УДК 004.056 ISSN 1995-5499
DOI: https://doi.org/
Поступила в редакцию 09.03.2022
Подписана в печать 22.04.2022

ШИФРОВАНИЕ ТЕКСТА НА ОСНОВЕ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ И ИНФОРМАЦИОННЫХ МАТРИЦ

© 2022 В. Н. Шашихин✉, А. В. Турулин

Санкт-Петербургский политехнический университет Петра Великого
ул. Политехническая, 29, 195251 Санкт-Петербург, Российская Федерация

Аннотация. Актуальность представленной работы обусловлена широким внедрением шифрования данных, включая и текстовые сообщения, в многочисленные сферы как гражданского, так и военного применения. Представлен обзор традиционных методов шифрования текстовой информации и методов, разрабатываемых на основе перспективных направлений (клеточные автоматы, нейронные сети, хаотические отображения). Работа посвящена разработке алгоритма шифрования текста с использованием информационных матриц и систем с детерминированным хаосом. В соответствии с предложенным алгоритмом шифрования исходный текст трансформируется в двумерный массив данных – информационную матрицу. Элементами этой матрицы являются символы текста. Позиция элемента информационной матрицы однозначно связана с позицией символа исходного текста, а значение элемента определяется двоичным кодом символом алфавита открытого текста. Для шифрования информационной матрицы используется трехмерная хаотическая система. Существенная зависимость хаотического отображения от начальных условий и наличие у него свойства транзитивности позволяют обеспечить одновременное перемешивание и рассеивание элементов информационной матрицы. На примере трехмерной хаотической системы Рёсслера исследованы критерии стойкости предложенного алгоритма шифрования к статическому криптоанализу (коэффициенты корреляции между элементами зашифрованной информационной матрицей, энтропия, распределение вероятностей значений элементов) и дифференциальному криптоанализу (процент измененных элементов и среднее изменение интенсивности). Проведенные вычислительные эксперименты показали достаточно хорошие (близкие к теоретически достижимым значениям) критерии стойкости и полное соответствие между дешифрованным текстом и исходным текстом. Вычислительные эксперименты выполнены с использованием разработанных программ на языке Python и Java.
Ключевые слова: текстовые сообщения, алфавит, информационная матрица, хаотические системы, критерии стойкости, критерии качества переданного сообщения.

ВВЕДЕНИЕ

С развитием информационных технологий и широким их внедрением в различные области становиться весьма актуальной проблема обеспечения передачи больших потоков данных различного характера. Среди передаваемых и требующих хранения данных значительную долю занимают текстовые документы.

В настоящее время для шифрования текстовых документов широкое распространение получили традиционные алгоритмы шифрования, например, DES, AES, шифры на основе ГОСТ 28147-89. Однако, эти алгоритмы разрабатывались без учета шифрования в условиях постоянно возрастающих требований к увеличивающемуся объему данных и ограничений на время обработки и передачи [1]. Поэтому возникла необходимость создания новых алгоритмов на основе использования нелинейных функций.

✉ Шашихин Владимир Николаевич
e-mail: shashihin@bk.ru

Одним из перспективных направлений в современной криптографии является разработка и исследование алгоритмов шифрования данных на основе динамического хаоса [2–4], которые позволяют в силу своих свойств (экспоненциальное расхождение траекторий, эргодичность и перемешивание) реализовать алгоритмы, выполняющие одновременно операцию перемешивания и запутывания.

Ведутся исследования по разработке алгоритмов на основе клеточных автоматов в системах симметричного шифрования, а также варианты построения криптосистем с открытым ключом [5–7]. Использование геометрических алгебр Клиффорда с гиперкомплексными числами (кватернионами и октонионами), позволяющими сократить время шифрования, рассматриваются в [8–10]. Строятся и алгоритмы шифрования с использованием фрактальных сортировочных матриц – квадратных матриц из неповторяющихся целых чисел [11].

В [12] рассмотрен метод шифрования текстовых сообщений, базирующийся на существовании для нелинейных отображений периодических возмущений, которые приводят к стабилизации циклов определенного периода и выводу системы на регулярный режим. Информация шифруется с помощью взаимно однозначного соответствия символов текста и устойчивых циклов возмущенного отображения.

В работе представлен алгоритм шифрования, основанный на трансформации исходного текста в информационную матрицу с последующим перемешиванием ее элементов с помощью хаотической системы.

1. ПОСТАНОВКА ЗАДАЧИ

1.1. Модель открытого текста

Открытый текст представляет собой вероятностную модель в виде последовательности знаков $c_1, c_2, ..., c_i, ..., c_m$, в которой каждый знак появляется с вероятностью $p(c_i)$, а вероятность появления данного открытого текста равна

$$p(c_1, c_2, ...c_i, ...c_m) = \prod_{i=1}^{m} p(c_i).$$

Здесь $A(a_1, a_2, ...a_j, ...a_v)$ – алфавит открытого текста. Таким образом, открытый текст рассматривается как реализация стационарного эргодического процесса с дискретным временем и конечным числом состояний.

