ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION TECHNOLOGIES

УДК 004.832.519.6
https://doi.org/10.37661/1816-0301-2026-23-3-62-75

Поступила в редакцию | Received 14.05.2026
Подписана в печать | Accepted 04.06.2026
Опубликована | Published 30.09.2026

Постквантовое шифрование на основе хаотической системы и принципа кубика Рубика

А. В. Сидоренко✉, И. В. Сергеев
✉E-mail: sidorenkoa@yandex.by

Белорусский государственный университет,
пр. Независимости, 4, Минск, 220030, Беларусь

Аннотация

Цели. Целями исследования являются разработка и экспериментальная проверка гибридного алгоритма постквантового шифрования изображений, основанного на 3D-хаотической системе и принципе кубика Рубика.

Методы. Рассмотрены вопросы устойчивости традиционных методов шифрования к атакам с использованием квантовых компьютеров. Для создания криптографически стойкого алгоритма предложено объединить преимущества хаотических систем и квантовых вычислений. Использована новая 3D-хаотическая система на базе модифицированной системы Лоренца для генерации псевдослучайных ключей. Применен принцип кубика Рубика для осуществления операций скремблирования (циклического сдвига строк и столбцов) изображения. Для квантового представления и обработки данных использована модель NEQR (Novel Enhanced Quantum Representation). Реализация алгоритма выполнена на языке Python с применением библиотек Quiskit, OpenCV и NumPy, а также симулятора квантовых вычислений AerSimulator.

Результаты. Разработан гибридный алгоритм шифрования, реализованный в виде компьютерной программы. Алгоритм протестирован на изображениях различного размера и формата. Экспериментально подтверждена устойчивость алгоритма к статистическим и дифференциальным атакам: коэффициент корреляции соседних пикселей зашифрованных изображений близок к нулю, информационная энтропия – к идеальному значению восемь, а значения NPCR (Number of Pixels Change Rate) и PSNR (Peak Signal to Noise Ratio) превышают 99,25 % и составляют менее 13 дБ соответственно.

Заключение. Предложенный гибридный алгоритм демонстрирует высокую криптографическую стойкость и эффективность. Чувствительность к ключам, использование квантовых принципов и оптимизация производительности за счет многопоточности делают его практичным для применения в сферах, критичных к безопасности, таких как IoT, телемедицина и облачные хранилища. Программная реализация работает локально, не требуя подключения к интернету, что обеспечивает безопасность данных.

Ключевые слова: постквантовое шифрование, изображения, хаотические системы, принцип кубика Рубика, квантовые вычисления, модель NEQR, библиотека Qiskit

Для цитирования. Сидоренко, А. В. Постквантовое шифрование на основе хаотической системы и принципа кубика Рубика / А. В. Сидоренко, И. В. Сергеев // Информатика. – 2026. − Т. 23, № 3. – С. 62–75. – https://doi.org/10.37661/1816-0301-2026-23-3-62-75.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Post-quantum image encryption based on a chaotic system and the Rubik's cube principle

Alevtina V. Sidorenko✉, Igor V. Sergeev
✉E-mail: sidorenkoa@yandex.by

Belarusian State University,
av. Nezavisimosti, 4, Minsk, 220030, Belarus

Abstract

Objectives. The aim of the work is the development and experimental verification of a hybrid post-quantum image encryption algorithm based on a 3D chaotic system and the Rubik's cube principle.

Methods. Issues of the vulnerability of traditional encryption methods to attacks using quantum computers are considered. To create a cryptographically robust algorithm, it is proposed to combine the advantages of chaotic systems and quantum computing. A new 3D chaotic system based on a modified Lorenz system is used for generating pseudorandom keys. The Rubik's cube principle is applied to perform image scrambling operations (cyclic shifting of rows and columns). The NEQR (Novel Enhanced Quantum Representation) model is used for quantum representation and data processing. The algorithm is implemented in Python using the Quiskit, OpenCV, and NumPy libraries, as well as the AerSimulator quantum computing simulator.

Results. A hybrid encryption algorithm has been developed and implemented as a computer program. The algorithm was tested on images of various sizes and formats. Resistance to statistical and differential attacks has been experimentally confirmed: the correlation coefficient of adjacent pixels in the encrypted images is close to zero, the information entropy is close to the ideal value of 8, and the NPCR and PSNR values exceed 99,25 % and are less than 13 dB, respectively.

Conclusion. The proposed hybrid algorithm demonstrates high cryptographic strength and efficiency. Key sensitivity, the use of quantum principles, and performance optimization through multithreading make it practical for use in security-critical areas such as IoT, telemedicine, and cloud storage. The software implementation operates locally without requiring an internet connection, which ensures data security.

Keywords: post-quantum encryption, images, chaotic systems, Rubik's cube principle, quantum computing, NEQR model, Qiskit library

For citation. Sidorenko A. V., Sergeev I. V. *Post-quantum image encryption based on a chaotic system and the Rubik's cube principle*. Informatika [*Informatics*], 2026, vol. 23, no. 3, pp. 62–75 (In Russ.). https://doi.org/10.37661/1816-0301-2026-23-3-62-75.

Conflict of interests. The authors declare of no conflict of interest.

