МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ

НІМЕНКО ЄВГЕНІЙ ВАСИЛЬОВИЧ

УДК 004.021

СИСТЕМА ХАОТИЧНОГО ШИФРУВАННЯ ЗІ ЗМІНАМИ НА БАЗІ ОДНОПЛАТНОГО КОМП'ЮТЕРА ORANGE PI

Спеціальність 123 – Комп'ютерна інженерія

Автореферат

магістерської роботи

на здобуття кваліфікації магістра з комп'ютерної інженерії

Миколаїв – 2020

Робота виконана у Чорноморському національному університеті ім. Петра Могили.

Науковий керівник: канд. техн. наук
Крайник Ярослав Михайлович,
ЧНУ ім. Петра Могили,
зав. кафедри комп'ютерної інженерії

Рецензент: др. техн. наук, проф. каф. ІІС
Кондратенко Юрій Пантелійович,
ЧНУ ім. Петра Могили,
професор кафедри інтелектуальних інформаційних систем

Консультант: д-р біол. наук, професор
Григор'єва Людмила Іванівна,
ЧНУ ім. Петра Могили,
завідувач кафедри екології Медичного інституту

Захист відбудеться «26» лютого 2020 р. о 9^{00} на засіданні Екзаменаційної комісії, ауд. 2-406

З магістерською роботою можна ознайомитись на сайті ЧНУ ім. Петра Могили за посиланням http://chmnu.edu.ua

Автореферат оприлюднений «21» лютого 2020 р.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Системи спостереження за об'єктами з внутрішнім шифруванням даних користуються великим попитом на сучасному ринку. Проблема якісного та швидкого шифрування отриманих зображень досі залишається недостатньо вирішеною для таких систем. Більшість наявних на ринку систем використовують традиційні алгоритми шифрування тексту, такі як AES, IDEA, RES. Ці алгоритми не завжди можуть бути доцільно використані для шифрування зображень, оскільки вони мають більші надлишкові дані та значення пікселів між собою сильно співвідносяться, і в результаті такі алгоритми вимагають більшої обчислювальної потужності та більшого обсягу пам’яті. Також, зображення, які були зашифровані такими алгоритмами можуть дещо втратити певні деталі зображення при процесі дешифровки. Використання хаотичних карт для шифрування зображень виглядає більш доцільною альтернативою серед усіх інших. Хаотичні карти часто використовуються при вивченні динамічних систем, які виявляють дуже чутливу до початкових умов поведінку і навіть невеликі зміни початкових значень можуть давати широко розбіжні результати. Існує тісний зв’язок між хаотичною системою та криптографією, що робить алгоритми, засновані на хаосі, чудовим кандидатом для шифрування зображень. Для заданих параметрів дві початкові умови можуть відхилятися в експоненціальному відношенні до двох різних інжекторів. Завдяки цим хаотичним параметрам та початковій умові можливо створити великий простір ключів, що ще більше підвищує безпеку. Через хаотичну поведінку, дані для зловмисника здаються випадковими, тоді як лише відправник і отримувач знають, що система чітко визначена.

Мета: вдосконалити існуючий алгоритм хаотичного шифрування, що використовує перестановки при шифруванні та інтегрувати його в систему спостереження на базі одноплатного комп'ютера.

Для досягнення поставленої мети необхідно вирішити такі **завдання**:

- з аналітичного огляду літератури та патентної інформації сформулювати завдання дослідження та розроблення;
- вдосконалити існуючий алгоритм;
- розробити алгоритм роботи шифратора та дешифратора зображень;
- розробити програмне забезпечення для системи спостереження на базі технології одноплатного комп'ютера Orange Pi;
- виготовити робочий прототип системи шифрування та здійснити його тестування;
- розробити питання з цивільного захисту та охорони праці.

Об'єкт: методи хаотичного шифрування на базі перестановок.

Предмет: апаратне та програмне забезпечення системи хаотичного шифрування зі зміщенням.

Гіпотеза: очікується, що вдосконалений алгоритм шифрування підвищить захищеність без суттєвих втрат в швидкодії.

Наукова новизна: полягає у тому, що буде вдосконалено алгоритм на основі теорії хаосу для систем спостереження.