Открытый текст преобразуется в информационную матрицу, представляющую собой двумерный массив элементов $q(i, j)$, которые характеризуются координатами $i \in \overline{1, N}$ и $j \in \overline{1, M}$. Числа N и M определяют количество строк и количество столбцов информационной матрицы соответственно. Каждый элемент является двоичным числом q из промежутка $[0, 255]$, которое соответствует коду символа алфавита открытого текста. Множество элементов q можно представить как функцию трех переменных:

$$Q = \varphi(i, j, q),$$

или как матрицу следующего вида

$$Q = \begin{bmatrix} q_{11} & q_{12} & \dots & q_{1M} \\ q_{21} & q_{22} & \dots & q_{2M} \\ \dots & \dots & \dots & \dots \\ q_{N1} & q_{N2} & \dots & q_{NM} \end{bmatrix}. \qquad (1)$$

1.2. Модель хаотического отображения

В канонической форме хаотическую систему можно представить как систему дифференциальных уравнений первого порядка

$$\begin{cases} \dot{x}_1 = f_1(x_1, x_2, x_3) \\ \dot{x}_2 = f_2(x_2, x_2, x_3) \\ \dot{x}_3 = f_3(x_1, x_2, x_3) \end{cases} \qquad (2)$$

или как автономное векторное уравнение

$$\dot{x}(t) = F(x(t)), \; x(0) = x_0, \qquad (3)$$

где $x(t) \in \mathrm{R}^n$ – фазовый вектор системы; $F(x(t)) = \left(f_i(x(t))\right)_{i=1}^{n}$ – векторная функция, удовлетворяющая условиям существования решений уравнения (3); $f_i(x(t))$ – вещественные функции, являющиеся компонентами векторной функции; $\dot{x}(t)$ – производная по времени.

Пусть $\mathrm{W} = (X, \rho)$ – метрическое пространство с множеством элементов X и расстоянием ρ. Отображение (векторная функ-

ция) $F(x(t)) : X \to X$ будет хаотическим, если выполняются следующие условия:

1. Отображение $F(x(t))$ обладает существенной зависимостью от начальных данных или сенситивно (если существует такое число $\delta > 0$, что для любого $\varepsilon > 0$ и любой точки $x' \in X$ найдется точка $x'' \in X$ и число $r \in \mathrm{N}$ такие, что $\rho(x', x'') < \varepsilon$, но $\rho(f^{(r)}(x'') - f^{(r)}(x') \geq \delta)$.

2. Отображение $F(x(t))$ транзитивно (для любой пары U, V открытых множеств существует такое $r > 0$, что $F^{(r)}(U) \bigcap V \neq 0$). Транзитивность эквивалентна наличию свойства перемешивания.

1.3. Задача шифрования с использованием хаотического отображения

Требуется получить информационную матрицу $Q^{(l)}$, полученную путём шифрования с применением l раз хаотического отображения $F^{(l)}$ к исходной информационной матрице $Q^{(0)}$:

$$Q^{(0)} \overset{F^{(l)}}{\to} Q^{(l)},$$

где $Q^{(0)}$ определено формулой (1), а отображение F – формулой (2) или (3).

Алгоритм шифрования должен обладать криптографической стойкостью $S = \{S_1, S_2\}$, где S_1 – стойкость к статистическим атакам, S_2 – стойкость к дифференциальным атакам:

$$S_1 = \begin{Bmatrix} \rho_C(p_i^c, p_{i+1}^c) \to 0 \\ H(m^C) \to 8 \end{Bmatrix},$$

$$S_2 = \begin{Bmatrix} NPCR \to 100\% \\ UACI \to 33\% \end{Bmatrix},$$

а $\rho_C(p_i^c, p_{i+1}^c)$ – коэффициент корреляции значений интенсивности между соседними элементами информационной матрицы по горизонтали, вертикали и диагонали; $H(m^C)$ – информационная энтропия; *NPCR* – процент измененных элементов (near pixel change rate), *UACI* – среднее изменение интенсивности (unified averaged changed intensity).

Алгоритм должен обеспечивать совпадение исходного текста и текста, полученного после дешифрования. Совпадение устанавливается путем поэлементного сравнения.

2. АЛГОРИТМ ШИФРОВАНИЯ ТЕКСТА

2.1. Хаотическое отображение

Шифрование текста рассматривается на примере применения трехмерной непрерывной системы Рёсслера [13]

$$\begin{aligned} \dot{x} &= -y - z, \\ \dot{y} &= x + ay, \\ \dot{z} &= b + (x - r)z, \end{aligned} \tag{4}$$

с параметрами равными

$$a = 0,2; \quad b = 0,2; \quad r = 5,7. \tag{5}$$

Особые точки системы (4) с параметрами (5) имеют координаты

$$O_1 = \left(-14,299 \quad 0,708 \quad -286,694\right),$$

$$O_2 = \left(-0,001 \quad 0 \quad -0,014\right),$$

а её характеристические показатели равны

$$\chi_1 = 0,061; \ \chi_2 = 0,018; \ \chi_3 = -5,443.$$

Фазовый портрет системы (4) представлен на рис. 1.