Введение

Развитие квантовых вычислений и компьютеров создает беспрецедентную угрозу для современных методов защиты передаваемых данных (информации). Государственная, профессиональная и коммерческая тайны, финансовые и персональные данные – все это перестает быть конфиденциальным, как только злоумышленник получает доступ к мощным квантовым компьютерам. Современные квантовые компьютеры пока не обладают мощностью, достаточной для взлома системы на основе традиционных методов шифрования. С появлением квантовых вычислительных систем возникает необходи-

мость перехода к новым методам криптографии, способным обеспечить надежную защиту в квантовую эпоху [1, 2]. При шифровании же изображений, для которых характерна обработка большого объема графических данных, возникает необходимость перехода к новым методам защиты информации, так как существующие традиционные методы типа RSA (асимметричный алгоритм шифрования) и ECC (криптография на эллиптических кривых) не обладают соответствующими свойствами. Переход на квантовую криптографию связан с необходимостью обновления оборудования, программного обеспечения и обучения специалистов. При использовании же постквантового шифрования, представляющего собой семейство криптографических алгоритмов, устойчивых к атакам со стороны как классических, так и квантовых компьютеров, возникает серьезная проблема совместимости.

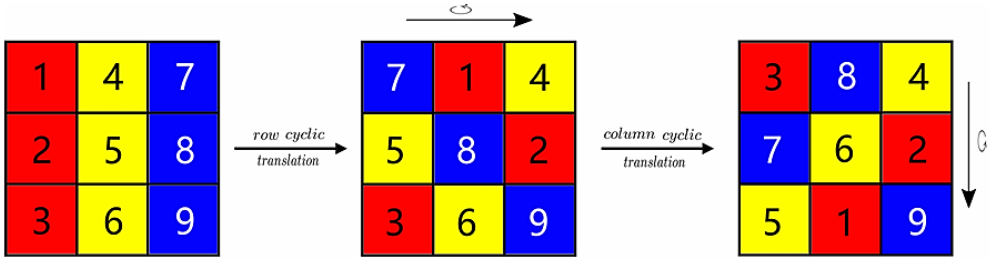
Одним из перспективных инновационных направлений является применение хаотических систем для генерации псевдослучайных ключей и осуществления процедур перемешивания и диффузии данных. Хаотические отображения, такие как отображение кота Арнольда, отображение Хенона и логистическое отображение, уже давно доказали свою совместимость при защите информации благодаря чувствительности к начальным условиям и способности кардинально менять структуру исходных данных даже при незначительных изменениях информационных параметров [3–5].

В данной работе предлагается объединить преимущества квантовой криптографии и хаотических алгоритмов, используя квантовую модель представления изображений и принцип кубика Рубика для реализации эффективного гибридного алгоритма шифрования. Ее целями являются разработка и экспериментальная проверка гибридного алгоритма квантового шифрования изображений, основанного на 3D-хаотической системе (алгоритме) и принципе кубика Рубика.

Алгоритм на основе новой 3D-хаотической системы и принципа кубика Рубика. Принцип кубика Рубика

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

Кубик Рубика представляет собой пластмассовый куб (форм-фактор в первоначальном варианте 3×3×3). Его видимые элементы снаружи выглядят как 54 грани малых кубиков, составляющих один большой куб и способных вращаться вокруг трех внутренних осей куба. Поворачивая строки и столбцы кубика, можно осуществлять циклический сдвиг строк и столбцов. Основываясь на этом, шифрование изображения может быть достигнуто путем циклического перемешивания строк и столбцов в процессе шифрования. Принцип кубика Рубика показан на рис. 1. Циклический перевод строки осуществляется следующим образом. При выполнении циклического сдвига вправо на одну единицу значения в этой строке изменяются от 147 до 714 (рис. 1, *a*, *b*). Аналогично при выполнении циклического сдвига вправо на две единицы во втором ряду (рис. 1, *a*, *b*) значения в этом ряду изменяются от 258 до 582. Циклический сдвиг столбцов заключается в том, что при сдвиге вниз на единицу первого столбца (рис. 1, *b*, *c*) значения в этом столбце изменяются от 753 до 375. Аналогично при циклическом сдвиге на две единицы (рис. 1, *b*) значения в этом столбце изменяются от 186 до 861 (рис. 1, *b*, *c*) [6].



a) *b)* *c)*

Рис. 1. Принцип кубика Рубика
Fig. 1. Rubik's cube principle

Группы пикселей изображения могут рассматриваться как блоки, где каждый из элементов изображения и каждый поворот грани представляет собой линейное или нелинейное преобразование вектора состояния блока. С математической точки зрения поворот грани аналогичен применению матрицы перестановки к множеству векторов, описывающих значения составляющих интенсивностей цвета RGB (R – red (красный), G – green (зеленый), B – blue (голубой)):

$$P' = M \cdot P, \tag{1}$$

где P – исходный набор пикселей, M – матрица поворота грани, P' – результат трансформации.

За счет рекурсивных итеративных перестановок в криптографии принцип кубика Рубика позволяет достигать высокой степени спутанности и рассеивания информации. Спутанность при этом достигается за счет частых перестановок пикселей между блоками, а рассеивание – за счет воздействия на значения цветовых компонентов (в частности, путем побитовой операции XOR с псевдослучайными последовательностями).

Важную роль играют хаотические отображения, применяемые в процессе управления поворотами, например отображение кота Арнольда, логистическое отображение, которые представлены выражениями

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 11 \\ 12 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N, \tag{2}$$

где x, y – координаты пикселя, N – размер изображения, и

$$x_{n+1} = r x_n (1 - x_n), x_n \in (0,1), r \in [3{,}57, 4], \tag{3}$$

где x_n – текущее значение координаты x в двумерном пространстве, r – динамический коэффициент хаоса [6].

