

РЕЦЕНЗІЯ

офіційного рецензента, кандидата технічних наук, доцента кафедри комп'ютеризованих систем та програмних технологій навчально-наукового інституту комп'ютерних систем Національного університету «Одеська політехніка» Григоренко Світлани Миколаївни
на дисертаційну роботу здобувача
Хамітова Віталія Миколайовича
на тему «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів»,
що подана до захисту в разову спеціалізовану вчену раду Національного університету «Одеська політехніка» Міністерства освіти і науки України
на здобуття наукового ступеня доктора філософії
за спеціальністю 122 – Комп'ютерні науки
галузь знань 12 – Інформаційні технології

1. Актуальність обраної теми дисертації

Сучасний стан цифрової економіки характеризується стрімким розвитком передачі інформації, серед якої обмін зображеннями (текстографічними документами, що представляються у вигляді цифрових, табличних даних, рисунків, графіків, діаграм, підписів, віз, резолюцій, які є по суті 2-D масивами даних) займає особливе місце в інформаційних системах різного прикладного призначення. Однією з суттєвих проблем для організації обміну зображеннями є необхідність забезпечення високого рівня конфіденційності, цілісності та безпеки інформації, яка передається. Тому тема дисертаційної роботи, що пов'язана з підвищенням конфіденційності та цілісності обміну зображеннями для групи довірених користувачів в інформаційних системах прикладного призначення, є *актуальною*.

Отже, дисертаційна робота Хамітова Віталія Миколайовича, присвячена удосконаленню методів захисних перетворень на основі хаотичних відображень спрямована на вирішення важливої науково-практичної задачі й є безумовно актуальною.

Дисертаційну роботу виконано у відповідності до пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні (Постанова Кабінету Міністрів України від 30.04.2024 р. № 476), згідно п. 1.2.1.1, 1.2.1.4, 1.2.4.6 і 1.2.1.7 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки» (постанова Президії НАН України від 30.01.2019 р. № 30) та також у відповідності до планів науково-дослідних робіт Національного університету «Одеська політехніка» при виконанні держбюджетної теми: НДР роботи № 719-61/161 – «Інтелектуальна підтримка прийняття рішень при

проєктуванні кісткових замінників для лікування воєнних травм» (номер державної реєстрації 0124U000388). Дисертант приймав участь у виконанні вказаних тем як виконавець.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Аналіз змісту дисертаційної роботи і наукових публікацій Хамітова Віталія Миколайовича дають змогу зробити висновок про те, що основні наукові положення, висновки і рекомендації, які сформульовано в дисертаційній роботі, відповідають темі досліджень, їх вірогідність забезпечено коректністю визначення об'єкту та предмету дослідження, які узгоджено з метою і задачами наукового дослідження.

Достовірність і обґрунтованість наукових положень, висновків і рекомендацій, викладених у дисертаційній роботі, забезпечується коректним використанням методів дискретної математики, статистики і методів обробки програмного коду, а також результатами комплексних експериментальних досліджень.

Обґрунтованість отриманих результатів додатково підтверджується експериментальними дослідженнями, проведеними на реальних та тестових зображеннях, з використанням метрик оцінювання якості моделей. Результати експериментів демонструють стабільність, відтворюваність та статистичну значущість отриманих висновків, а також підтверджують ефективність запропонованих методів і моделей у порівнянні з існуючими підходами.

Таким чином, наукові положення, висновки та рекомендації, сформульовані у дисертаційній роботі, є достатньо обґрунтованими, логічно несуперечливими та підтвердженими як теоретичними міркуваннями, так і результатами експериментальних досліджень.

3. Наукова новизна одержаних результатів

Дисертаційна робота вирішує актуальне та важливе для галузі комп'ютерних наук науково-практичне завдання, містить раніше захищені наукові положення та результати, які отримані автором особисто, а саме:

- удосконалено інтегральний критерій якості захисних перетворень, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), що побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів;

- запропоновано метод захисного перетворення зображень на основі хаотичного відображення Тент з управлінням, що дозволило на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування за інтегральним критерієм якості;

- отримала подальший розвиток модель побудови псевдовипадкових послідовностей, яка заснована на зв'язку між похідними поліномів Чебишева

другого роду та поліномами Чебишева, а також на зв'язку згорнутих чисел k -перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка, що дало можливість отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації при її обміні у групі довірених користувачів;

– розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням захистного перетворення на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтгомері, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості.

Положення наукової новизни, які виносяться на захист сформульовані відповідно до тематики дослідження, відповідають меті дисертації, виконані повністю, здобувач володіє методологією наукової діяльності повною мірою.

4. Повнота викладення результатів дисертації в опублікованих працях

Публікації за темою дисертаційної роботи охоплюють усі її основні розділи та достатньо повно відображають зміст і результати проведених досліджень. Аналіз наукових публікацій і особистого внеску здобувача у виконанні дослідження свідчить про те, що основні наукові положення, висновки та рекомендації, викладені у дисертації та винесені на захист, отримано здобувачем особисто в період з 2022 по 2026 рік і узагальнено під час оформлення дисертаційної роботи.

