УДК 004.056

АНАЛИЗ АЛГОРИТМОВ ХАОТИЧЕСКОГО ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ

БОЛТЕНКОВ В.А., НИКОЛЬСКИЙ Е.С.

Одесский национальный политехнический университет

ANALYSIS OF ALGORITHMS FOR CHAOTIC IMAGES ENCRYPTING

BOLTENKOV V.A., NIKOLSKY E.S.

Odessa National Polytechnical University

Аннотация. *Исследованы шифры на основе детерминированного хаоса. Исследование показало, что при шифровании изображений шифры достаточно легко реализуются программно на основании логистических динамических систем. Промоделирован и исследован алгоритм Лиу-Сун-Ксу. Предложен и протестирован усовершенствованный алгоритм с четырьмя логистическими хаотическими системами. Усовершенствованный алгоритм в процессе тестирования показал существенно лучшие характеристики стойкости.*

Abstract. . *The ciphers on the basis of the determined chaos have been studied. Research has shown that at enciphering of images using such ciphers are easily enough realized as program on the basis of logistical dynamic systems. The algorithm of Liu-Sun-Xu has been simulated and investigated. The advanced algorithm with four logistical chaotic systems is offered and tested. The advanced algorithm in the course of testing has shown essentially best characteristics of firmness.*

ВВЕДЕНИЕ И ПОСТАНОВКА ЗАДАЧИ

Криптографические методы защиты информации при ее передаче и хранении остаются наиболее надежными и стойкими по отношению к атакам различного рода. Наряду с традиционными алгоритмами шифрования, который разрабатываются и совершенствуются постоянно [1], все большую популярность в криптографическом сообществе приобретают алгоритмы шифрования на основе систем детерминированного хаоса [2]. Теория хаоса начала разрабатываться в 1970-х годах во многих исследовательских областях, таких как физика, математика, инженерия, биология, и в конечном итоге получила законченное развитие в работах по синергетике. Напомним, что системами детерминированного хаоса называются динамические системы с экспоненциальной зависимостью от начальных условий, т.е. небольшое изменение начального состояния системы приводит к существенному изменению всей траектории системы на фазовой плоскости. Изменение в начальных условиях экспоненциально усиливается во времени. С середины 1990-х годов многие исследователи заметили, что существует тесная связь между хаосом и криптографией [2]. Как в криптографии, так и в хаотических системах осуществляется нелинейное преобразование информации. С одной стороны это преобразование абсолютно детерминировано (он аппаратно или программно осуществляется компьютерными средствами), с другой стороны, оно является практически непредсказуемым для внешнего наблюдателя, что и требуется в криптосистемах. Проявляющиеся внешне свойства хаоса, такие как эргодичность, квазислучайность, сильная зависимость от начальных условий и системных параметров, делает хаотическую динамику новой многообещающей альтернативой для стандартных криптографических алгоритмов. Существует два основных способа для разработки цифровых хаотических шифров:

1) Использование хаотических систем для генерации псевдослучайного ключа, который далее применяется для шифрования открытого текста; это направление соответствует потоковым шифрам;

2) Использование открытого текста и/или секретного ключа как начальных условий и/или управляющих параметров для итеративного применения хаотической системы для получения шифртекста; это направление соответствует блочным шифрам.

Несмотря на большой интерес к криптосистемам на базе детерминированного хаоса, их характеристики криптостойкости практически не исследовались. Целью настоящей работы является исследование одного из популярных алгоритмов шифрования изображений – алгоритма Лиу-Сун-Ксу и его усовершенствование.