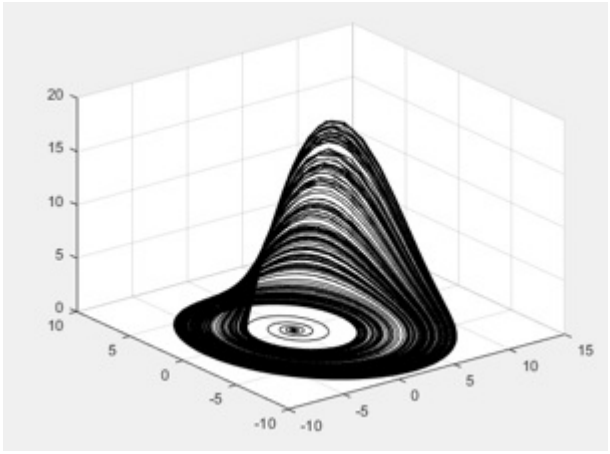


Рис. 1. Фазовый портрет системы Рёсслера [Fig. 1. Phase portrait of the Rossler system]

2.2. Алгоритм шифрования

Алгоритм шифрования и дешифрования текста определяется следующими шагами.

Шаг 1. Текст преобразуется в квадратную информационную матрицу вида (1)

$$Q = (q_{ij})_{i,j=1}^{N,M} \in \mathrm{N}^{N \times M},$$

где i – номер элемента в вертикальном ряду; j – номер элемента в горизонтальном ряду; $q_{i,j}$ – значение элемента в позиции i, j; N – количество строк, а M – количество столб-

цов матрицы символов. В матрице Q каждый элемент соответствует одному символу текста. Размерность матрицы вычисляется исходя из длины текста, округленного в большую сторону, а недостающие элементы заполняются пробелами.

Шаг 2. На основе ключа формируется массив псевдослучайных чисел

$$\mathrm{E} = \{\varepsilon_0, \varepsilon_1, \ldots \varepsilon_c, \ldots \varepsilon_s \,|\, s = N \times M\},$$

который используется для задания начальных условий для третьей компоненты хаотической системы. Здесь $\varepsilon_c \in \mathrm{R}$ и принимает значения из интервала $[0\,;10]$.

Шаг 3. Формируется вектор начальных условий для хаотической системы

$$X(t_0) = (x_1(t_0) = i = 1,\ x_2(t_0) = j = 1,\ x_3(t_0) = \varepsilon_0)$$

и начинается процесс интегрирования уравнений (2). Здесь $x_1(t_0) = i = 1,\ x_2(t_0) = j = 1$ – начальные условия для первой и второй компоненты, которые определяются позицией первого элемента информационной матрицы. Значения первой и второй компоненты вектора состояния системы (3) в момент времени t_1 определяют новое положение элемента информационной матрицы: $i^1 = [x_1(t_1) \bmod M]$ – номер строки и $j^1 = [x_2(t_1) \bmod N]$ – номер столбца. Таким образом производится перемешивание элементов информационной матрицы в процессе первого раунда. Новое значение элемента определяется суммой третьей компоненты хаотической системы и псевдослучайным числом $q_{i,j}^{(1)} = [(x_3(t_1) + \varepsilon_0) \bmod AL]$, что обеспечивает рассеивание элементов. Здесь AL – мощность алфавита открытого текста.

Шаг 4. В результате применения операций третьего шага к каждому элементу исходной информационной матрицы, вычисляется информационная матрица первого раунда шифрования

$$Q^{(1)} = \begin{bmatrix} q_{1,1}^{(1)} & q_{1,2}^{(1)} & \cdots & q_{1,M}^{(1)} \\ q_{2,1}^{(1)} & q_{2,2}^{(1)} & \cdots & q_{2,M}^{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ q_{N,1}^{(1)} & q_{N,2}^{(1)} & \cdots & q_{N,M}^{(1)} \end{bmatrix} \in \mathrm{R}^{N \times M}.$$

Для вычисления следующей точки траектории хаотической системы для каждого элемента информационной матрицы, в качестве вектора начальных условий выбираются две координаты текущего элемента в исходной информационной матрице и очередное число из псевдослучайной последовательности.

Шаг 5. Шаги 3 и 4 повторяются l раз, l – количество раундов шифрования.

Процесс дешифрования аналогичен алгоритму шифрования, но элементы информационной матрицы берутся в обратном порядке и суммирование с псевдослучайным числом заменяется на его вычитание.

