

РЕЦЕНЗІЯ

на дисертаційну роботу

Гаврилович Марії Павлівни

на тему «Верифікація користувача методами глибокого навчання на основі поведінкових та біометричних характеристик»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 122 Комп'ютерні науки

Актуальність теми дисертації.

Верифікація користувача методами глибокого навчання на основі поведінкових та біометричних характеристик стає дедалі актуальнішою в умовах зростаючої кількості кібератак та необхідності забезпечення надійного захисту особистих даних. Традиційні методи автентифікації, такі як паролі та PIN-коди, часто виявляються вразливими до злому та фішингу. Використання біометричних характеристик, таких як відбитки пальців, обличчя або голос, у поєднанні з аналізом поведінкових моделей користувача забезпечує більш високий рівень безпеки, оскільки ці характеристики є унікальними для кожної особи і їх важко підробити.

Інтеграція глибокого навчання в процес верифікації користувачів дозволяє значно підвищити точність та швидкість автентифікації. Глибокі нейронні мережі здатні обробляти великі обсяги даних та виявляти складні патерни, які можуть бути непомітними для традиційних алгоритмів. Завдяки цьому можна розпізнавати користувачів з високою точністю навіть у випадках зміни їх поведінки або зовнішнього вигляду. Це особливо важливо в умовах динамічного оточення, де користувачі можуть взаємодіяти з системами в різних умовах та контекстах. Також, біометрична верифікація може ефективно боротися з діпфейками, використовуючи свої унікальні можливості для розпізнавання справжніх фізичних та поведінкових характеристик користувачів. Системи біометричної верифікації, які використовують глибокі нейронні мережі, здатні аналізувати такі тонкі деталі, як мікро-рухи обличчя, зміни в голосових паттернах або інші динамічні ознаки, які важко підробити навіть за допомогою діпфейків. Ці системи можуть виявляти аномалії або невідповідності, що дозволяє їм розпізнавати підроблені відео та аудіо.

Крім того, використання поведінкових та біометричних характеристик для верифікації сприяє покращенню користувацького досвіду. Замість необхідності вводити складні паролі або відповідати на безліч запитань, користувачі можуть проходити автентифікацію безперервно та без перепон під час своєї взаємодії з системою. Це не тільки підвищує зручність, але й знижує ризик помилок, пов'язаних із забутими паролями або неправильними відповідями. Таким чином, верифікація на основі поведінкових та біометричних характеристик з використанням методів глибокого навчання не лише підвищує безпеку, але й робить процес автентифікації більш ефективним та приємним для користувачів.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1. Створення нових гібридних архітектур, які базуються на комбінації стискуючих і варіаційних автокодувальників з трансформерами, дозволило підвищити ефективність систем верифікації, використовуючи поведінкові та біометричні характеристики користувачів, і забезпечити значне поліпшення у порівнянні з існуючими підходами.
2. На базі запропонованих архітектур розроблено систему підтримки прийняття рішень для верифікації користувачів.
3. Введено нову інформаційну ознаку для підвищення точності біометричних систем верифікації через використання фрактальних розмірностей.
4. Визначені та набули подальшого розвитку прикладні сценарії та компоненти системи верифікації на базі уточненої практичної методології побудови систем глибокого навчання на основі запропонованих архітектур.

Адекватність результатів обчислювальних експериментів підтверджена за допомогою коректного застосування методів глибокого навчання та нейронних мереж, використовуючи реальні дані про біометричні і поведінкові характеристики. Незалежність тестувань та вимірювань метрик якості забезпечує високу достовірність отриманих наукових результатів, які базуються на ретельному використанні актуальних наукових джерел і методологій машинного навчання.

Наукові дослідження були виконані здобувачем на кафедрі штучного інтелекту КПІ ім. Ігоря Сікорського в рамках ініціативної теми під керівництвом професора КПІ ім. Ігоря Сікорського, доктора технічних наук, професора Данилова Валерія Яковича.