БАЗОВЫЙ АЛГОРИТМ ЛИУ-СУН-КСУ ЕГО АНАЛИЗ И УСОВЕРШЕНСТВОВАНИЕ

Рассмотрим алгоритм, взятый в качестве базового для потокового шифрования изображений [3]. Алгоритм построен на псевдослучайном генераторе ключа, который базируется на двух хаотических системах. В качестве хаотической системы в алгоритме используется популярная логистическая парабола М. Фейгельбаума (M. Feigenbaum) [2], итерационная функция, которой задается соотношением:

$$x_{n+1} = ax_n(1-x_n),$$

здесь x_n — значение параметра системы на шаге n, начальное состояние системы задается значением $x_0 \in (0,1)$, $a \in (3{,}5699;4]$ — системный управляющий параметр. В зависимости от значения a динамика системы существенно изменяется. Выбор a в заданных пределах гарантирует хаотическое состояние системы, и выходная последовательность x_n имеет высокую степень случайности. Логистическая система Фейгенбаума очень простым путем порождает временной ряд, который кажется псевдослучайным. Особо отметим простоту реализации логистической динамической системы. Схема базового алгоритма приведена на рис.1.

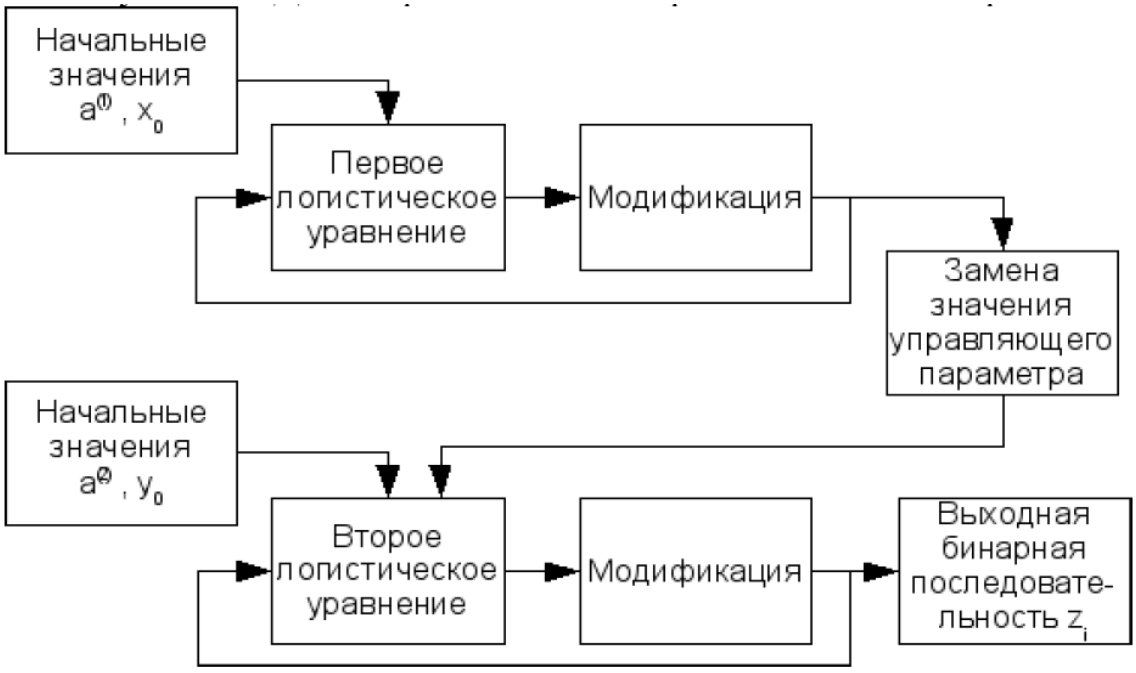

Рисунок 1 - Схема базового алгоритма

Как видно из рисунке 1, две логистические хаотические системы используют одинаковый итеративный принцип с разными начальными значениями. Первая система генерирует случайные числа для обновления параметров второй, пока соблюдаются

определённые условия. Система генерации ключа использует две логистические хаотические системы:

$$x_{n+1} = a^{(1)} x_n (1 - x_n) \ ; \ \ y_{n+1} = a^{(2)} y_n (1 - y_n) .$$

С помощью первой логистической системы формируется вещественное число x_n, которое далее преобразуется в свое двоичное представление X_n. Простой вариант преобразования двоичного числа x_n в дискретный битовый символ X_n реализуется с помощью формулы:

$$x_n = 0, b_{n1} b_{n2} ... b_{nL} = 2^{-1} b_{n1} + 2^{-2} b_{n2} + ... + 2^{-L} b_{nL} .$$