Многократное применение выбранного отображения обеспечивает равномерную перестановку пикселей.

Новая 3D-хаотическая система, предложенная для разработки алгоритма

В настоящей работе используется модификация системы Лоренца, выраженная в добавлении нелинейного члена и корреляционных параметров рассматриваемых последовательностей с целью получения новой хаотической системы [7].

Дополнительные нелинейные члены усиливают хаотическое поведение системы, а также дают более высокие значения экспоненты Ляпунова, что делает систему более подходящей для шифрования. Математическую модель аттрактора хаотической системы получаем путем введения параметров a, b, c, d. Математически отображение Лоренца записывается следующим образом:

$$\begin{cases} \frac{dx}{dt} = ay - bxz, \\ \frac{dy}{dt} = -x + cyz, \\ \frac{dz}{dt} = 1 - dy^2. \end{cases} \quad (4)$$

В данной хаотической системе начальное состояние (x_0, y_0, z_0) выбрано (1,01; 0; 0), параметры выбраны a = 1, b = 0,6, c = 47, d = 0,5. Фазовый портрет хаотической системы демонстрирует сложную трехмерную двукрылую структуру с замысловатыми траекториями растяжения и сложения. На рис. 2 изображена фазовая диаграмма предложенной хаотической системы.

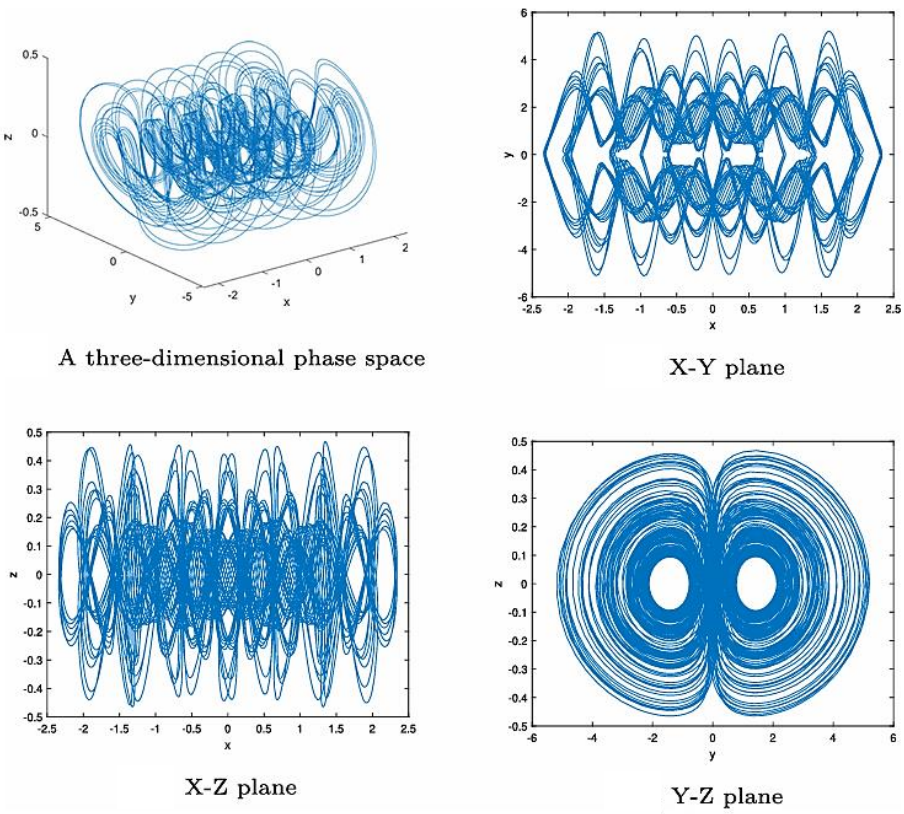


Рис. 2. Фазовая диаграмма 3D-хаотической системы

Fig. 2. Phase Diagram of the 3D-Chaotic System

Предложенная хаотическая система с использованием принципа кубика Рубика

Рассмотрим некоторые аспекты дополнительных сведений, необходимых при разработке алгоритма. Используем изображение размером $M \times N$ в диапазоне серого 2^q. В соответствии с исходным значением ключа (x_1, y_1, z_1) итерируем хаотическую систему (определим, сколько раз был выполнен полный раунд шифрования) 3000 + $M \times N$ раз, чтобы получить три хаотические последовательности X_1, Y_1, Z_1:

$$\begin{cases} X_1 = X(3 = 3001{:}\,3001 + M), \\ Y_1 = Y(3001{:}\,3001 + N), \\ Z_1 = Z(3001{:}\,3001 + M \times N). \end{cases} \quad (5)$$

Для достижения лучшей рандомизации первые 3000 значений отбрасываются. Затем полученные хаотические последовательности преобразуются в псевдослучайные с помощью операции модуляции

$$\begin{cases} K_r = mod(round(X_1 * 10^4), M - 1) + 1), \\ K_c = mod(round(Y_1 * 10^4), N - 1) + 1), \\ K_r = mod(round(Z_1 * 10^4), 2^q), \end{cases} \quad (6)$$

где *mod* обозначает операцию модуляции *Modulus Operation*, описанную в работе [7].

