ШИФРОВАНИЕ ИЗОБРАЖЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ ХАОТИЧЕСКОЙ ДИНАМИКИ И ЭЛЕМЕНТЫ ЛИНЕЙНОГО КРИПТОАНАЛИЗА

М. С. Шишко

ВВЕДЕНИЕ

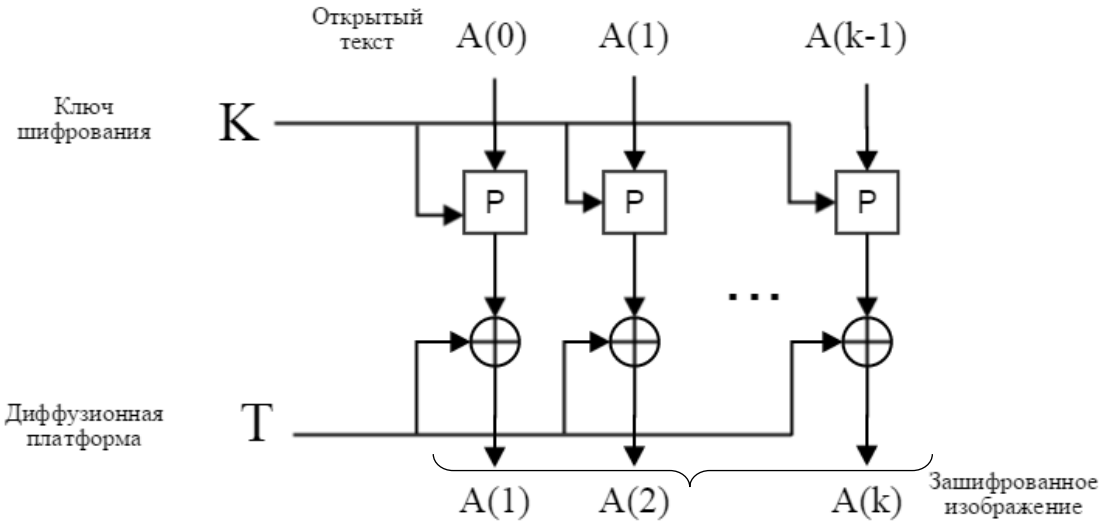
Широкое распространение информационных технологий практически во всех сферах жизнедеятельности человека способствует появлению новых задач, связанных с обеспечением необходимой степени защиты информации. Интернет и мобильная связь, являясь привлекательными направлениями для передачи информации, не могут гарантировать должную степень защиты и конфиденциальности данных.

Среди разнообразных методов защиты информации и обеспечения ее целостности выделяются криптографические методы. Одним из перспективных направлений в современной криптографии является разработка алгоритмов шифрования на основе динамического хаоса. Использование же криптографических средств в практически реализуемых системах неразрывно связано со стойкостью алгоритмов шифрования. При традиционном подходе стойкость алгоритма шифрования определяется стойкостью к известным видам криптографических атак, применяемых с целью прочтения, замены зашифрованного сообщения или вычисления ключа шифрования. К наиболее популярным методам криптоанализа относятся: статистический, дифференциальный и линейный криптоанализ. Линейный криптоанализ исследует возможности взлома алгоритма шифрования на основе изучения закономерностей в парах открытого текста и шифротекста. Как правило, при этом известен алгоритм шифрования, а также имеется достаточное количество пар открытого текста и шифротекста, но не известен ключ шифрования.

Целью данной работы является построение алгоритма шифрования изображения с использованием динамического хаоса и проведение линейного криптоанализа компонент шифра.

АЛГОРИТМ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ХАОСА

В предлагаемой работе рассматривается и анализируется перестановочно-диффузионный алгоритм шифрования [1]. Хаотическое отображение используется как для перестановки пикселей, так и для рассеяния. В качестве ключа используются начальные условия и параметр хаотического отображения, а также количество циклов перестановки-рассеяния. Для зашифрования и расшифрования используется один и тот же ключ, поэтому шифр является симметричным. Схема алгоритма представлен на рис. 1.



