МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Обратимые клеточные автоматы в криптографии

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Ромаденкина Артема Геннадиевича

Научный руководитель

д.ф.-м.н., профессор _____ В. А. Молчанов

21.01.2023 г.

Заведующий кафедрой

д. ф.-м. н., доцент _____ М. Б. Абросимов

21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

Криптография давно стала частью повседневной жизни. Наиболее широко используемые алгоритмы шифрования с открытым ключом полагаются на передовые результаты теории чисел для достижения высокого уровня безопасности, такие как RSA, безопасность которого, как полагают, зависит от сложности проблемы целочисленной факторизации. Эти системы, как правило, имеют относительно медленную реализацию, и, поскольку всегда нужны более эффективные и безопасные алгоритмы шифрования, имеет смысл рассмотреть альтернативные методы.

Теория клеточных автоматов началась в 40-х годах. Пространство состояло из двумерного массив ячеек, где каждая ячейка могла находиться в одном из двух состояний: включено или выключено. От первоначального варианта временная эволюция клеток определялась некоторыми математическими отношениями между соседями. Эта простая система позволяла генерировать довольно сложные паттерны, некоторые из них имели поведение, похожее на биологические процессы самовоспроизведения.

Клеточные автоматы, как среда для шифрования, являются одной из существующих альтернативных идей в теории, поскольку большинство клеточных автоматов могут быть реализованы на очень быстром оборудовании, поэтому схема на основе клеточных автоматов может иметь потенциал для более быстрого шифрования и дешифрования, чем существующие методики.

Клеточные автоматы принадлежат к классу сложности NP – задач, так как использованные локальные функции связи в моделях клеточного автомата эффективно вычисляются за полиномиальное время на детерминированной машине Тьюринга.

Цель работы – реализация алгоритма шифрования / дешифрования изображений с помощью модели обратимого клеточного автомата.

Решаемые задачи:

1) рассмотреть модели построения обратимых клеточных автоматов;

2) изучить схему шифрования и дешифрования с помощью обратимого клеточного автомата;

3) разработать программный комплекс на языке программирования Python для реализации шифрования / дешифрования изображений с помощью модели обратимого клеточного автомата;

4) провести оценку разработанного программного комплекса с общеизвестными результатами на основе сравнения гистограмм, энтропии и корреляции пикселей изображений.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и приложения. Общий объем работы – 57 страниц, из них 40 страниц – основное содержание, включая 36 рисунков и 2 таблицы, список использованных источников из 24 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы рассматриваются основные понятия теории клеточных автоматов и состоит из трёх подразделов.

В первом подразделе описывается теорема Кертиса-Хедлунда-Линдона.

Во втором подразделе приводится теорема сада Эдема.

В третьем подразделе описываются основные понятия обратимых клеточных автоматов, модель их построения.

Второй раздел состоит из двух подразделов. В первом подразделе приводится описание PRP – шифрования при помощи модели обратимого клеточного автомата. Во втором подразделе приводится описание схемы шифрования / дешифрования изображений с помощью модели обратимого клеточного автомата.