Метод генерации квантового образа ключа

Следует отметить, что рассматриваемый гибридный алгоритм квантового шифрования изображений является постквантовым, а постквантовое шифрование изображения поддерживается целым рядом библиотек, которые лежат в основе других продуктов – от почтовых до веб-серверов и операционных систем. Это позволило при разработке алгоритма использовать модель NEQR, которая является способом представления изображений в квантовых компьютерах для более эффективного хранения и обработки цифровых изображений в квантовом формате. Модель использует ортогональные квантовые состояния для хранения информации о положении пикселя и градациях серого, т. е. информация об изображении может быть точно извлечена. Для получения полутонового изображения $2^n \times 2^n$ в диапазоне серого $[0, 2^q - 1]$ согласно модели NEQP требуется всего $2n + q$ кубитов, где последовательность из $2n$-кубитов представляет положение пикселей изображения, а последовательность из q кубитов – положение для каждого пикселя [8].

Последовательности ключей (K_r, K_c, K_{xor}) преобразуются в квантовые состояния с помощью модели NEQR. Запишем квантовое представление в виде уравнения

$$\begin{cases} K_r\rangle = \frac{1}{\sqrt{2^n}} \sum_{Y_t=0}^{2^n-1} |K_r(Y_t)\rangle \otimes |Y_t\rangle, \\ K_c\rangle = \frac{1}{\sqrt{2^n}} \sum_{X_t=0}^{2^n-1} |K_c(X_t)\rangle \otimes |X_t\rangle, \\ K_{xor}\rangle = \frac{1}{2^n} \sum_{Y_k=0}^{2^n-1} \sum_{X_k=0}^{2^n-1} |K_{xor}(Y_k X_k)\rangle \otimes |Y_k\rangle X_k), \end{cases} \quad (7)$$

где $|Y_t\rangle$, $|X_t\rangle$ – информация о положении ключевого потока; $K_r(Y_t)\rangle$, $K_c(X_t)\rangle$ – значения, полученные при циклическом сдвиге; $K_{xor}\rangle$ – значение для выполнения операции XOR.

Формируется ключевое изображение того же размера, что и скремблированное. Это используется для достижения эффекта диффузии [8].

Принцип кубика Рубика в квантовом изображении

Принцип скремблирования кубика Рубика заключается в достижении эффекта скремблирования путем аналогии игрушки кубик Рубика и циклического перемещения строк и столбцов изображения. В квантовых изображениях достигается эффект циклического сдвига при выполнении модульного сложения над координатными позициями квантового изображения. Для усиления эффекта скремблирования циклический сдвиг строк изображения влево (вправо) и циклический перевод столбцов вверх (вниз) определяются на основе четности значения ключа. Операция циклического сдвига изображения может быть разложена на две разделяемые части: направление X и направление Y. В качестве примера операции циклического сдвига рассмотрим направление X.

При $x \geq K_c$ получаем, что $0 \leq x, K_c \leq 2^n - 1$. Следовательно, выполняется соотношение $0 \leq x - K_c \leq 2^n - 1$ и можно сделать вывод, что $(x - K_c) \cdot mod\ 2^n = b - a$. При $x < K_c$ можно сделать вывод, что $x < K_c \Rightarrow 1 - 2^n \leq x - K_c \leq -1 \Rightarrow 1 \leq 2^n + (b - a) \leq 2^n - 1$. Здесь a и b представляют собой вводимые согласно модели NEQR параметры. Таким образом, выполняется соотношение $(b - a)\ mod\ 2^n = 2^n + (b - a)$. В связи с этим квантовый вычитатель является квантовым вычитателем по модулю 2^n [9].

Для циклического сдвига строки:

– сдвиг вправо

$$|x,y\rangle \rightarrow \left|\left(x + K_r(i)\right) mod\ 2^n, y\right\rangle, \tag{8}$$

– сдвиг влево

$$|x,y\rangle \rightarrow \left|\left(x + K_r(j)\right), y\right\rangle. \tag{9}$$

Для циклического сдвига столбца:

– сдвиг вниз

$$|x,y\rangle \rightarrow \left|\left(x, \left(y + K_c(j)\right) mod\ 2^n\right\rangle, \right. \tag{10}$$

– сдвиг вверх

$$|x,y\rangle \rightarrow \left(y + K_c(j)\right)\rangle. \tag{11}$$

Гибридный алгоритм квантового шифрования изображений

Алгоритм шифрования состоит из нескольких этапов. Прежде чем перейти к описанию алгоритма, остановимся на двух моментах.

Для квантового изображения размером $2^n \times 2^n$ выражение $I_0\rangle$, основанное на модели NEQR, в случае черно-белого изображения имеет вид

$$I_0\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1} C_{YX}\rangle \vee YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}\vee C_{YX}^{i}\rangle \vee YX\rangle, \tag{12}$$

где $C_{YX}\rangle = C_{YX}^{7}C_{YX}^{6} \ldots C_{YX}^{0}\rangle$, $C_{YX}^{i} \in \{0,1\}$.

В рассматриваемом алгоритме оригинальный исходный ключ и ключ изображения представлены с использованием модели NEQR [9].

При описании алгоритма вводится элемент *ITER*, который представляет собой счетчик итераций, т. е. переменную, которая отслеживает, сколько раз был выполнен один полный раунд шифрования.