Таким образом, шифрование текста, по существу, сводится к генерации хаотической системой при заданных начальных условиях трёх последовательностей

$$\begin{aligned} X_1 &= \{x_1(t_1), \ldots x_1(t_k), \ldots x_1(t_s)\}, \\ X_2 &= \{x_2(t_1), \ldots x_2(t_k), \ldots x_2(t_s)\}, \quad s = N \times M\,. \\ X_3 &= \{x_3(t_1), \ldots x_3(t_k), \ldots x_3(t_s)\}. \end{aligned} \quad (6)$$

Последовательности X_1 и X_2 определяют перемешивание элементов, а последовательность X_3 совместно с последовательностью псевдослучайных чисел – рассеивание (изменения кода) элементов [14].

Здесь каждый член последовательностей (6) формируются по правилу

$$\begin{aligned} \dot{x}_1(t) &= f_1[x(t)], \\ \dot{x}_2(t) &= f_2[x(t)], \Leftrightarrow \dot{x}(t) = F[x(t)], \\ \dot{x}_3(t) &= f_3[x(t)], \end{aligned}$$

где $F[x(t)] = (f_1(x(t), f_2(x(t)\ f_3(x(t))^T$ – векторная функция, компонентами которой являются функции в правой части уравнения (3).

3. ИСЛЕДОВАНИЕ АЛГОРИТМА ШИФРОВАНИЯ

3.1. Критерии стойкости

Для исследования криптографической стойкости алгоритма к статическим атакам используются следующие критерии [15].

Гистограмма. Инвариантная мера значений элементов информационной матрицы определяется вероятностью попадания значений элемента в какой-либо уровень из интервала $s = [0\,;255]$. Для хорошего алгоритма шифрования все значения элементов должны быть равновероятными.

Корреляция. Парная зависимость между двумя соседними элементами исходной или зашифрованной информационной матрицы. Для её выявления вычисляется корреляция по вертикале, горизонтали и диагонали с использованием следующей формулы

$$\rho(u_i, v_{i+1}) = \frac{\frac{\sum_{i=1}^{N\times M}(u_i - \bar{U})(v_{i+1} - \bar{V})}{N\times M}}{\sqrt{\frac{\sum_{i=1}^{N\times M}(u_i - U)^2}{N\times M}}\sqrt{\frac{\sum_{i=1}^{N\times M}(v_{i+1} - V)^2}{N\times M}}} \quad (7)$$

$$\bar{U} = \frac{\sum_{i=1}^{N\times M} u_i}{N\times M},\ \bar{V} = \frac{\sum_{i=1}^{N\times M} v_i}{N\times M},$$

где u_i, v_{i+1} – значение i-го элемента информационной матрицы и соседнего с ним элемента;

$$U = \{u_1, u_2, \dots u_i, \dots u_{N\times M}\},$$
$$V = \{v_1, v_2, \dots v_i, \dots v_{N\times M}\}$$

– ряд значений интенсивности элемента и ряд значений соседних элементов.

Энтропия. Мера неопределенности. Энтропия вычисляется по формуле

$$H(m) = \sum_{s=0}^{2^N-1} P(m_s)\log_2\frac{1}{P(m_s)}, \quad (8)$$

где $P(m_s)$ – вероятность принадлежности элемента матрицы уровню $s \in [0\,;255]$.

В пределе энтропия должна равняться количеству бит, которые отводятся на каждый элемент. На каждый элемент, как правило, выделяется один байт и элемент может принимать значения от 0 до 255, откуда следует, что идеальная энтропия должна равняться 8.

Для оценки криптографической стойкости алгоритма к дифференциальным атакам используются следующие критерии.

Процент измененных элементов (Near Pixel Change Rate). Это процент элементов криптограммы, которые претерпели изменения относительно исходной информационной матрицы или предыдущих криптограмм.

$$NPCR(Q_1, Q_2) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} D(i,j)}{N\times M}\times 100\,\%,$$

$$D(i,j) = \begin{cases} 1, & \text{если } q_1(i,j) = q_2(i,j) \\ 0, & \text{если } q_1(i,j) \neq q_2(i,j) \end{cases} \quad (9)$$

$$\forall i = \overline{1,N},\ \forall j = \overline{1,M},$$

Данная оценка должна стремиться к 100 %, то есть все элементы должны измениться.

Среднее изменение интенсивности (Unified Averaged Changed Int). Мера разницы в значениях элементов двух криптограмм.

$$UACI(Q_1, Q_2) = \frac{1}{N\times M}\times$$
$$\times\sum_{i=1,\ j=1}^{N,\ M}\frac{|q_1(i,j) - q_2(i,j)|}{255}\times 100\,\%, \quad (10)$$

$UACI$ должно стремиться к 33 %, то есть каждый элемент должен изменить своё значение примерно на треть.