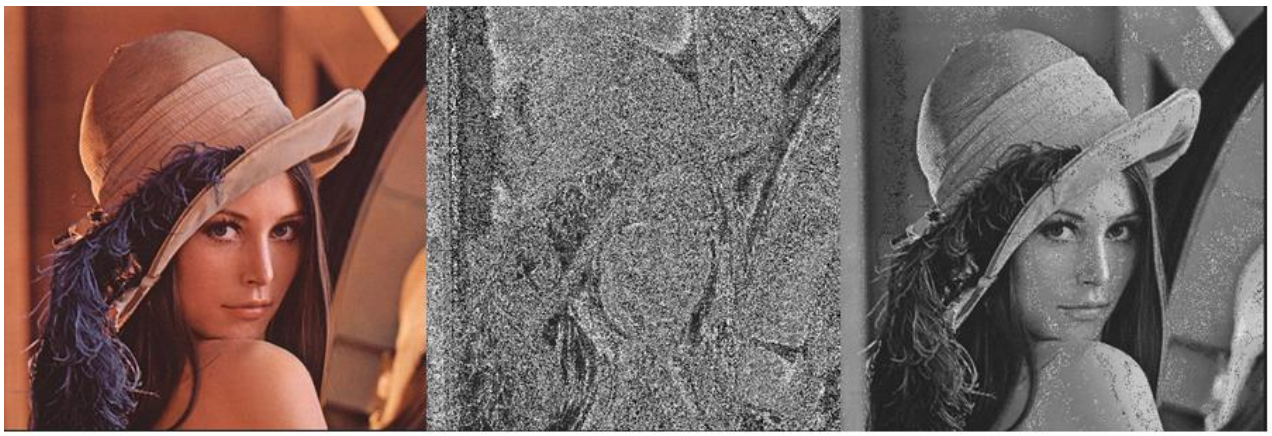
Третий раздел включает в себя три подраздела. В первом подразделе приводится описание и демонстрируется модели построения обратимого клеточного автомата, используя правило 90. Во втором подразделе рассматривается функциональность интерфейса пользователя, блок-схема программы и демонстрируются примеры выполнения на разных исходных данных. В третьем подразделе производится сравнение нашей программной реализации с общеизвестными результатами других программных комплексов.

В третьем разделе дипломной работы рассматривается программная реализация шифрования / дешифрования изображения с помощью модели обратимого клеточного автомата. Программный комплекс разработан на языке Python. Для создания графического интерфейса использована платформа Qt Designer. Для сборки проекта использована стандартная библиотека python – pyinstaller. Так же использована библиотека PyQt5 для реализации интерфейсной части программы и библиотека cv2 для работы с изображениями. Среда разработки – PyCharm.

Функциональность программы довольно проста. Сначала пользователь выбирает путь до изображения, каталог сохранения результатов и необходимую операцию: шифрование или дешифрование. Далее данные пути проверяются на корректность, при успешной проверке выполняется выбранная пользователем операция. После этого по кнопке можно просмотреть результаты выполнения.

Третий раздел дипломной работы содержит описание программной реализации, примеры выполнения операций и включает в себя сравнительную характеристику разработанного программного комплекса с общеизвестными результатами.

На данном рисунке можно увидеть результаты выполнения операции шифрования и дешифрования нашим программным комплексом.



(а) **(б)** **(в)**

Рисунок 1 – Изображение: а – оригинальное, б – зашифрованное, в - дешифрованное

Сравнительная характеристика производится с помощью оригинального изображения, представленного слева на рисунке 1 (а).

Гистограмма оригинального изображения под номером 1 (а) и зашифрованного изображения под номером 1 (б) представлена на рисунке 2 и 3. Из рисунка 3 видно, что гистограмма зашифрованного изображения однородна, и поэтому никакая статистическая атака не может раскрыть любую информацию об оригинальном изображении без знания секретного ключа.

Изображение 1 (а) было взято в качестве копии из pdf – файла, вследствие чего различия в полученных результатах могут быть связаны с отличием в характеристиках изображений, таких как: контрастность, плотность пикселей и т.д.

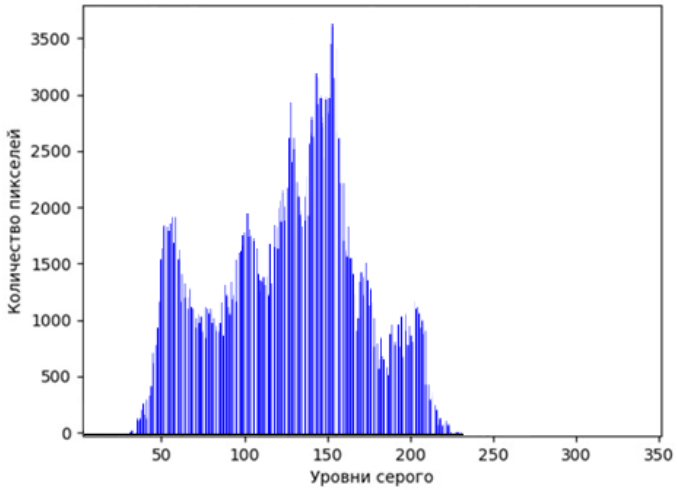


Рисунок 2 – Гистограмма оригинального изображения для рисунка 1 (а)