X_n образуется как последовательность бит $\{ b_{n1}, b_{n2}, ..., b_{nL} \}$. Далее ключ генерируется так. С помощью первой логистической системы генерируется вещественное число x_n, которое преобразуется в бинарное представление X_n при $L = 45$. Далее вычисляется число $X'_{n+1} = \{ b_1 ... b_{15} \} \oplus \{ b_{16} ... b_{30} \} \otimes \{ b_{31} ... b_{45} \}$, здесь значком $\oplus$ обозначена операция XOR. Представим X'_{n+1} как последовательность $\{ p_1 ... p_{15} \}$. X'_{n+1} преобразуется в вещественное число x'_{n+1} по соотношению:

$$x'_{n+1} = 2^{-1} p_1 + 2^{-2} p_2 + ... + 2^{-15} p_{15} .$$

Затем вычисляется $x''_{n+1} = x'_{n+1} * 10$. Если $x''_{n+1} \in (3{,}5699; 4]$ и количество итераций после предыдущего обновления $a^{(2)}$ больше или равно 100, то x''_{n+1} используется для обновления параметра $a^{(2)}$ второй логистической системы. Преобразование данных во второй логистической системе аналогично. Схема генерации ключа приведена на рис.2.

Алгоритм шифрования и расшифрования изображений выглядят так. Изображение преобразуется в поток бинарных данных. На него накладывается в качестве гаммы псевдослучайная последовательность ключа и образуется зашифрованное изображение. Как ясно из изложенного выше, поведение двух логистических систем определяется значениями $(a^{(1)}, x_0, a^{(2)}, y_0)$. Эти значения и являются ключом шифрования. Дешифрование, как и во всех потоковых шифрах гаммирования, осуществляется аналогично благодаря обратимости операции XOR.

Базовый алгоритм был исследован на различных изображениях с помощью программы, разработанной по алгоритмам, представленным на рис.1, 2. В качестве количественной меры криптостойкости шифра использовался коэффициент корреляции по смежным пикселям изображения [4]:

$$C_p = \frac{N \sum_{j=1}^{N} x_j y_j - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j}{\sqrt{\left\{ N \sum_{J=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j \right)^2 \right\}} \sqrt{\left\{ N \sum_{J=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j^2 \right)^2 \right\}}},$$

где x, y - значения градаций серого двух смежных пикселей изображения, N - число пикселей изображения, выбранных для расчета коэффициента корреляции.