*Перестановка (*р) и рассеяние (XOR – ⊕)

Рис. 1. Схема алгоритма

На стадии перестановки сначала производится смещение цветовых компонент изображения: красной – по горизонтали, зеленой – по вертикали. Затем происходит перестановка компонент пикселей одной строки. Новая позиция компоненты генерируется с помощью двумерного отображения Кота Арнольда [2]:

$$y' = (y + p * z) \bmod M \quad (1)$$

$$z' = (y * q + (p * q + 1) * z) \bmod 3 \quad (2)$$

Далее производится перестановка компонент пикселей в пределах всего изображения с помощью трехмерного отображения Кота Арнольда (3) и трехмерного Стандартного отображения (4) [2,3]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a_z & 0 \\ b_z & a_z b_z + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & a_y \\ 0 & 1 & 0 \\ b_y & 0 & a_y b_y + 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a_x \\ 0 & b_x & a_x b_x + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod \begin{bmatrix} M \\ N \\ 3 \end{bmatrix} \quad (3)$$

$$\begin{cases} x_{n+2} = (\llbracket x \rrbracket_{n+1} + y_{n+1}) \bmod M \\ y_{n+2} = (y \rrbracket_{n+1} + z_{n+1} + K_1 \sin \llbracket x_{n+1}) \bmod N \\ z_{n+2} = (z \rrbracket_{n+1} + K_1 \sin x_{n+1} + K_2 \sin \llbracket y_{n+1}) \bmod 3 \end{cases} \quad (4)$$

$$I'(x_{n+2}, y_{n+2}, z_{n+2}) = I(x, y, z) \quad (5)$$

После перестановки происходит рассеяние, которое представляет собой сумму по модулю два преобразованного изображения и диффузионной платформы. Диффузионная платформа вначале имеет вид градиентного изображения размерами, совпадающими с шифруемым изображением. Однако перед рассеянием осуществляется перестановка ее компонент с помощью трехмерного стандартного отображения (4).

ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ

Метод линейного криптоанализа впервые был предложен в начале 90-х гг. XX в. японским ученым М. Матсуи (Matsui) [4]. Для оценки стойкости алгоритма к линейному криптоанализу нами разработана программа на языке C++, реализующая рассматриваемый алгоритм. Программа позволяет построить статистические аналоги для хаотических отображений и оценить вероятность их выполнения. Оценка проводилась для 10 различных наборов параметров для каждого отображения. В таблице 1 приведены усредненные результаты для 10 различных наборов параметров отображений. Параметры, позволяющие оценить стойкость к линейному криптоанализу:

$N_{0.3}$ – Количество аналогов с отклонением вероятности большим 0.3.

η_{max} – Максимальное отклонение.

$N_{\max}$ – Количество использованных бит в аналоге с максимальным отклонением.

$u + v$ – Общее количество бит во входных и выходных данных.

N_{avg} – Среднее количество использованных бит в аналогах с отклонением больше 0.3.

Таблица

Параметры отображений

Хаотическое Отображение	$u + v$	$N_{0.3}$	N_{avg}	$\eta_{\max}$	N_{max}
Двумерное Кота Арнольда	11	44	5,4	0,41	8
Трехмерное Кота Арнольда	12	29	4,8	0,44	11
Трехмерное Стандартное	12	92	6,5	0,44	9

Как видно из таблицы, максимальное отклонение у всех отображений при большом проценте использованных бит достаточно велико. Однако успешный взлом шифра затрудняет тот факт, что статистический аналог, полученный в результате линейного криптоанализа,

будет эффективен для нахождения только одного ключа. С учетом того, что количество бит на входе и на выходе хаотических отображений в данном случае зависит от размера изображения, для больших размеров сложность анализа многократно возрастает. Отсюда следует, что алгоритм обладает умеренной стойкостью к линейному криптоанализу.

ЗАКЛЮЧЕНИЕ

В результате проведенной работы был реализован алгоритм шифрования изображений на основе динамического хаоса, а также реализо-

вана оценка стойкости данного алгоритма к линейному криптоанализу. Оценка показала приемлемый уровень стойкости к линейному криптоанализу.

Литература

1. *Gupta K.* New Approach for Fast Color Image Encryption Using Chaotic Map / Silakari S. // Journal of Information Security – 2011 –Vol. 2 – Pages 139–150
2. *Chen G.* A symmetric image encryption scheme based on 3D chaotic cat maps / Mao Y., Chui C. // Chaos, Solitons and Fractals – 2004 – Vol. 21 – pp. 749–761
3. *Lian S.* A block cipher based on a suitable use of the chaotic standard map / Sun J., Wang Z. // Chaos, Solitons and Fractals – 2005 – Vol. 26 – pp. 117–129
4. *Matsui M.*, Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology – 1998–386 p.