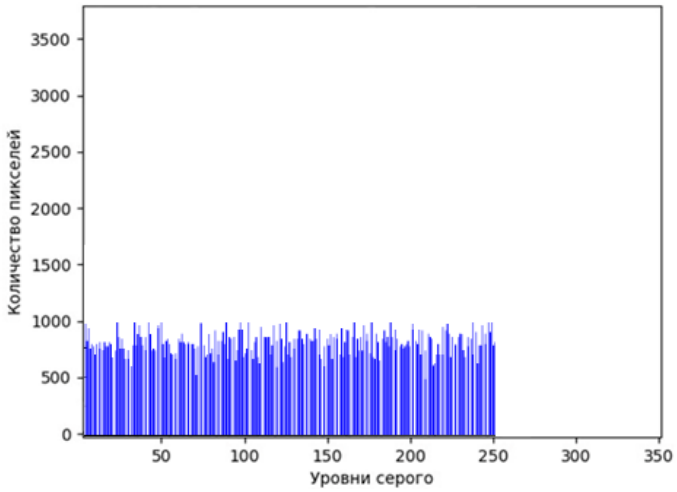
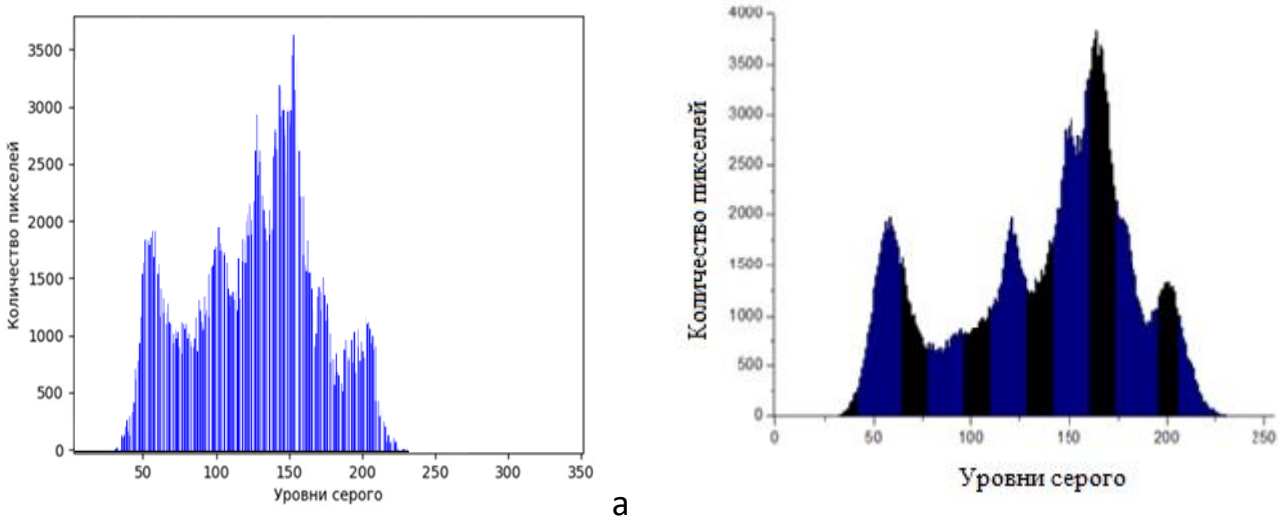