Практичне значення: полягає у тому, що розроблена система стане більш надійною та зможе використовуватись на ринку систем спостереження.

Апробація результатів магістерської роботи відбулася під час:

- XXII Всеукраїнської науково-практичної конференції «Могилянські читання-2019» (Миколаїв, 2019).

Публікації. Результати та основні положення магістерської роботи опубліковані у вигляді тез в збірнику матеріалів науково-практичної конференції «Могилянські читання – 2019: Досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти» [1].

Структура та обсяг роботи. Магістерська робота складається з анотації на 3 сторінках, вступу, трьох розділів, висновків, переліку джерел посилання з 35 найменувань, 2 додаток на 3 сторінках,. Основна частина роботи становить 72 сторінки, серед яких 48 рис. та 1 табл.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** подано обґрунтування актуальності теми магістерської роботи, зазначено її зв’язок з науковою новизною, сформульовано мету та завдання дослідження, вказано практичне значення одержаних результатів, представлено відомості про апробації результатів роботи та публікації автора. Системи спостереження за об'єктами з внутрішнім шифруванням даних користуються великим попитом на сучасному ринку. Проблема якісного та швидкого шифрування отриманих зображень досі залишається недостатньо вирішеною для таких систем.

У **першому розділі** магістерської роботи **«Аналітичний огляд систем хаотичного шифрування**» досліджуються основні алгоритми з використанням детермінованого хаосу. Проаналізовано історію розвитку теорії хаосу, пояснюється причини тісного взаємозв’язку хаосу та криптографії. Описані основні вимоги до систем шифрування на основі динамічного хаосу, та можливості їх порівняння. Наведено порівняльна характеристика стандартних алгоритмів, їх переваг на недоліків. На основі отриманих даних обирається алгоритм для подальшого вдосконалення.

У **другому розділі** магістерської роботи **«Розробка апаратної частини системи хаотичного шифрування зі зміщенням»** здійснюється аналіз апаратного забезпечення, а саме одноплатних комп'ютерів, плат розширення, та різної периферії. Наведено основні технічні характеристики одноплатного комп'ютера Orange Pi Zero. Визначено можливості плати для розробки та програмування вбудованих систем та систем керування та контролю. Обґрунтовується використання плати розширення для додаткової периферії. Описано процес створення схемотехнічної документації, програмне забезпечення Fritzing для створення схемотехнічної документації. Пояснюється вибір елементної бази та описується етапи створення принципової схеми та етапи автотрасування. Демонструється прототип пристрою (рис 1).

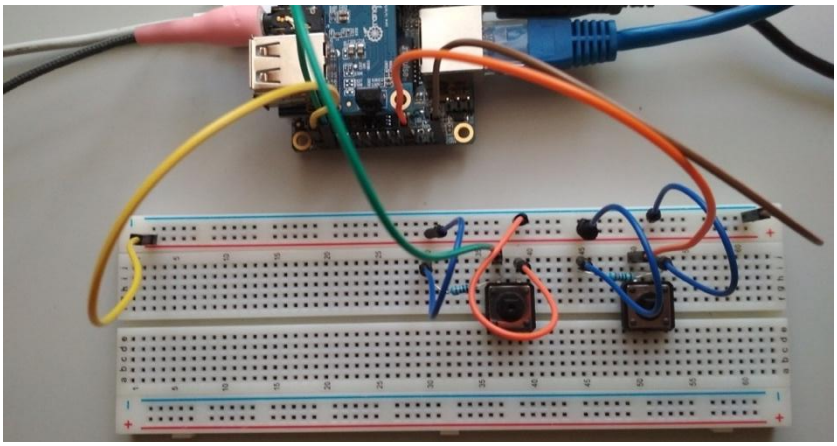

Рисунок 1 – Прототип пристрою

Третій розділ магістерської роботи **«Розробка програмної частини системи хаотичного шифрування зі зміщенням»** присвячений модифікації обраного в першому розділі алгоритму, інтеграції його в систему спостереження та тестування отриманого алгоритму для порівняння з традиційними алгоритмами на основі детермінованого хаосу. Після завершення всіх ітерацій вхідне зображення буде зашифровано достатньо навіть після виконання одного проходу шифрування. На рисунку 1.2 зображено результати виконання першої ітерації алгоритму Arnold`s cat map та її модифікованої версії. Як можемо бачити, в

результаті стандартного алгоритму зображення недостатньо спотворюється, а після першої ітерації модифікованого алгоритму зі зміщенням чітко простежується поява так званого «екранного шуму», значення пікселів та їх розташування здаються хаотичними.