Основні наукові результати дисертаційної роботи викладено в 13 наукових публікаціях, серед яких: 2 статті, опубліковані у виданнях, включених до Переліку фахових видань України (категорія «Б»), що індексуються у міжнародних наукометричних базах даних, зокрема Index Copernicus International та Google Scholar; 2 статті, опубліковані у виданні, включеному до Переліку фахових видань України (категорія «А»), що індексується у міжнародній наукометричній базі Scopus; 2 статті, опубліковані у зарубіжних наукових виданнях та проіндексовані у наукометричній базі Scopus; 1 стаття опублікована у зарубіжному науковому виданні; 6 доповідей міжнародних наукових конференцій.

Дисертаційну роботу Хамітова Віталія Миколайовича оформлено відповідно до вимог освітньо-наукової програми підготовки доктора філософії за спеціальністю 122 «Комп'ютерні науки», розробленої на основі стандарту вищої освіти за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» для третього (освітньо-наукового) рівня вищої освіти.

5. Значення роботи для науки та практики

Наведені в дисертаційній роботі результати досліджень дозволяють зробити висновок про її наукову значущість, що підтверджується комплексом теоретичних і експериментальних досліджень, проведених здобувачем для обґрунтування ефективності запропонованих методів і моделей підвищення

конфіденційності та цілісності обміну зображеннями для групи довірених користувачів шляхом захисного перетворення зображень на основі хаотичних відображень для підвищення швидкодії та/або зменшення ресурсозалежності.

Отримані результати розширюють наявні наукові підходи до конфіденційності та цілісності обміну інформацією та сприяють розвитку методів захисту інформації.

Результати дисертаційного дослідження є практично значущими та орієнтованими на використання у реальних інформаційних системах, в яких здійснюється обмін зображеннями високої роздільної здатності для групи довірених користувачів. Запропоновані методи та моделі дозволяють підвищити точність і своєчасність усунення потенційних загроз та знизити ймовірність спотворення зображень. Розроблені рішення реалізовано у вигляді програмних модулів, придатних для інтеграції в існуючі системи.

Результати дисертаційної роботи впроваджені у діяльності державного підприємства «Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України», у діяльності Військово-медичного клінічного центру Південного регіону та знайшли відображення у навчальному та у науково-дослідницькому процесі Національного університету «Одеська політехніка», що підтверджує їх практичну придатність і ефективність.

6. Відсутність (наявність) порушення академічної доброчесності

В результаті вивчення дисертаційної роботи порушень академічної доброчесності не виявлено. Всі запозичення, які є в роботі, мають посилання на відповідні джерела, інші – є загальноновживаними і не є плагіатом.

Публікації здобувачем результатів досліджень у рецензованих виданнях, які передбачають попередню перевірку матеріалів на відсутність запозичень, є одним із важливих підтверджень відсутності порушень академічної доброчесності. Крім того, перевірка дисертації здобувача, яку проведено членами групи забезпечення підготовки докторів філософії за ОНП по спеціальності 122 «Комп'ютерні науки», не виявила фактів порушення академічної доброчесності.

7. Дискусійні положення та зауваження щодо змісту дисертації

1. Більшість рисунків у Розділі 1 (наприклад, рис. 1.2, 1.3, 1.4, 1.5, 1.6, 1.8) мають підписи та осі англійською мовою (наприклад, «Logistic Map Bifurcation Diagram», «Lyapunov Exponent Lambda»). Слід було б для усіх позначень на графіках та рисунках у тексті роботи дати переклад українською мовою (або навести відповідні пояснення в підписі).

2. В роботі недостатньо чітко висвітлено, як саме згорнуті числа k -перетину послідовності Фібоначчі інтегровані в загальну архітектуру захисного перетворення зображень поруч із хаотичним відображення Тент.

3. У фінальній версії програми автор залишає тільки протокол Бурместера-Десмедта. Незрозуміло, чому тут відсутній деревоподібний протокол, хоча склад групи довірених користувачів може змінюватися.

4. У тексті розглянутої роботи присутні певні стилістичні та граматичні неточності: зокрема, «мавпячі тести» (стор. 55) – краще сформулювати як «тести на основі теореми про нескінченну кількість мавп» («Monkey tests»).

Зазначені зауваження мають дискусійний характер, не впливають на загальну позитивну оцінку дисертаційної роботи та не знижують наукової і практичної цінності отриманих результатів.

8. Загальний висновок про відповідність роботи встановленим вимогам

Дисертаційна робота Хамітова Віталія Миколайовича «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів» є цілісним, самостійним, завершеним науковим дослідженням, що має науково-прикладне значення, тема і зміст якого відповідає спеціальності 122 «Комп'ютерні науки».

З огляду на актуальність теми дисертації, обґрунтованості наукових положень, висновків і рекомендацій, які сформульовані в дисертації, їхньої наукової новизни, практичної цінності, повноти викладення в наукових публікаціях, відсутності порушень академічної доброчесності, вважаю, що дисертація відповідає вимогам «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 року №44 із змінами, а її автор Хамітов Віталій Миколайович заслуговує на присудження наукового ступеня доктора філософії у галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Офіційний рецензент:

кандидат технічних наук, доцент
кафедри комп'ютеризованих систем
та програмних технологій
навчально-наукового інституту
комп'ютерних систем
Національного університету
«Одеська політехніка»

Світлана ГРИГОРЕНКО