Здесь Q_1, Q_2 – исходная информационная матрица и матрица, в котором изменён один элемент; q_1, q_2 – значения элементов исходной и измененной информационной матрицы.

Оценка качества алгоритма шифрования и дешифрования. Одним из наиболее важных свойств любого алгоритма шифрования является показатель потери информации после дешифрования.

Для измерения качества шифрования используется показатель процента измененных элементов исходной матрицы и полученной после дешифрования информационной матрицы.

Качество воспроизведения текста определяется также поэлементным сравнением исходного текста и текста, полученного после дешифрования. Критерием является процент совпадающих символов обоих текстов.

3.2. Результаты исследования алгоритма

Эксперименты по оценке стойкости и качества алгоритма проводились на тексте из литературного источника [16]. Фрагмент текста состоит из 3865 символов и представлен на рис. 2.

Гистограммы исходного текста и зашифрованной информационной матрицы представлены на рис. 3.

Наличие всплесков на криптограмме объясняется тем, что криптограммы соответствуют небольшому количеству раундов шифрования и небольшим значением старшего положительного характеристического показателя Ляпунова хаотической системы,

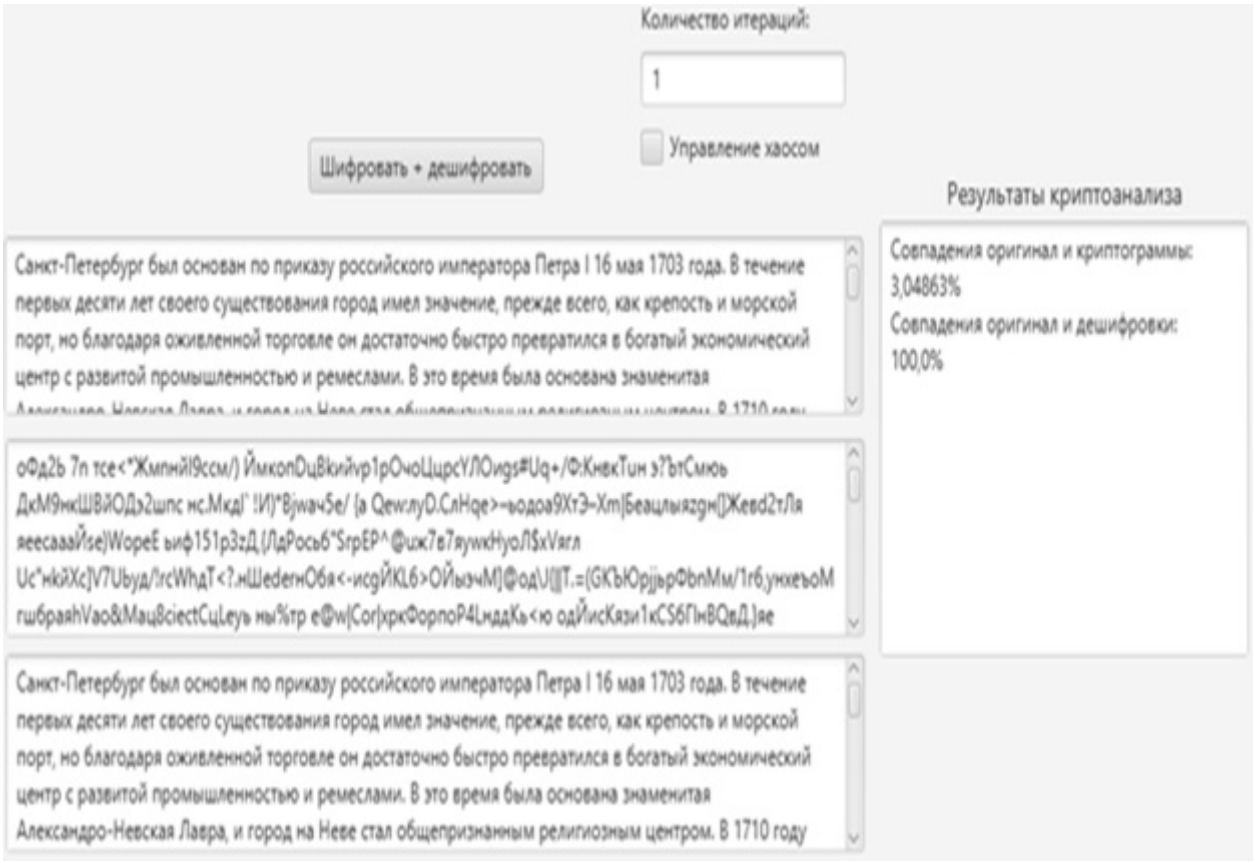
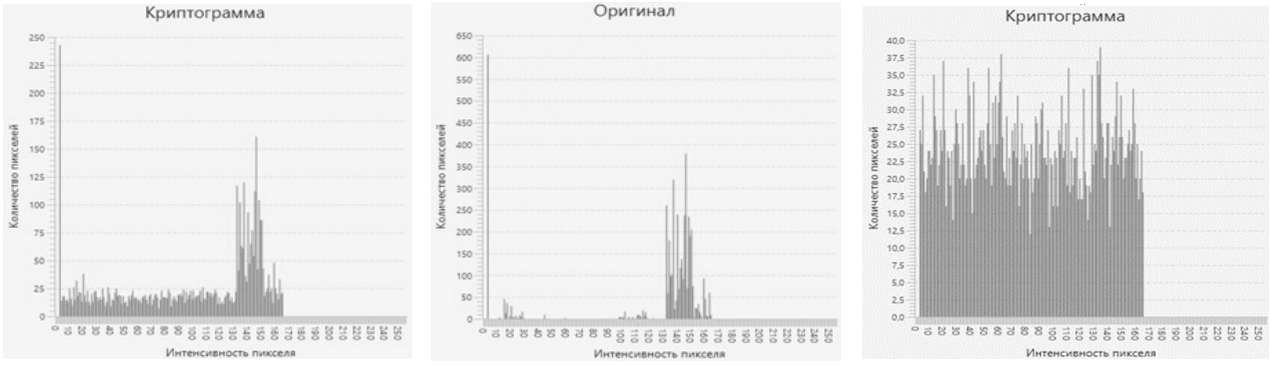