Гибридный алгоритм шифрования сводится к следующему:

1. Установить количество скремблирований $ITER_{max}$ и инициировать *ITER* на 0: $ITER = 0$.

2. Увеличить счетчик *ITER* на единицу: $ITER = ITER + 1$.

3. Циклически сдвинуть строку i квантового изображения $I_0\rangle$. Если значение $K_r(i)\rangle$ нечетное, то с помощью модуля $CT(+)$ циклически перевести строку j влево на позицию $K_r(i)$. В противном случае используется модуль $CT(-)$, чтобы циклически перевести изображение в i-м ряду вправо на позицию $K_r(i)\rangle$:

$$\langle I_1\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\langle C_{YX}\rangle|X \pm K_r(i))mod\ 2^n\rangle. \quad (13)$$

4. Циклически сдвинуть столбец j квантового изображения $I_0\rangle$. Если значение $K_c(j)\rangle$ нечетное, то с помощью модуля $CT(+)$ циклически сдвинуть строку j в позицию вверх на $K_c(j)$. В противном случае используется модуль CT для циклического сдвига изображения в строке j в позиции вниз на $K_c(j)$:

$$\langle I_{scr}\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\langle C_{YX}\rangle|X \pm K_c(j))mod\ 2^n\rangle \vee X\rangle. \quad (14)$$

Повторив вышеописанные операции, получаем квантовый образ $I_{scr}\rangle$, построенный по принципу кубика Рубика.

5. Выполнить побитовую операцию XOR между скремблированным изображением $I_{scr}\rangle$ и ключевым изображением $K_{x\vee\rangle}$:

$$I_{enc}\rangle = I_{scr}\rangle \otimes \vee K_{x\vee\rangle} =$$
$$= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\langle C_{YX}\rangle mod\ 2^n\rangle|YX\rangle \otimes \sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\langle K_{xor}(Y_kX_k)\rangle \vee Y_kX_k) =$$
$$= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\otimes_{i=0}^{q-1}\vee C_{YX}^i \otimes k_{xor}^i(YX)\rangle \vee YX\rangle. \quad (15)$$

6. Процесс шифрования полностью выполняется до тех пор, пока значение *ITER* не достигнет значения $ITER_{max}$. В противном случае алгоритм переходит к шагу 2.

Поскольку квантовые системы обратимы, процесс дешифрования в такой схеме является обратным процессу шифрования, поэтому не будет описываться дополнительно.

Программная реализация алгоритма на основе хаотической системы и принципа кубика Рубика

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

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

2. Оптимизирован алгоритм обработки изображений с использованием многопоточности, что позволило сократить общее время выполнения процесса шифрования и повысить производительность системы.

3. Созданы квантовые схемы с применением библиотеки Quiskit для представления изображения, осуществления операций трансляции и диффузии, а также моделирования проведения квантовых вычислений на симуляторе AerSimulator.

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

Для реализации алгоритма шифрования с применением языка программирования Python использовались следующие библиотеки:

```
import numpy as np,
import cv2,
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister, transpile,
from qiskit_aer import AerSimulator,
from math import ceil, log2,
import concurrent.futures,
import os.
```

При разработке компьютерной программы авторы использовали следующую конкретизацию:

• numpy (np) – библиотека для работы с массивами, создания ключей и хранения значений изображения.

• cv2 (OpenCV) – библиотека для работы с изображениями. Применяется для чтения изображения и преобразования его в нужные форматы.

• Qiskit – библиотека для создания квантовых схем.

В коде используются QuantumCircuit, QuantumRegister, ClassicalRegister (создание и работа с квантовыми и классическими регистрами) и transpile (преобразование схемы в оптимизированную форму для симуляции или выполнения на реальном квантовом компьютере).

• AerSimulator – симулятор квантовых схем от Qiskit.

• math – функция для математических вычислений (ceil, log2).

• concurrent.futures – обработка блоков изображения параллельно с помощью многопоточности.

• os – число процессоров при многопоточности.

Следует более подробно остановиться на библиотеке Qiskit, разработанной компанией IBM и представляющей собой открытый программный фреймворк для разработки, моделирования и выполнения квантовых алгоритмов. В основе Qiskit лежит модульная архитектура, где каждый компонент отвечает за определенный аспект квантовых вычислений. Базовый модуль Terra обеспечивает функционал для построения и оптимизации квантовых схем, включая их трансляцию в аппаратно-зависимые инструкции. Модуль Aer выступает в роли высокопроизводительного симулятора, который позволяет тестировать алгоритмы в условиях, приближенных к реальным квантовым процессорам, включая моделирование различных видов шумов. Сервис Runtime предназначен для эф-

фективного выполнения квантовых программ непосредственно на физических процессорах IBM[1]. В контексте данного исследования Qiskit была использована как платформа для моделирования и анализа предложенного алгоритма квантового шифрования изображений.

Для определения работоспособности и надежности работы алгоритма проведено тестирование разработанной компьютерной программы на черно-белых и цветных изображениях, имеющих различные размеры. В качестве тестируемых использованы изображения: Babbon.png размером 512×512 пикселей в черно-белом формате, HorizonZero.png размером 250×250 пикселей, Peppers.png размером 435×435 пикселей и Lena.png размером 800×800 пикселей в цветном формате. Как пример рассмотрим тестовое изображение Lena.png размером 800×800 пикселей в цветном формате (рис. 3).