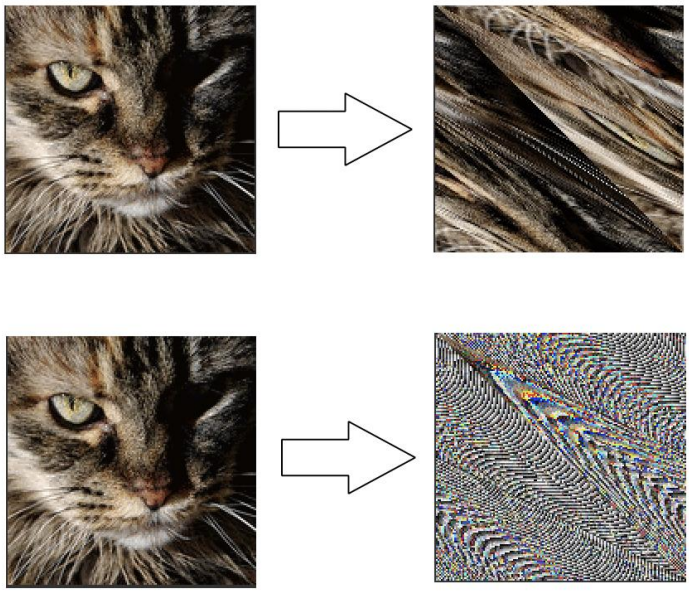

Рисунок 1.2 – Порівняння алгоритмів шифрування

В даному розділі також наведені результати тестування надійності алгоритму шифрування за допомогою показників NPCR та UACI. В результаті порівняння було доведено, що модифікований алгоритм є більш надійним та достатньо швидким для використання в системах спостереження.

Додатки містять лістинг основних класів програмної реалізації системи хаотичного шифрування зі зміщенням.

У **спеціальній частині «Охорона праці та безпека у надзвичайних ситуаціях»** проведено аналіз факторів виробничого середовища у приміщенні підприємства «ФОП Яковенко Сергій Вікторович», а також визначено їх вплив на працівників. Встановлено, що всі показники відповідають санітарним нормам, що свідчить про оптимальні умови роботи на підприємстві «ФОП Яковенко Сергій Вікторович».

ВИСНОВКИ

Під час виконання магістерської роботи було отримано такі результати:

- алгоритми шифрування на основі детермінованого хаосу набувають все більшої популярності в контексті шифрування зображень;
- розроблений алгоритм шифрування зі зміщенням показав високі показники надійності порівняно з іншими алгоритмами хаотичного шифрування;
- загальна надійність системи на основі модифікованого алгоритму значно підвищилась та майже не втратила в швидкодії.

Було проведено аналітичний огляд існуючих алгоритмів шифрування з використанням хаотичних відображень, на основі їх переваг та недоліків було обрано відображення Arnold`s cat map в якості кандидата на вдосконалення.

Для реалізації системи спостереження було проведено аналіз найбільш популярних одноплатних комп’ютерів та було обрано Orange Pi Zero в якості основної платформи, обґрунтовано доцільність використання додаткової плати розширення.

Під час розробки програмної частини було здобуто практичні навички написання скриптів на мові Python та Bash, та роботи в інтегрованому середовищі розробки PyCharm.

Розроблена система здатна функціонувати без втручання розробника завдяки створеному сценарію автозапуску.

Перспективи розвитку даної системи полягає у використанні алгоритму хаотичного шифрування зі зміщенням для шифрування відео. Розроблений алгоритм можна розширити для роботи з зображеннями будь-якого розміру.

Враховуючи, що алгоритм, який був взятий за основу – мав найгірші показники серед йому подібних, то можна сказати, що завдання виконано в

повній мірі. На даний момент алгоритм відповідає існуючому стандарту шифрування даних.