Рис. 2. Фрагмент исходного и дешифрованного текста
[Fig. 2. A fragment of the original and decrypted text]



а) *б)* *в)*

Рис. 3. Гистограммы: (а) открытого текста; (б) зашифрованной информационной матрицы при одном раунде; (в) зашифрованной информационной матрицы при четырех раундах
[Fig. 3. Histograms: (a) plaintext; (b) of the encrypted information matrix in one round; (c) of the encrypted information matrix with four rounds]

который определяет интенсивность перемешивания и рассеивания. По мере увеличения раундов шифрования распределение вероятностей значений элементов выравнивается и приближается к равномерному.

Изображения информационных матриц: исходной, зашифрованной и после дешифрования представлены на рис. 4.

Результаты расчетов критериев стойкости алгоритма с использованием системы Рёссле-

а) *б)* *в)*

Рис. 4. Информационная матрица: (а) исходная; (б) зашифрованная; (в) дешифрованная
[Fig. 4. Information matrix: (a) the original; (b) the encrypted; (c) the de-encrypted

ра по формулам (7)–(10) при четырех раундах шифрования приведены в табл. 1.

Таблица 1. Критерии стойкости алгоритма
[Table 1. Algorithm durability criteria]

Критерии стойкости		Информационная матрица	
		исходная	зашифрованная
Коэффициент корреляции	горизон.	0,071	0,035
	вертик.	0,038	–0,006
	диагон.	$9{,}116\times10^{-4}$	$3{,}687\times10^{-4}$
Энтропия		4,647	7,312
Процент измененных элементов, %		–	99,244
Среднее изменение интенсивности, %		–	26,318

При шифровании информационной матрицы коэффициенты корреляции уменьшаются, принимая в некоторых случаях отрицательные значения, что указывает на обратную связь между элементами зашифрованной информационной матрицы (для двух соседних элементов значения одного элемента могут увеличиваться, а для другого уменьшаться или наоборот).

Значение энтропии увеличивается за счет перемешивания и рассеивания с использованием хаотической системы с положительным старшим характеристическим показателем Ляпунова. Процент измененных элементов и среднее значение интенсивности близки к теоретически достижимым значениям (к 100% и 33%) и могут быть увеличены за счет изменения параметров хаотической системы или введением в неё обратной связи с целью увеличения старшего характеристического показателя.

Вычислительные эксперименты проводились на компьютере с процессором Intel Core i5-11600 при тактовой частоте 2,8 ГГц. Алгоритм шифрования запрограммирован на языке Java. Время выполнения четырех раундов шифрования – дешифрования текста объемом 3865 знаков составило примерно 40 мс. Для текста объемом 700000 знаков при одном раунде время выполнения алгоритма составило примерно 400 мс.

ЗАКЛЮЧЕНИЕ

Разработан алгоритм шифрования текстовых сообщений на основе хаотических систем и информационной матрицы. Информационная матрица строится путем трансформации исходного текста в двумерный массив. Использование хаотической системы позволяет реализовать одновременное перемешивание и рассеивание элементов информационной матрицы. Вычислительные эксперименты подтверждают стойкость разработанного алгоритма к статистическому и дифференциальному анализу.

КОНФЛИКТ ИНТЕРЕСОВ

Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Сидоренко, А. С.* Шифрование изображений на основе хаотических отображений с использованием параллельных вычислений / А. С. Сидоренко, М. С. Шишко // Информатика. – 2017. – № 4. – С. 78–88.