Отже, в дисертаційній роботі поставлене наукове завдання дослідження та побудови ефективних та точних систем біометричної верифікації користувача на

основі нейронних мереж глибокого навчання виконано повністю, здобувачка повною мірою оволоділа методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Гаврилович М.П. повністю відповідає Стандарту вищої освіти зі спеціальності 122 Комп'ютерні науки та напрямкам досліджень відповідно до освітньої програми Комп'ютерні науки.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям "Комп'ютерні науки".

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Гаврилович Марії Павлівни є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою.

Результати аналізу та досліджень представлені чітко, логічно та зрозуміло. Автор дотримується наукового стилю викладу і використовує сучасну наукову термінологію. Текст дисертації відзначається добре продуманою структурою, яка полегшує розуміння та аналіз досліджуваної проблематики. Це дозволяє зосередитись на ключових моментах роботи та використовуваних наукових джерелах. Завдяки цьому методу викладення, який базується на теоретичних дослідженнях та практичних експериментах, матеріал розкривається глибше, сприяючи подальшому науковому розвитку в обраній області.

Дисертація складається з вступу, 3 розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 126 сторінок.

У вступі детально розглянуто мету і завдання дослідження, а також підкреслено значущість обраної теми дисертації. Обговорено актуальні проблеми сучасних методик, висвітлено інноваційні аспекти дослідження та його практичну цінність. Авторка обґрунтовує свій вклад у наукове дослідження, зазначає апробацію досліджень викладених в матеріалах дисертації.

Перший розділ містить детальний аналіз існуючої літератури, що охоплює архітектури нейронних мереж для біометричної верифікації. Описано їхні недоліки та можливості для розробки нових ефективних рішень у цій сфері. Наводяться переваги та недоліки існуючих методів, та визначаються архітектури нейронних мереж для подальшого дослідження.

У другому розділі розглядається проблема неперервної біометричної верифікації користувача, представлена удосконалена методологія для оптимізації моделей, а також проведено порівняльний аналіз різних типів автокодувальників із класичними методами машинного навчання, такими як однокласові опорні машини векторів та ізоляційний ліс. Представлені також розрахунки та прикладні сценарії, реалізовані за допомогою вдосконаленої методології.

Третій розділ описує систему підтримки прийняття рішень для неперервної верифікації, вводить нову гібридну архітектуру, яка базується на стискуючих автокодувальниках з використанням трансформерів. Ця архітектура демонструє покращені показники часу висновку та помилок для різних фізичних активностей. Також проведено аналіз впливу фрактальної розмірності Хігучі на якість верифікації.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи.

Наукові результати дисертації висвітлені у 4 наукових публікаціях здобувача, серед яких: 1 стаття у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 3 статті у періодичних наукових виданнях, проіндексованих у базах даних Scopus.

Також результати дисертації були апробовані на 2 наукових фахових конференціях.

Публікації здобувачки відзначаються високим науковим рівнем і містять глибокий аналіз основних результатів проведеного дослідження. Важливий особистий вклад здобувачки в співавторські роботи, зокрема у розробці та виконанні експериментальних секцій. У всіх публікаціях дотримано принципів академічної доброчесності.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. В роботі глибоко досліджено вплив різних компонентів та їх комбінацій на загальний результат. Бажано було б розглянути вплив різних компонентів не тільки акселерометра, а також інших типів давачів, як-от магнетометра, гіроскопа, тощо.
2. В другому розділі розроблена практична методологія для вирішення задачі верифікації користувача. Можливо було б доповнити розрахунки більшою кількістю варіацій існуючих параметрів.

3. У першому розділі бажано більш детально порівняти попередні результати отримані іншими авторами для розв'язання задачі верифікації для різних архітектур нейронних мереж та методів глибокого навчання.
4. У роботі зустрічається граматичні та стилістичні неточності.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Гаврилович Марії Павлівни на тему «Верифікація користувача методами глибокого навчання на основі поведінкових та біометричних характеристик» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для інформаційних технологій. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6 – 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувачка Гаврилович Марія Павлівна заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Рецензент:

Професор кафедри математичних
методів системного аналізу
НН ІПСА КПП ім. Ігоря Сікорського
доктор технічних наук, доцент



Олена ЗАЙЧЕНКО



«05» 08 2024 року