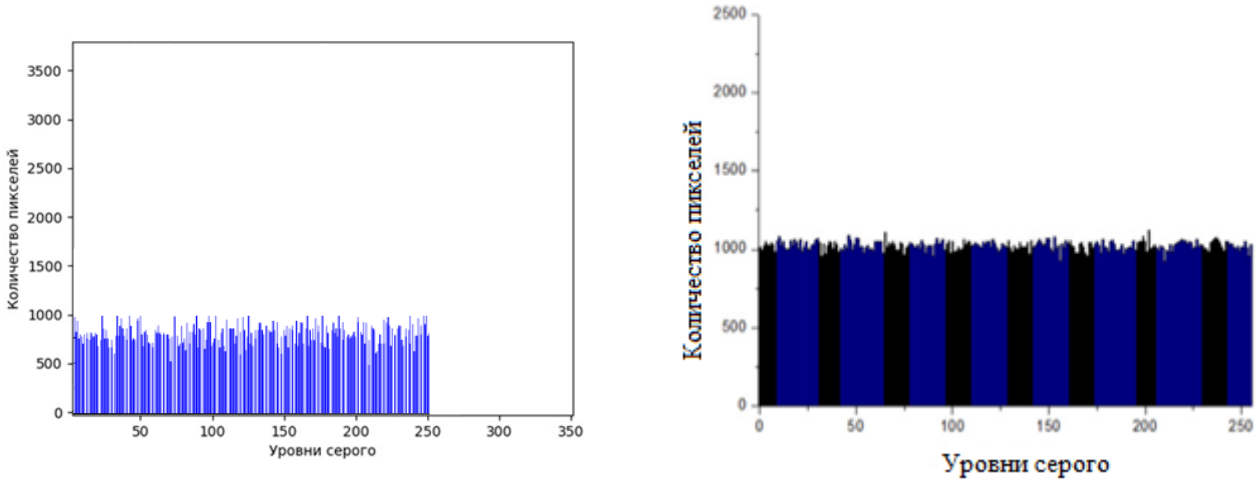
Рисунок 3 – Гистограмма зашифрованного изображения для рисунка 1 (б)

Сравнение результатов полученных гистограмм с общеизвестными результатами, можно увидеть на рисунке 4 и 5.



а б

Рисунок 4 – Гистограмма оригинального изображения: а – для рисунка 1 (а), б – для рисунка 1 (а) из общеизвестных результатов



а б

Рисунок 5 – Гистограмма зашифрованного изображения: а – для рисунка 1 (б), б – для рисунка 1 (б) из общеизвестных результатов

Таблица 1 иллюстрирует различные значения энтропии, полученные для оригинальных и зашифрованных изображений. Зашифрованные изображения имеют энтропию, близкую к оптимальной, и поэтому обладают случайными свойствами, которые предотвращают любые атаки статистического криптоанализа, поскольку никакая важная информация не может быть получена из зашифрованного изображения без секретного ключа.

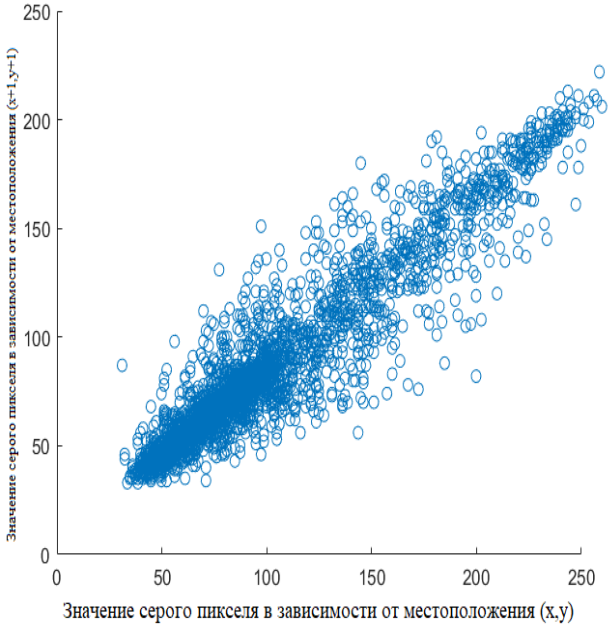
Таблица 1 – Энтропия оригинального и зашифрованного изображения

Изображение	**Энтропия изображения**	
	оригинального	**зашифрованного**
Девушка (Рисунок 19)	7.2009	7.9977
Девушка (Рисунок 19) из общеизвестных результатов	7.2103	7.9999