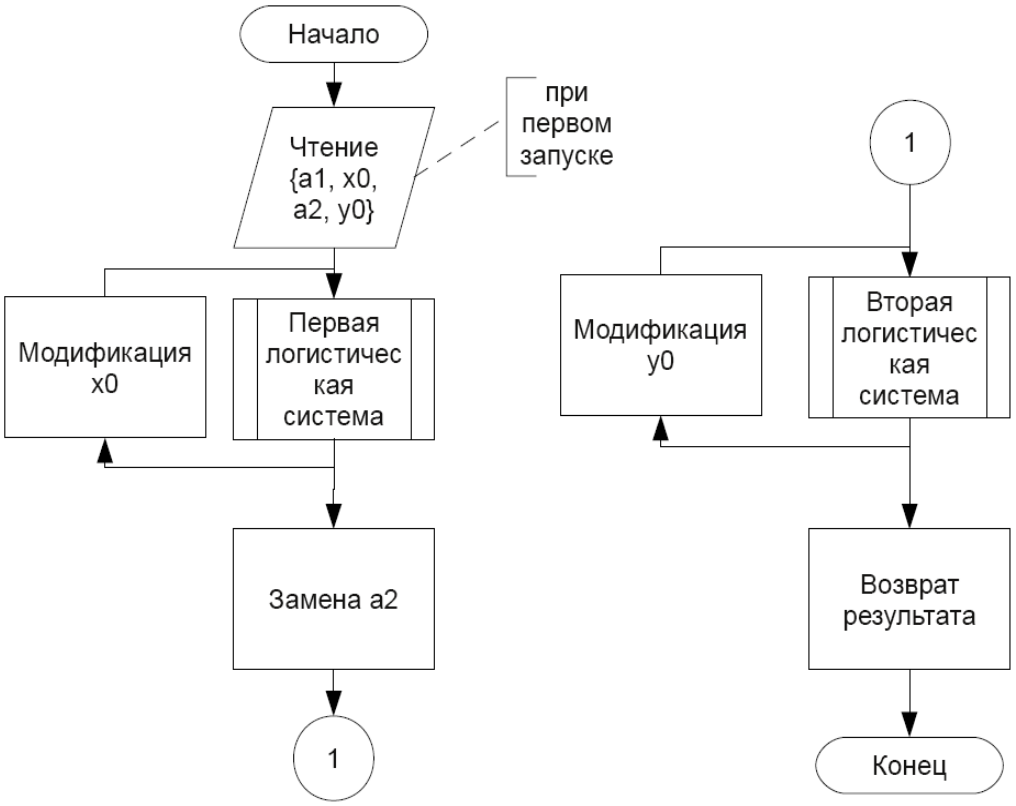

Рисунок 2 - Схема генерации ключа

По последнему соотношению рассчитывались коэффициенты корреляции (КК) различных изображений для исходного и зашифрованного их представления. Если для исходного изображения КК лежит в пределах 0,95-0,98, то для зашифрованных изображений его значения составляют 0,1-0,12. Эти значения указывают на невысокую криптостойкость базового алгоритма. Поэтому алгоритм был усовершенствован путем добавления в него еще двух логистических систем, функционирующих по описанной выше схеме. Схема усовершенствованного алгоритма приведена на рис.3.

Тестирование усовершенствованного алгоритма показало, что КК зашифрованных изображений для тех же тестов, которые применялись в базовом алгоритме, не превосходит значений 0,03-0,032. Таким образом, криптостойкость алгоритма существенно повышена.

На рисунке 4 показан интерфейс программы шифрования и тестирования. Левое поле представляет исходное изображение, среднее поле – зашифрованное изображение, правое поле – расшифрованное изображение. В левом нижнем углу выведен рассчитанный КК.

