditional static verification methods are gradually losing effectiveness due to the emergence of new tools for reproducing graphical patterns. In this regard, the author conducted a comprehensive comparative analysis of a custom-developed ML solution against the recognized commercial industry standard — Wacom Ink SDK for Verification. The primary focus is placed on the systems' ability to differentiate a genuine signature from a skilled forgery performed by an attacker with visual access to the original.*

*The experimental study was conducted using a professional Wacom STU-540 signature pad, which provides a high sampling rate (200 Hz) and 1024 levels of pressure sensitivity. The choice of such hardware enabled the collection of detailed time series, including pen coordinates (x, y), tilt angles, azimuth, and the dynamics of pressure changes. Based on the analysis of real-world data from six users, who provided both reference samples and imitation forgery attempts, a multi-criteria optimization of the decision-making threshold was performed. It was established that at an adaptive threshold value, the developed system demonstrates balanced performance metrics: a False Acceptance Rate (FAR) of 1.33 % and a False Rejection Rate (FRR) of 6.67 %.*

*The scientific novelty of the work lies in the substantiation and selection of a set of the most informative dynamic parameters for the XGBoost gradient boosting model. Unlike standard approaches, the proposed model considers not only the signature geometry but also derivative characteristics: instantaneous velocity, acceleration, and pressure change rate (jittering). The use of the regularization mechanism in XGBoost prevented overfitting on small datasets, which is typical for single-user biometric data. This allowed for achieving an accuracy level competitive with closed-source commercial algorithms (Equal Error Rate EER ~4 %).*

*Features of the software implementation include a data preprocessing stage where interpolation is applied to align time steps and feature normalization is used to bring them to a single scale. This is critical for the stable operation of the XGBoost model, as each user's hand micromotors possess unique amplitude characteristics. The developed processing pipeline enables real-time verification, spending less than 100 ms per request, making the system suitable for high-intensity document management environments.*

*The practical significance of the results lies in the possibility of integrating the proposed approach into corporate electronic document management systems and automated personnel identification systems (e.g., for verifying drivers or financial managers). The main advantage is the lack of dependence on expensive proprietary software and licensing restrictions while maintaining a high level of security.*

*The comparison results confirmed that the use of gradient boosting, taking into account deep micromotor parameters, effectively detects intruders even during attempts of meticulous visual style copying.*

**Keywords:** cybersecurity, threat, biometric identification, biometric authentication, machine learning, access control systems, modeling, artificial intelligence.

***Lukichov Vitalii V.*** — Cand. Sc. (Eng), Associate Professor of the Department of Information Security, e-mail: lukichov.vitalyi@vntu.edu.ua . https://orcid.org/0000-0002-3423-5436;

***Pidchornyi Danylo O.*** — Student of the Department of Information Technology and Computer Engineering, e-mail: danyadenpod@gmail.com . https://orcid.org/0009-0008-8348-4106