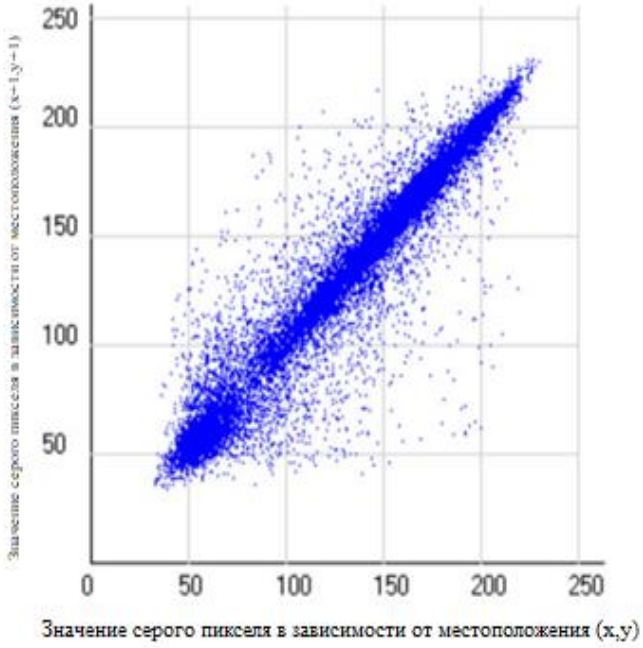
Сравнивая энтропию копии изображения с pdf – файла, различия в значениях, как при сравнении оригинального, так зашифрованного изображения, получаются менее 5%.

Еще один важный статистический тест, позволяющий показать высокое качество свойств диффузии и путаницы, предлагаемой криптосистемы, является корреляция между пикселями изображений. Поскольку цифровые изображения, как правило, содержат избыточное содержимое, они демонстрируют сильную корреляцию между соседними пикселями в отличие от зашифрованных изображений, которые должны иметь корреляцию, близкую к нулю, чтобы избежать любого возможного вывода информации, что приводит к возможной статистической атаки. Для выполнения теста корреляции пикселей на изображении выбирается набор из 20000 случайных пар соседних пикселей (в вертикальном, диагональном и горизонтальном направлениях), а затем вычисляется коэффициент корреляции.

Корреляция изображения для рисунка 1 (а) в диагональном, вертикальном и горизонтальном направлении представлена на рисунках 6, 7, 8 соответственно.

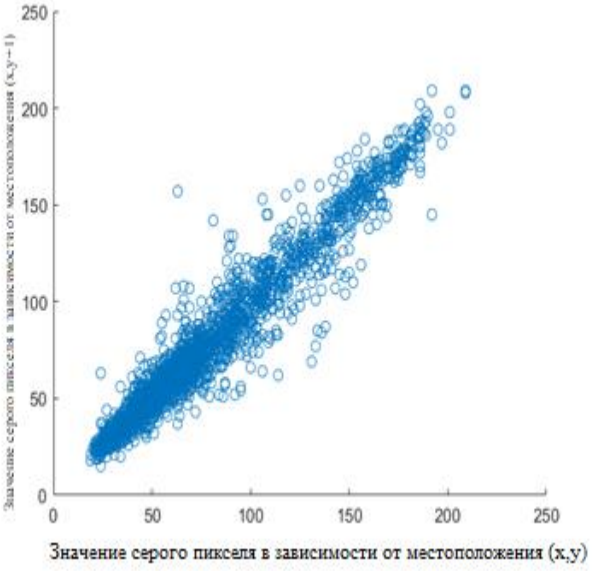


а

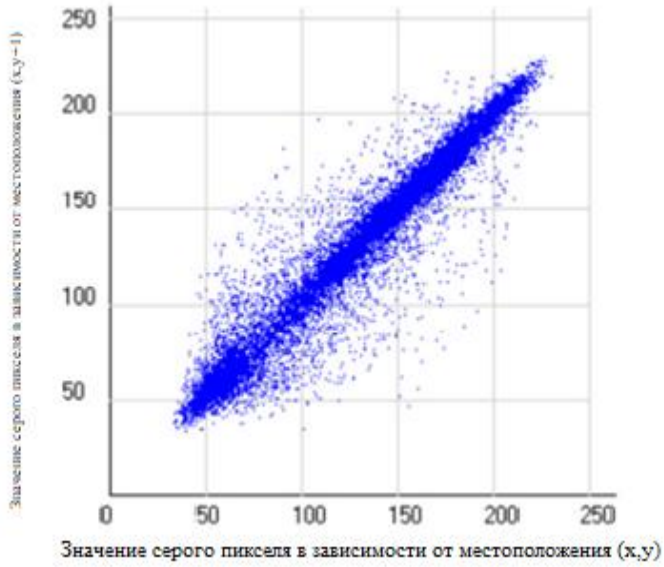


б

Рисунок 6 – Корреляция изображения в диагональном направлении: а – для рисунка 1 (а), б – для рисунка 1 (а) из общеизвестных источников