2. *Сидоренко, А. С.* Шифрование изображений на основе хаотической динамики с элементами генетического алгоритма / А. С. Сидоренко, М. С. Шишко // Информатика. – 2018. – № 1. – С. 95–100.

3. *Xiuli, C.* An image encryption algorithm based on chaotic system and compressive sensing / C. Xiuli, Z. Xiaoyu, G. Zhihua // Signal Processing. – 2018. – Vol. 148, No 7. – P. 124–144.

4. *Kaur, M.* Color image encryption using non-dominated sorting generated algorithm with local chaotic search based 5D chaotic map / M. Kaur, D. Singh, K. Sun // Future Generation Computer Systems. – 2020. – Vol. 107, No 6. – P. 333–350.

5. *Hanis, S.* Double image compression and encryption and cellular automata / S. Hanis, R. Amutha // Multimed Tool Appl. – 2018. – No 77. – P. 6897–6912. DOI:10.1007/s11042-017-4606-0.

6. *Zhang, F.* Parallel thinning and skeletonization algorithm based on cellular automation / F. Zhang, X. Chen, X. Zhang // Multimed Tool Appl. – 2020. – No 79. DOI:10.1007/s11042-020-09660-5.

7. *Кулешова, Е. А.* Методы применения клеточных автоматов в системах защиты информации / Е. А. Кулешова // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2021. – № 2. – С. 81–93. DOI:10.17308/sait.2021.2/3506.

8. *Nagase, T.* Dispersion of sequences for generating a robust enciphering system / N. Nagase, R. Roide, N. Araki Y. Yasegawa // Computer and Information Theory. – 2005. – Vol. 1, No 1. – P. 9–14.

9. *Кузнецова, К. С.* Аппаратно-ориентированный алгоритм кватернионной криптосистемы / К. С. Кузнецова, Е. И. Духнич // Известия ЮФУ. Технические науки. – 2018. – Т. 202. – № 8. – С. 182–190.

10. *Чуканов, С. Н.* Передача сигналов с шифрованием методом геометрической алгебры // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2020. – № 3. – С. 25–31. DOI:10.17308/sait.2020.3/3037.

11. *Xian, Y.* Fractal sorting matrix and its application on chaotic image encryption / X. Xian, X. Wang // Information Sciences. – 2021. – Vol. 547. – P. 1154–1169.

12. *Лоскутов, А. Ю.* Использование хаотических отображений для защиты информации / А. Ю. Лоскутов, А. А. Чураев // Вестник Московского университета. Серия 3. Физика. Астрономия. – 2008. – № 2. – С. 15–19.

13. *Rossler, O. E.* An equation for continuous chaos / O. E. Rossler // Physics letters. – 1976. – Vol. 57, No 5. – P. 397–398.

14. *Shashihin, V. N.* Image encryption algorithm based on controlled chaotic maps / V. N. Shashihin, A. V. Turulin, C. V. Budnik // Computing, Telecommunications and Control. – 2021. – Vol. 14, No 1. – P. 7–21. DOI:10.18721/JCST-CS.14404

15. *Сидоренко, А. В.* Элементы дифференциального и линейного криптоанализа алгоритма шифрования с использованием динамического хаоса / А. В. Сидоренко, Д. А. Жуковец // Системный анализ и прикладная информатика. – 2015. – № 3. – С. 48–56.

16. Историческая справка о городе / Экономический форум в Санкт-Петербурге. – Режим доступа: https://forumspb.com/o-sankt-peterburge/history

Шашихин Владимир Николаевич – д-р тех. наук, проф., профессор высшей школы киберфизических систем и управления института компьютерных наук и технологий Санкт-Петербургского политехнического университета Петра Великого.
E-mail: shashihin@bk.ru
ORCID iD: https://orcid.org/0000-0002-3718-9623

Турулин Александр Владимирович – магистрант 2-го года обучения высшей школы киберфизических систем и управления института компьютерных наук и технологий Санкт-Петербургского политехнического университета Петра Великого.
E-mail: sanya.turulin.98@list.ru
ORCID iD: https://orcid.org/0000-0001-7988-0132

DOI: https://doi.org/ ISSN 1995-5499
Received 09.03.2022
Accepted 22.04.2022

TEXT ENCRYPTION BASED ON CHAOTIC MAPPINGS AND INFORMATION MATRICES

© 2022 V. N. Shashikhin✉, A. V. Turulin

Peter the Great St. Petersburg Polytechnic University
29, Politechnicheskaya Street, 195251 Saint Petersburg, Russian Federation