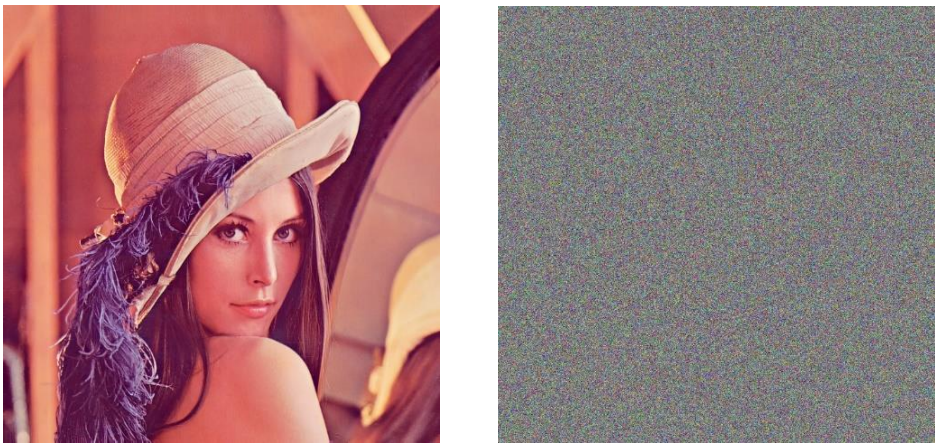


Рис. 3. Оригинальное и зашифрованное изображения Lena.png

Fig. 3. The original and encrypted Lena.png image

На рис. 4 представлены гистограммы интенсивностей цветов оригинального и зашифрованного изображений Lena.png разрешением 800×800 пикселей.

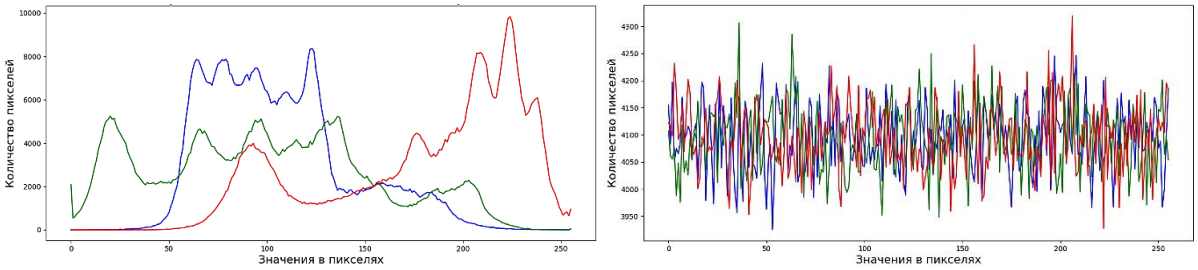


Рис. 4. Гистограммы интенсивностей цветов оригинального и зашифрованного изображений Lena.png

Fig. 4. Color intensity histograms of the original and encrypted Lena.png image

[1]IBN. Accurate Your Development with Qiskit functions. – URL: https://www.ibm.com/quantum (date of access: 18.04.2025).

Проведенный анализ графиков корреляции соседних пикселей оригинальных и зашифрованных изображений (рис. 5) позволил сделать вывод, что при использовании исследуемого алгоритма коэффициент корреляции соседних пикселей близок к нулю. Это усложняет прослеживание закономерностей пикселей.

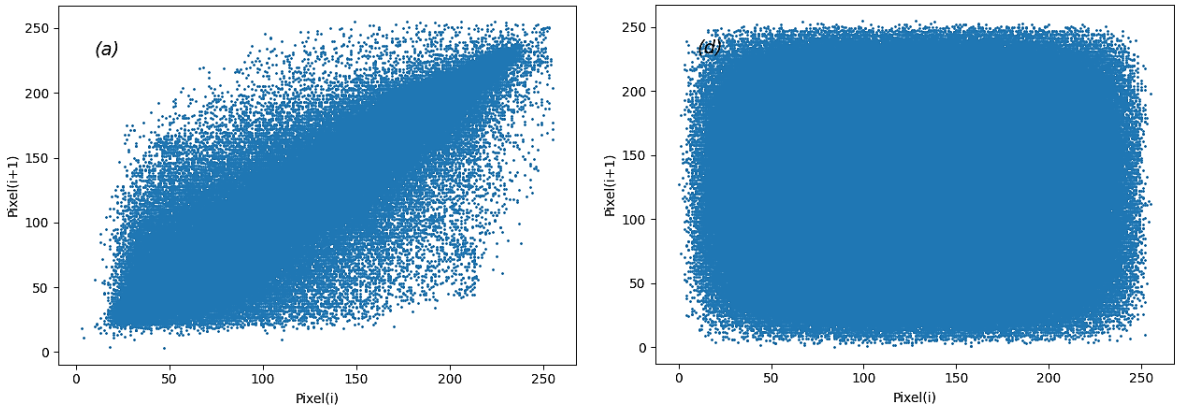


Рис. 5. Корреляция пикселей оригинального и зашифрованного изображений Lena.png
Fig. 5. Pixel correlation of the original and encrypted Lena.png image

Коэффициенты корреляции соседних пикселей, рассчитанных в горизонтальном, вертикальном и диагональном направлениях, для тестируемых и зашифрованных изображений приведены в таблице.