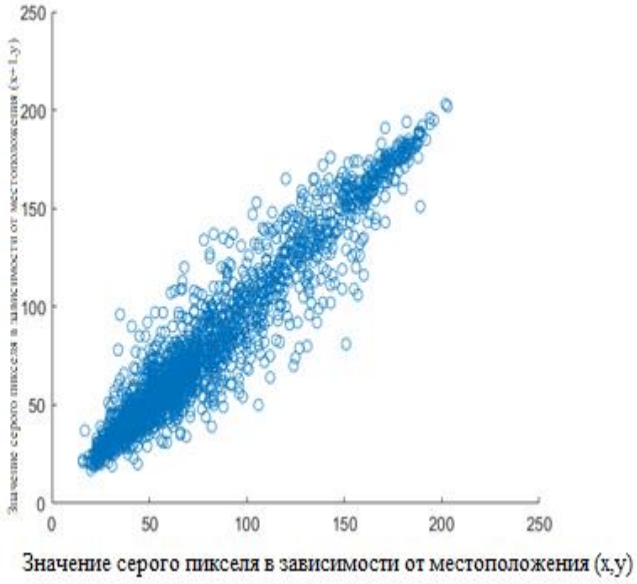


а

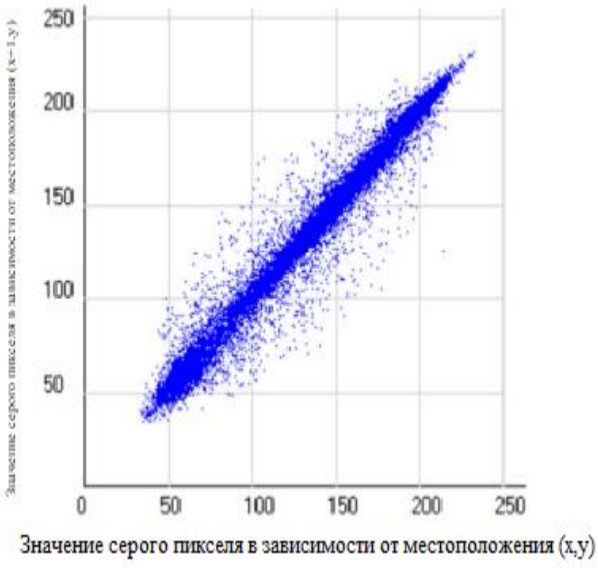


б

Рисунок 7 – Корреляция изображения в вертикальном направлении: а – для рисунка 1 (а), б – для рисунка 1 (а) из общеизвестных источников



а



б

Рисунок 8 – Корреляция изображения в горизонтальном направлении: а – для рисунка 1 (а), б – для рисунка 1 (а) из общеизвестных источников

Из сравнения результатов реализаций можно установить, что корреляции имеют, в обоих случаях, схожую структуру.

ЗАКЛЮЧЕНИЕ

В ходе работы изучены модели построения обратимых клеточных автоматов, рассмотрена схема шифрования / дешифрования изображений с помощью модели обратимого клеточного автомата, а также проведена сравнительная оценка с общеизвестными результатами;

В практической части работы разработан программный комплекс на языке Python для реализации операции шифрования / дешифрования изображений с помощью модели обратимого клеточного автомата. Программный комплекс представлен в виде оконного приложения для MS-Windows и выполнен на платформе Qt Designer что значительно упрощает его использование.

Поставленные задачи полностью решены.

Программный комплекс может применяться в учебных целях, а также в прикладных задачах, связанных с необходимостью передачи конфиденциальной информации.