УДК 004.001

АЛГОРИТМ ПОСТКВАНТОВОГО ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ И ПРИНЦИПА КУБИКА РУБИКА

А.В.Сидоренко, И.В.Сергеев

Учреждение образоваия «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе приведены основные аспекты гибридного алгоритма постквантового шифрования изображений, основанного на 3D- хаотической системе и принципе Кубика Рубика. Для создания криптографически стойкого алгоритма предложено объединить преимущества хаотических систем и квантовых вычислений.

Представлены основные особенности разработанного алгоритма в виде компьютерной программы.

Ключевые слова: постквантовое шифрование, изображение, хаотические системы, принцип Кубика Рубика.

POSTQUANTUM IMAGE ENCRYPTION ALGORYTHM WITH CHAOTIC SYSTEM AND RUBIK'S CUBE PRINCIPLE

A.V. Sidorenko, I.V. Sergeev
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The main aspects of combine the advantages new 3D-chaotic system and quantum computing based on a modified Lorenz system for generating pseudorandom keys and Rubk's Kyber principle for perform image scrambling operarions (cyclic shifting of row and column) is used. The main features, structure and properties of created algorithm are received as computer program.

Keywords: post-quantum encoding; image; chaotic system; Rybic's Kyber principle

Введение

С появлением новых квантовых вычислительных систем возникает необходимость перехода к новым методам криптографии, способным обеспечить надежную защиту в квантовую эпоху [1,2]. При шифровании изображений, характерным для которых является обработка большого объема данных, возникает необходимость перехода к новым методам защиты информации, так как существующие традиционные методы типа RSA, ECC не обладают соответствующими свойствами. При использовании постквантового шифрования, представляющего собой семейство криптографических алгоритмов, устойчивых к атакам как со стороны классических, так и квантоых компьютеров, возникает проблема совместимости.

Одним из перспективных инновационных направлений является использование хаотических систем для генерации псевдослучайных ключей и реализации процедур перемешивания и диффузии данных. В данной работе предлагается объединить преимущества квантовой криптографии и хаотических алгоритмов, используя квантовую модель представления изображения и принцип Кубика Рубика для реализации эффективного алгоритма щифрования.

Алгоритм на основе хаотической системы и принципа Кубика Рубика

Современные методы защиты информации все чаще применяют идеи из смежных областей, включая динамические системы и комбинаторную математику.

Кубик Рубика представляет собой пластмассовый куб (форм-фактор в первоначальном варианте 3x3x3). Его видимые элементы снаружи выглядят как 54 грани малых кубиков, составляющих один большой куб, и способны вращаться вокруг трех внутренних осей куба. Поворачивая строки и столбцы кубика можно осуществлять циклически сдвиг строк и столбцов. Основываясь на этом, эффект шифрования изображения может быть достигнут путем циклического перемешивания строк и столбцов в процессе шифрования [3]. Полученные путем сдвига блоки могут быть представлены в виде массивов пикселей элементов шифруемого изображения. С математической точки зрения поворот граней кубика аналогичен применению матрицы перестановки к множеству векторов, описывающих значения составляющих итенсивностей цвета (RGB- (R- red (красный), G-green (зеленый), B- blue (голубой). За счет рекурсивных итеративных перестановок в криптографии принцип Кубика Рубика позволяет достичь высокой степени спутанности и рассеяния информации. Спутанность при этом достигается за счет частых перестановок пикселей между блоками, а рассеянне – за счет воздействия на значения цветовых компонентов (в частности, за счет побитовой операции-XOR с псевдослучайными последовательностями).

Важную роль играют хаотические отображений, применяемые в процессе управления поворотами, например, отображение Кота Арнольда, логистическое отображение [4]. Многократное применение выбранного отображения обеспечивает равномерную перестановку пикселей.

Программная реализация алгоритма

В данной работе реализация алгоритма проводится в виде компьютерной программы следующим образом:

Разработана программная реализация алгоритма квантового шифрования изображений, основанная на предложенной новой хаотической системе и принципе Кубика Рубика, обеспечивающих устойчивость к атакам и высокую степень запутанности данных.

Оптимизирован алгоритм обработки изображений с использованием мнопоточности, что позволило сократить время выполнения шифрования и повысить производительность системы.

Созданы квантовые схемы с прнменением библиотеки Quiskit для представления изображения, осуществления операции трансляции и диффузии, а также моделирования квантовых вычислений на симуляторе Aersimulator.