Серед подальших напрямів вдосконалення алгоритму можна розширити його можливості для роботи не тільки з квадратними зображеннями. Можливо застосувати алгоритм розбиття прямокутника на скінчену кількість квадратів, та для кожного квадрату виконати шифрування розробленим алгоритмом. Також, розроблений алгоритм можна використовувати для шифрування відео покадрово.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ РОБОТИ

1. Німенко Є. В., Крайник Я. М. Система хаотичного шифрування зі зміщенням на базі одноплатного комп’ютера Orange Pi. Могилянські читання-2019, XXI Всеукраїнська науково-методична конференція: тези доповідей / ЧНУ ім. Петра Могили. 2019. С. 98-99.

АНОТАЦІЯ

Німенко Є. В. Система хаотичного шифрування зі змінами на базі одноплатного комп’ютера Orange Pi. – На правах рукопису.

Магістерська наукова робота на здобуття освітньої кваліфікації «Магістр комп’ютерної інженерії». – Чорноморський національний університет імені Петра Могили, Миколаїв, 2020., спрямована на дослідження систем шифрування на основі детермінованого хаосу. Розглянуто основні хаотичні відображення, які застосовуються для шифрування зображень, їх переваги та недоліки. Практичне значення результатів дослідження та розроблення полягає у тому, що розроблена система стане більш надійною та зможе використовуватись на ринку систем спостереження.

Пояснювальна записка магістерської роботи складається зі вступу, чотирьох розділів, висновків та двох додатків. У вступі визначається актуальність теми,

сформульовані мета, об’єкт, предмет та завдання дослідження та розроблення. У першому розділі досліджується зв’язок хаосу та криптографії, розглядаються основні хаотичні відображення та порівнюються їх характеристики. На основі порівняння обирається хаотичне відображення для вдосконалення. У другому розділі здійснюється аналіз апаратного забезпечення, а саме одноплатних комп’ютерів, плат розширення та компонентів периферії. Третій розділ присвячений вдосконаленню обраного алгоритму хаотичного шифрування за допомогою додаткового зміщення кольору пікселів при шифруванні. Запропоновано два шляхи інтеграції вдосконаленого алгоритму в систему спостереження. Також в даному розділі наведені результати роботи реалізованої системи та аналіз надійності модифікованого алгоритму. Також був розроблений розділ ООП, в якому розглянуто питання охорони праці в офісному приміщенні, виконано інтегральну оцінку умов праці та запропоновано заходи, спрямовані на їх покращення. У висновках наведено аналіз виконаної роботи та отриманих результатів дослідження та розроблення. У додатку А наведений лістинг сценарію роботи з камерою. У додатку В наведений лістинг шифратора та дешифратора на основі модифікованого алгоритму.

В цілому, магістерська робота без додатків містить 72 сторінки, 48 рисунків, 1 таблицю, 35 джерел посилання.

ABSTRACT

Nimenko Y. System of chaotic encryption with offset based on a single-board Orange Pi computer. – On the rights of the manuscript.

Master's work for obtaining an educational qualification "Master of Computer Engineering". – Petro Mohyla Black Sea National University, Mykolaiv, 2020., is aimed at the study of encryption systems based on deterministic chaos. The basic chaotic mappings that are used for image encryption, their advantages and disadvantages are considered. The practical significance of the R&D results is that the developed system will become more reliable and can be used in the market for surveillance systems.

The master's explanatory note consists of an introduction, four sections, conclusions and two appendices. The introduction defines the relevance of the topic, the stated purpose, object, subject and tasks of the research and development. The first section examines the relationship between chaos and cryptography, examines the basic chaotic mappings and compares their characteristics. Based on the comparison, a random display is selected for improvement. The second section analyzes hardware, such as single board computers, expansion boards, and peripheral components. The third section is dedicated to improving the selected chaotic encryption algorithm by further shifting the color of the pixels when encrypted. Two ways of integrating the advanced algorithm in the observation system are proposed. Also, in this section are the results of the implemented system and the reliability analysis of the modified algorithm. An OOP section was also developed to address occupational safety issues, integrate an assessment of working conditions and propose measures to improve them. The conclusions provide an analysis of the work performed and the results of the research and development. Appendix A lists the camera scripts. Annex B lists the encoder and decoder based on a modified algorithm.

In total, the master's work without applications contains 72 pages, 48 drawings, 1 table, 35 references.