Коэффициенты корреляции оригинальных и зашифрованных изображений
Correlation coefficients of the original and encrypted images

Изображение *Image*	Направление *Direction*		
	горизонтальное *horizontal*	вертикальное *vertical*	диагональное *diagonal*
Baboon оригинальное	0,86345	0,75419	0,72183
Baboon зашифрованное	–0,0020	–0,00142	–0,00142
HorizonZero оригинальное	0,93121	0,93767	0,88818
HorizonZero зашифрованное	0,00481	–0,00559	–0,00220
Lena оригинальное	0,96355	0,97867	0,95300
Lena зашифрованное	0,00095	–0,0030	–0,00120
Peppers оригинальное	0,98971	0,99241	0,98167
Peppers зашифрованное	0,00132	0,00377	0,00399

Как видно из таблицы, для исходных изображений коэффициент корреляции соседних пикселей в трех направлениях близок к единице, а у зашифрованных – к нулю. Это указывает на то, что злоумышленник не может получить статистической информации из гистограмм зашифрованного изображения. Поэтому основанный на анализе гистограмм алгоритм может рассматриваться как устойчивый к статистическим атакам.

Проведенный энтропийный анализ показал, что рассматриваемый алгоритм является устойчивым к атакам, так как информационная энтропия зашифрованного изображения близка к идеальной величине, равной восьми.

Как показал анализ, значения параметров NPCR и PSNR превышают 99,25 % (в первом случае) и ниже 13 дБ (во втором случае). Коэффициент NPCR является общим показателем для оценки качества сжатия, передачи и восстановления изображений. Коэффициент PSNR используется в качестве инструмента для оценки устойчивости к дифференциальной атаке, измеряющей чувствительность пикселей схемы шифрования.

Таким образом, тестирование разработанной компьютерной программы показало наличие стойкости к статистическим и дифференциальным атакам. Предложенный алгоритм эффективен и может быть использован в практических задачах защиты изображений, особенно в сферах, критичных к безопасности, таких как IoT и телемедицина.

Заключение

В работе рассматривается гибридный алгоритм квантового шифрования изображений, основанный на 3D-хаотической системе и принципе кубика Рубика. Описаны ключевые принципы квантовых вычислений, хаотических систем и современных криптографических алгоритмов, что позволило обосновать гибридный подход, объединяющий преимущества квантовой и хаотической криптографии.

Рассмотрены основные принципы квантовой криптографии, включая квантовую суперпозицию и запутывание; проанализированы хаотические системы Лоренца, Хенона, кота Арнольда и их применение для генерации псевдослучайных последовательностей при шифровании. Разработана новая 3D-хаотическая система с улучшенными криптографическими свойствами, связанными с высокой чувствительностью к начальным условиям и сложной фазовой динамикой.

Предложен алгоритм шифрования, сочетающий циклическую трансляцию пикселей (аналогично механике кубика Рубика) и диффузию на основе квантовых операций (CX-гейты). Использована и реализована модель NEQR для кодирования изображений в квантовых системах, обеспечивающая точное восстановление данных. Оптимизирована обработка изображений за счет выполнения операций с применением многопоточности.

Программная реализация алгоритма выполнена на языке Python с использованием библиотек Quiskit, OpenCV и NumPy. Алгоритм поддерживает шифрование изображений произвольного размера с приведением к степени двойки. Проведено тестирование на изображениях различного разрешения (Babbon.png размером 512×512 пикселей в черно-белом формате, HorizonZero.png размером 250×250 пикселей, Peppers.png размером 435×435 пикселей и Lena.png размером 800×800 пикселей в цветном формате), которое подтвердило устойчивость алгоритма к статистическим и дифференциальным атакам. Визуальный и гистограммный анализ показал равномерное распределение пикселей в зашифрованных изображениях, а также отсутствие корреляции между соседними пикселями.

Разработанный алгоритм демонстрирует три ключевых свойства, обеспечивающих практическую ценность и безопасность. Во-первых, он обладает исключительной чув-

ствительностью к ключам: даже минимальные изменения начальных параметров хаотической системы приводят к принципиально разным результатам шифрования, что существенно затрудняет подбор ключей методом перебора. Во-вторых, алгоритм обеспечивает надежную защиту от потенциальных атак с использованием квантовых компьютеров. В-третьих, несмотря на вычислительную сложность квантовых операций, применение оптимизационных подходов, включая блочную обработку данных и многопоточные вычисления, позволило достичь приемлемого уровня производительности, что делает алгоритм пригодным для практического использования. Указанные свойства в совокупности обеспечивают уникальное сочетание криптографической стойкости и работоспособности в реальных условиях.

Вклад авторов. *А. В. Сидоренко* осуществила сбор, анализ и оформление результатов работы и подготовила окончательный вариант статьи. *И. В. Сергеев* предложил концепцию работы и реализовал компьютерную программу гибридного алгоритма квантового шифрования изображений, основанного на 3D-хаотической системе и принципе кубика Рубика.

Список использованных источников

1. Quantum-secured blockchain / E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev [et al.]. – 2018. – URL: https://arxiv.org/pdf/1705.09258 (date of access: 23.03.2026).

2. Belkhir, M. Quantum vs classic computing: A comparative analysis / M. Belkhir, H. Benkaouha, E. Benkhelifa // Proc. of Seventh Intern. Conf. on Fog and Mobile Edge Computing (FMEC 2022), Paris, France, 12–15 Dec. 2022. – Paris, 2022. – URL: https://ieeexplore.ieee.org/document/10062753 (date of access: 23.03.2026). –https://doi.org/10.1109/FMEC57183.2022.10062753.