Проведено тестирование корректности работы алгоритма, визуального анализа результатов и сравнения зашифрованных изображений с целью подтверждения соответствия реализации требованиям безопасности

и эффективности. Важную роль играют хаотические отображения, применяемее в процессе управления поворотами, например, отображение кота Арнольда, логистическое отображение.

Для реализации алгоритма шифрования на языке программирования Python использовались следующие библиотеки:

```
Import numpy as np
import cv 2
from qiskit import Quantum Circuit, Quantum Register, Classical Register,
transpile
from qiskit import AerSimulator
from math import ceile, log2
import concurrent.futures
import os
```

где numpy(np) –используется для работы с массивами, создания ключей и хранения значений изображения, cv2 (Open CV) –бибдиотека для работы с изображениями, используется для чтения изображения и преобразвания его в нужные форматы, Quiskit -библиотека для создания квантовых схем. В коде используются: Quantum Circuit, Quantum Register, Classical Register – создание и работа с классическими и квантовыми регистрами. Transpile-преобразование схемы в оптимизированную форму для симуляции или выполнения на реальном квантовом компьютере. AerSimulator –симулятор квантовых схем от Quiskit, math –используются функции для математических вычислений – (cell, log2), concurrent. futures –позволяет обрабатывать блоки изображения параллельно с помощью многопоточности, Qs –используется для получения числа процессоров при многопоточности.

Следует отметить, что библиотека Quiskit разработана компанией IBM и в нашем исследовании была использована как платформа для моделирования и анализа алгоритма квантового шифрования изображений. Для определения работоспособности и надежности работы алгоритма проведено тестирование разработанной программы. Тестирование проводилось на черно-белых и цветных тестовых изображениях, имеющих различные размеры.

Проведенный анализ показал, что в результате работы исследуемого алгоритма коэффициент корреляции соседних пикселей, рассчитанных в горизонтальном, вертикальном и диагональном направлениях оригинальных и зашифрованных изображений близок к нулю, что усложняет прослеживание закономерностей пикселей.

Выполненный энтропийный анализ, проведенный с использованием симуляционных данных показал, что рассматриваемый алгоритм является

устойчивым к атакам, так как информационная энтропия близка к идеальной величине, равной восьми.

Заключение

В работе рассматривается гибридный алгоритм квантового шифрования изображений, основанный на хаотической системе и принципе Кубика Рубика и его программная реализация. Программная реализация выполнена на языке Python, а также с использованием библиотек: Quiskit, Open CV и Numpy. Визульный и гистограммный анализ показал равномерное распределение пикселей в зашифрованных изображениях, а также отсутствие корреляции между соседними пикселями.

Список использованных источников

1. Kiktenko E.O (2018) Quantum Sequired Blokchain.*ArXiv:*1795.09258.v.3[quant]3 Jan20181.

2. Belklur M (2022) Quantum vs Classic Computing. A Comparative Analysis *Sevens International Conference on Fog and Mobile Edge Computing*,Pars, France,IEEE, p.1-8.
https://doi,org.10/1109/FMEC, s7-153. 2022.10062753

3. Landhaoukha R.A. Secure Image Algorithm Based on Rubik's Cube Principle.*Journal of Electric Computer Engineering* Article ID 173931(13)

4. Сидоренко А.В.(2016) Информационные системы на основе динамического хаоса. Беларусь, Минск. Издательство БГУ.

References

1. Kiktenko E.O (2018) Quantum Sequired Blokchain.*ArXiv:*1795.09258.v.3[quant]3 Jan20181.

2. Belklur M (2022) Quantum vs Classic Computing. A Comparative Analysis *Sevens International Conference on Fog and Mobile Edge Computing*,Pars, France,IEEE, p.1-8.
https://doi,org.10/1109/FMEC, s7-153. 2022.10062753

3. Landhaoukha R.A. Secure Image Algorithm Based on Rubik's Cube Principle.*Journal of Electric Computer Engineering* Article ID 173931(13)

4. Sidorenko A.V.(2016) *The Information Systems Based on Dynamic Chaos.Minsk. Belarusian State University* (in Russian)

Сведения об авторах

Сидоренко А. В., д-р техн. наук, проф. проф, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», SidorenkoA@yandex.by.

Сергеев И. В., студент 4 курса факультета радиофизики и компьютерных технологий, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the authors

Sidorenko A.V., Dr.Sci.(Techn), Prodfessor, professor, prof, Educational Institution "Belarusian State University of Informatics and Radioelectronics", sidorenkoA@yandex.by

Sergeev I.V., student, faculty of radiophysics and electronics, Educational Institution "Belarusian State University of Informatics and Radioelectronics".