ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора, завідувача кафедри програмної інженерії Харківського національного університету радіоелектроніки Кирила Сергійовича Смелякова на дисертаційну роботу Хамітова Віталія Миколайовича на тему «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів», представлену на здобуття ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки»

Актуальність теми дисертації

Актуальність теми зумовлена двома фактами. По-перше, тим, що характерною тенденцію розвитку сучасних інформаційних технологій є стрімке зростання обсягів безпечної передачі зображень та відеоданих в режимі реального часу. Такий обмін зображеннями, де вимагається високий рівень безпеки, є затребуваним для телемедицини, «інтернета речей», геоінформаційних систем (супутникові знімки високої роздільної здатності), дистанційній судовій медицини (доказові зображення) тощо. По-друге, тим, що, на жаль, сучасні інформаційні технології та технології штучного інтелекту створили сприятливі умови для зловмисників, оскільки надають можливість перехоплення, знищення, фальсифікації та інших незаконних маніпуляцій з інформацією, яка подана у різних форматах представлення: тестові документи, аудіо файли, зображення та відеофайли тощо.

Ці фактори привели к проведенню чисельних різнопланових досліджень, що присвячені удосконаленню методів для захисних перетворень (шифрування) зображень, серед яких найбільш перспективними є методи на основі хаотичних відображень та послідовностей. Однак їх використання обмежується як недоліками самих методів, так і їхньою швидкодією та залежністю від програмно-апаратної реалізації та ресурсозалежністю.

Тому удосконалення моделей та методів захисного перетворення зображень на основі хаотичних відображень та послідовностей є важливою науково-прикладною задачею для підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

Зазначені чинники в сукупності обґрунтовують доцільність, актуальність та своєчасність обраного здобувачем напряму дослідження.

Наукова та структурна характеристика результатів дослідження

Структура дисертаційної роботи сформована відповідно до логіки розв'язання поставленого наукового завдання. Робота загальним обсягом 200 сторінок, з яких 144 сторінок становить основний текст, складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел із 102 найменувань та додатків. Текст ілюстровано 53 рисунком та 6 таблицями.

У вступі обґрунтовано актуальність дослідження, пов'язану з розробкою моделей та методів підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. Визначено методологічні засади роботи, сформульовано мету та завдання дослідження, висвітлено наукову новизну й практичне значення отриманих результатів, а також наведено відомості про їхню апробацію та публікації.

У першому розділі виконано системний аналіз проблеми підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. Визначено, що однією з перспективних тем досліджень для підвищення конфіденційності та цілісності є захисне перетворення зображень на основі хаотичних відображень. За результатами проведеного аналізу сформульовано мету та завдання досліджень.

У другому розділ запропонована нова динамічна система, а саме узагальнене відображення Тент з управлінням, яке стабілізує цикли заданої довжини. Ці цикли залежать від параметрів системи та початкового значення; ці величини є коротким ключем для генерації довгої псевдовипадкової послідовності.

Одновимірне відображення Тент із додатково введеним до нього предикативним управлінням стало математичною основою для побудови нових методів генерації псевдовипадкових криптосистем. Запропоновано та досліджено метод генерації псевдовипадкових послідовностей на основі відображення Тент.

Обґрунтовано розробку інтегрального критерія якості шифрування, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтовано вибирати потокові та блочні шифри.

У третьому розділі запропонована модель побудови псевдовипадкових послідовностей на основі згорнутих чисел *k*-перетину послідовності Фібоначчі. В результаті проведених досліджень отримано сімейство узагальнених послідовностей зі зростанням вищого порядку і складнішими коефіцієнтами зв'язку, ніж у відомих послідовностей Фібоначчі. Доведено, що отримані послідовності є оригінальними і згідно з поданою заявою були представлені в онлайн-енциклопедії цілочисельних послідовностей (OEIS) під номерами A395431, A393329, A395902, A396356, що підтверджує потенціал запропонованого підходу до формування різних послідовностей, які можуть бути використані для підвищення надійності інформаційних систем.

У четвертому розділі запропоновано методику дослідження ефективності протоколів групового узгодження ключів. Показано, що при формуванні груп довірених користувачів з невеликим числом користувачів та малою динамікою найбільш ефективним є поєднання протоколу Бурместера-Десмедта та еліптичної кривої Монтгомері.

Розроблено метод обміну конфіденційними зображеннями групи довірених користувачів. Конфіденційність зображень забезпечується шифруванням із застосуванням псевдовипадкових послідовностей на основі модифікованого хаотичного відображення Тент. розроблено протокол формування групи довірених користувачів, яким дозволено доступ до зображень. Збереження зображень

забезпечується шістьма рівнями захисту. Проведено імітаційне моделювання розробленого методу. Моделювання продемонструвало працездатність методу в масштабі часу, близькому до реального, та масштабування на основі швидкодіючого протоколу Бурместера-Десмедта.