Annotation. The relevance of the work is due to the widespread implementation of data encryption, including text messages, in numerous areas of civil and military applications. A review of traditional methods of encryption of textual information and methods developed based on promising development directions (cellular automata, neural networks, chaotic mapping) is presented. The work is devoted to developing an algorithm for text encryption using information matrices and systems with deterministic chaos. Following the proposed encryption algorithm, the original text is transformed into a 2D array of data – the information matrix. The elements of this matrix are the text characters. The position of the information matrix element is uniquely related to the position of the source text character, and the value of the element is determined by the binary code of the open text alphabet character. A 3D chaotic system is used to encrypt the information matrix. The essential dependence of the chaotic mapping on the initial conditions and its transitivity property allows for simultaneous mixing and diffusion of the information matrix elements. By the example of Ressler's 3D chaotic system, we investigated the stability criteria of the proposed encryption algorithm to static cryptanalysis (correlation coefficients between the elements of the encrypted information matrix, entropy, probability distribution of element values) and differential cryptoanalysis (percentage of changed elements and the average change of intensity). The computational experiments showed sufficiently good (close to theoretically achievable values) stability criteria and 100 % correspondence between the decoded text and the original text. Computational experiments were performed using the developed programs in Python and Java.
Keywords: text messages, alphabet, information matrix, chaotic systems, persistence criteria, quality criteria of the transmitted message.

✉ Shashikhin Vladimir N.
e-mail: shashihin@bk.ru

CONFLICT OF INTEREST

The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.

REFERENCES

1. *Sidorenko A. S. and Shishko M. S.* (2017) Image encryption based on chaotic mappings using parallel computing. *Informatics*. 4. P. 28–38.

2. *Sidorenko A. S. and Shishko M. S.* (2018) Image encryption based on chaotic dynamics with elements of genetic mapping algorithm using parallel computing. *Informatics*. 1. P. 95–100.

3. *Xiuli C., Xiaoyu Z. and Zhihua G.* (2018) An image encryption algorithm based on chaotic system and compressive sensing. *Signal Processing*. 148(7). P. 124–144.

4. *Kaur M., Singh D. and Sun K.* (2020) Color image encryption using non-dominated sorting generated algorithm with chaotic local search based 5D chaotic map. *Future Generation Computer Systems*. 107(6). P. 333–350.

5. *Hanis S. and Amutha R.* (2018) Double image compression and encryption and cellular automata. *Multimed Tool Appl.* 77. P. 6897–6912. DOI:10.1007/s11042-017-4606-0.

6. *Zhang F., Chen X. and Zhang X.* (2020) Parallel thinning and skeletonization algorithm based on cellular automation. *Multimed Tool Appl*. 79. DOI:10.1007/s11042-020-09660-5.

7. *Kuleshova E. A.* (2021) Methods of applying cellular automata in information protection systems. *Bulletin of Voronezh State University. Ser. System analysis and information technology*. 2. P. 81–93. DOI:10.17308/sait.2021.2/3506.

8. *Nagase T., Roide R., Araki N. and Yasegawa Y.* (2005) Dispersion of sequences for generating a robust enciphering system. *Computer and Information Theory*. 1(1). – P. 9–14.

9. *Kuznetsova K. S. and Dukhnich E. I.* (2018) Hardware-oriented algorithm of the quaternion cryptosystem. *SFU Izvestiya. Technical sciences*. 202(8). P. 182–190.

10. *Chukanov S. N.* (2020) Signal transmission with encryption by geometric algebra method. *Bulletin of Voronezh State University. Ser. System analysis and information technology*. 3. P. 25–31. DOI:10.17308/sait.2020.3/3037.

11. *Xian Y. and Wang X.* (2021) Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*. 547. P. 1154–1169.

12. *Loskutov A. Yu. and Churaev A. A.* (2008) Using chaotic mappings for information protection. *Bulletin of the Moscow University. Series 3. Physics. Astronomy*. 2. P. 15–19.

13. *Rossler O. E.* (1976) An equation for continuous chaos. *Physics letters*. 57(5). P. 397–398.

14. *Shashikhin V. N., Turulin A. V. and Budnik C. V.* (2021) Image encryption algorithm based on controlled chaotic maps. *Computing, Telecommunications, and Control*. 14(1). P. 7–21. DOI:10.18721/JCST-CS.14404

15. *Sidorenko A. V. and Zhukovets D. A.* (2015) Elements of differential and linear cryptanalysis of encryption algorithm using dynamic chaos. *System analysis and applied informatics.* 3. P. 48–56.

16. Historical information about the city. Economic Forum in St. Petersburg. Available at: https://forumspb.com/o-sankt-peterburge/history

Shashikhin Vladimir N. – Doctor of Technical Sciences, Professor, Professor of the Higher School of Cyber-Physical Systems and Control at the Institute of Computer Science and Technology, Peter the Great St. Petersburg Polytechnic University.
E-mail: shashihin@bk.ru
ORCID iD: https://orcid.org/0000-0002-3718-9623

Turulin Alexander V. – 2nd-year master's student of the Higher School of Cyberphysical Systems and Control at the Institute of Computer Science and Technology, Peter the Great St. Petersburg Polytechnic University.
E-mail: sanya.turulin.98@list.ru
ORCID iD: https://orcid.org/0000-0001-7988-0132