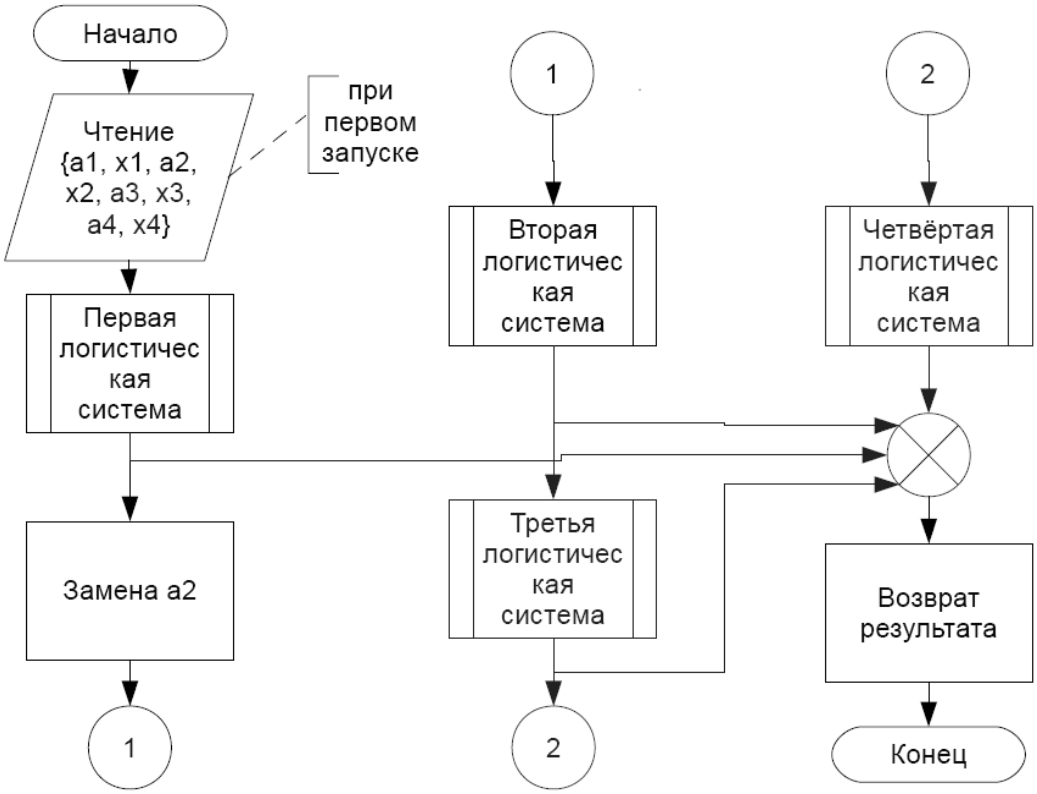

Рисунок 3 - Схема усовершенствованного алгоритма с четырьмя логистическими динамическими системами

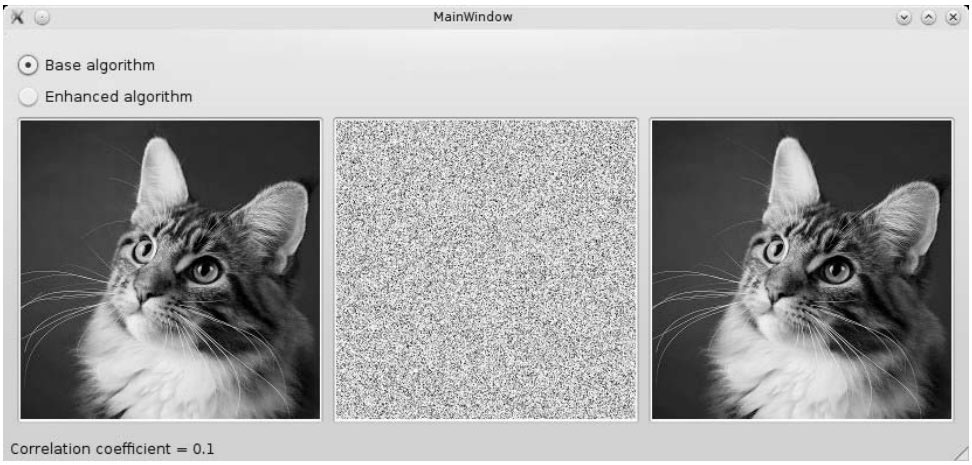

Рисунок 4 - Интерфейс программы шифрования и тестирования

ВЫВОДЫ

Исследование шифров на основе детерминированного хаоса показало, что при шифровании изображений шифры достаточно легко реализуются программно (а, в принципе могут быть реализованы и аппаратно) на основании логистических динамических систем. Разработано программное средство, реализующее алгоритм Лиу-Сун-

Ксу. Его тестирование показало невысокую криптостойкость алгоритма, оцененную по коэффициенту корреляции смежных пикселей. Предложен и протестирован усовершенствованный алгоритм с четырьмя логистическими хаотическими системами. Усовершенствованный алгоритм в процессе тестирования показал существенно лучшие характеристики стойкости.

В качестве направления дальнейших исследований планируется провести оценки криптостойкости алгоритмов с хаотическим шифрованием по числу операций, необходимых для вскрытия ключа.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Бабаш А.В., Шанкин Г.П. Криптография – М.: Солон-пресс, 2007. – 512 с.
2. Птицын Н.В. Приложение теории детерминированного хаоса в криптографии – М.: Изд. МГТУ им Н.Э Баумана, 2002. – 80 с.
3. Liu S., Sun J., Xu Zh. An Improved Image Encryption Algorithm Based on Chaotic System // Journal of Computers. — 2009. — Vol.4 — No.11 — Pp. 1091-1100.
4. Pareek N.K., Patidar V., Sud K.K. Image Encryption Using Chaotic Logistic // Image and Vision Computing. — 2006. — Vol.24 — Pp. 926-934.