Висновки узагальнюють результати виконаного дослідження, підтверджують досягнення поставленої мети та наукову обґрунтованість запропонованих рішень.

Наукова новизна отриманих результатів

Відповідно до сформульованих завдань, у дисертаційній роботі отримано такі основні нові наукові результати:

- 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

захисного перетворення на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтґомері, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості.

Дотримання вимог академічної доброчесності, мова та стиль викладення результатів

За результатами аналізу тексту дисертації та публікацій автора за темою дисертації встановлено відсутність академічного плагіату, фабрикації чи фальсифікації результатів дослідження. Таким чином, порушення академічної доброчесності в дисертаційній роботі відсутні.

Дисертаційна робота написана українською мовою і має чітку структуру. Представлені в роботі аспекти викликають позитивні враження та свідчать про високий науковий рівень дослідницької праці. Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Ступінь обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Достовірність та обґрунтованість наукових положень, висновків і рекомендацій, що представлені у дисертаційній роботі, підтверджується коректним використанням математичного апарату, зокрема, дискретної математики, теорії множин та динамічних систем та методи обробки та передачі зображень. А також вони забезпечуються цілісною методологією проведення досліджень, які поєднують всі необхідні складові: теоретичний аналіз, математичне моделювання, експериментальну перевірку та порівняльне аналіз із застосуванням надійних критеріїв і метрик для оцінювання точності отриманих результатів.

Коректність запропонованих програмних рішень підтверджується результатами експериментів, проведених на різнорідних даних.

Повнота повнота викладу наукових положень та результатів в опублікованих працях

Наукові результати дисертації висвітлені у 13 наукових працях у вітчизняних та закордонних фахових виданнях, серед яких 4 статті в періодичних фахових виданнях України категорій А та Б, з них 2 статті проіндексовані у міжнародній наукометричній базі Scopus. Апробація результатів дослідження здійснювалася шляхом їх представлення на всеукраїнських та міжнародних наукових конференціях. Таким чином, вважаю, що наукові результати, описані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

Практичне значення отриманих результатів

Практичне значення дисертаційної роботи полягає у розробленні математичних моделей та методів, які можуть бути використані під час створення інформаційних систем для забезпечення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

Метод обміну цифровими зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням шифрування на основі модифікованого хаотичного відображення Тент, дозволив підвищити швидкодію шифрування та розшифрування при збереженні стійкості.

Модель побудови псевдовипадкових послідовностей дозволяє отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації для широкого кола завдань криптографічного захисту інформації. Отримані послідовності є оригінальними і згідно з поданою заявою були представлені в енциклопедії OEIS.

Розроблені в роботі наукові положення та практичні результати отримали впровадження 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».

Недоліки та зауваження по роботі

1. Розділ 2 дуже об’ємний, але окремі оглядові фрагменти мають довідковий характер, практично далі не використовуються і могли б бути подані більш стисло. Зокрема це стосується біфуркаційних діаграм і показника Ляпунова.

2. Підрозділ 2.2.2, присвячений дослідженню псевдохаотичної послідовності Тент візуальним способом, перебільшений за об’ємом, адже кількісні методи тестування послідовностей, що використані далі, дають більш об’єктивні результати.

3. Потрібно було б зробити текстові пояснення до рисунків 4.7-4.9, щоб пояснити, як саме вони відображують масштабованість методу для різних протоколів.

4. Рисунок 4.16 містить структурно-логічну схема розробленого методу, що налічує шість рівнів захисту зображень. Доцільно було б зробити кількісну оцінку внеску кожного рівня в інтегральний рівень захисту.

5. У розділі 4 дисертації використано значну кількість англомовних термінів та умовних абревіатур, характерних для галузі криптопротоколів на еліптичних кривих. Для полегшення сприйняття матеріалу доцільно було б у наводити їх українські відповідники.

6. У тексті дисертації подекуди зустрічаються поодинокі стилістичні та термінологічні неточності, які, однак, не впливають на основні наукові положення та результати дослідження.

Вважаю, що наведені зауваження мають переважно рекомендаційний характер, не знижують наукової новизни та практичного значення отриманих результатів і не впливають на загальну позитивну оцінку дисертаційної роботи.

Загальні висновки по дисертації

Вважаю, що дисертаційна робота Хамітова Віталія Миколайовича «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є завершеним науковим дослідженням, у

межах якого розв’язано актуальне науково-прикладне завдання у сфері захисних перетворень зображень.

Дисертація за актуальністю, належним рівнем наукової новизни та практичної значущості 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 (зі змінами), а Хамітов Віталій Миколайович заслуговує на присудження ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп’ютерні науки».

Офіційний опонент
завідувач кафедри програмної інженерії
Харківського національного університету радіоелектроніки
доктор технічних наук, професор

Кирило СМЕЛЯКОВ