3. Ahmad, J. A secure image encryption scheme based on chaotic maps and affine transformation / J. Ahmad, S. O. Hwang // Multimedia Tools and Applications. – 2016. – Vol. 75, iss. 21. – P. 13951–13976.

4. Сидоренко, А. В. Алгоритм хеширования на основе SHA-3 с использованием хаотических отображений / А. В. Сидоренко, М. С. Шишко // Информатика. – 2020. − Т. 17, № 1. – С. 109–118. https://doi.org/10.37661/1816-0301-2020-17-1-109-118.

5. Sidorenko, A. V. The use of chaotic maps for image encription / A. V. Sidorenko, I. V. Sergeev // Nonlinear Phenomena in Complex Systems. – 2024. – Vol. 27, no. 4. – P. 404–409. – https://doi.org/10.5281/zenodo.14512115.

6. Loukhaoukha, K. A secure image encryption algorithm based on Rubik′s cube principle / K. Loukhaoukha, J.-Y. Chouinard, A. Berdai // Journal of Electrical and Computer Engineering. – 2012. – Art. 173931. – URL: https://onlinelibrary.wiley.com/doi/10.1155/2012/173931 (date of access: 23.03.2026). – https://doi.org/10.1155/2012/173931.

7. Image encryption scheme based on blind signature and an improved Lorenz system / G. Ye, H. Wu, M. Lin, V. Shi // Expert Systems with Applications. – 2022. – Vol. 205. – Art. 117709. – URL: https://www.sciencedirect.com/science/article/abs/pii/S0957417422009964 (date of access: 23.03.2026). – https://doi.org/10.1016/j.eswa.2022.117709.

8. NEQR: a novel enhanced quantum representation of digital images / Y. Zhang, K. Lu, Y. Gao, M. Wang // Quantum Information Processing. – 2013. – Vol. 12, iss. 8. – P. 2833–2860. – https://doi.org/10.1007/s11128-013-0567-z.

9. Wang, J. Quantum image translation / J. Wang, N. Jiang, L. Wang // Quantum Information Processing. – 2015. – Vol. 14, iss. 5. – P. 1589–1604. – https://doi.org/10.1007/s11128-014-0843-6.

References

1. Kiktenko E. O., Pozhar N. O., Anufriev M. N., Trushechkin A. S., Yunusov R. R., …, Fedorov A. K. *Quantum-secured blockchain*, 2018. Available at: https://arxiv.org/pdf/1705.09258 (accessed 23.03.2026).

2. Belkhir M., Benkaouha H., Benkhelifa E. Quantum vs classic computing: A comparative analysis. *Proceedings of Seventh International Conference on Fog and Mobile Edge Computing (FMEC 2022), Paris, France, 12–15 December 2022.* Paris, 2022. Available at: https://ieeexplore.ieee.org/document/10062753 (accessed 23.03.2026). https://doi.org/10.1109/FMEC57183.2022.10062753.

3. Ahmad J., Hwang S. O. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications*, 2016, vol. 75, iss. 21, pp. 13951–13976.

4. Sidorenko A. V., Shishko M. S. *Hashing technique based on SHA-3 using chaotic maps*. Informatika [*Informatics*], 2020, vol. 17, no. 1, pp. 109–118 (In Russ.). http://doi.org/10.37661/1816-0301-2020-17-1-109-118.

5. Sidorenko A. V., Sergeev I. V. The use of chaotic maps for image encryption. *Nonlinear Phenomena in Complex Systems*, 2024, vol. 27, no. 4, pp. 404–409. https://doi.org/10.5281/zenodo.14512115.

6. Loukhaoukha K., Chouinard J.-Y., Berdai A. A secure image encryption algorithm based on Rubik′s cube principle. *Journal of Electrical and Computer Engineering*, 2012, art. 173931. Available at: https://onlinelibrary.wiley.com/doi/10.1155/2012/173931 (accessed 23.03.2026). https://doi.org/10.1155/2012/173931.

7. Ye G., Wu H., Lin M., Shi V. Image encryption scheme based on blind signature and an improved Lorenz system. *Expert Systems with Applications*, 2022, vol. 205, art. 117709. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0957417422009964 (accessed 23.03.2026). https://doi.org/10.1016/j.eswa.2022.117709.

8. Zhang Y., Lu K., Gao Y., Wang M. NEQR: a novel enhanced quantum representation of digital images. *Quantum Information Processing*, 2013, vol. 12, iss. 8, pp. 2833–2860. https://doi.org/10.1007/s11128-013-0567-z.

9. Wang J., Jiang N., Wang L. Quantum image translation. *Quantum Information Processing*, 2015, vol. 14, iss. 5, pp. 1589–1604. https://doi.org/10.1007/s11128-014-0843-6.

Информация об авторах

Сидоренко Алевтина Васильевна, доктор технических наук, профессор, Белорусский государственный университет.
E-mail: sidorenkoa@yandex.by

Сергеев Игорь Вячеславович, студент, Белорусский государственный университет.
E-mail: sergeevi750@gmail.com

Information about the authors

Alevtina V. Sidorenko, Dr. Sci. (Eng.), Prof., Belarusian State University.
E-mail: sidorenkoa@yandex.by

Igor V. Sergeev, Student, Belarusian State University.
E-mail: sergeevi750@gmail.com