Шифрование изображений с использованием хаотической динамики

Сидоренко А.В., Шишко М. С.

Белорусский государственный университет, г. Минск

E-mail: sidorenkoa@yandex.ru

Введение

- Одним из перспективных направлений в современной криптографии является разработка алгоритмов шифрования с использованием хаотической динамики.
- Позитивными для шифрования информации, в том числе, и представленной в виде изображений, является наличие таких важных свойств, как чувствительность к начальным условиям и системным параметрам, свойства псевдослучайности и топологической транзистивности.

Введение

В работе предложен алгоритм шифрования изображений на основе хаотической динамики, оптимизированный для параллельных вычислений.

Проводится оценка стойкости к статистическому и линейному криптоанализу, а также оценка производительности алгоритма.

Алгоритм шифрования изображений на основе хаоса

Для снижения количества шифруемой информации в процессе шифрования производится сжатие растрового изображения. Для этого к исходному шифруемому изображению применяется дискретное вейвлет - преобразование. При этом данные вейвлет - преобразования применяются поочередно ко всем строкам, а затем ко всем столбцам растрового изображения.

Для сжатия без потерь используется биортогональный вейвлет CDF 5/3.

Алгоритм шифрования изображений на основе хаоса

- Изображение разбивается на четыре поддиапазона:

LL, HL, LH, HH.

- LL –поддиапазон содержит уменьшенную копию исходного изображения, а LH-, HL- и HH-поддиапазоны- уточняющие коэффициенты, позволяющие восстановить изображение.
- После вейвлет - преобразования коэффициенты LL-поддиапазона отделяются от остальных вейвлет - коэффициентов.
- LL-поддиапазон содержит максимальное количество информации об исходном изображении по сравнению с другими поддиапазонами и поэтому шифруется отдельно.

Алгоритм шифрования изображений на основе хаоса

- В предлагаемой работе LL-диапазон шифруется с помощью перестановочно-рассеивающего алгоритма.
- Для улучшения безопасности параметры, управляющие перестановкой и диффузией, могут быть различными в разных раундах.
- Это достигается циклическим ключевым генератором с изначальным секретным ключом.
- В криптографических системах этап перестановки, этап диффузии и ключевой генератор могут быть реализованы с помощью хаотических отображений.

Алгоритм шифрования изображений на основе хаоса

- Для перестановки и рассеяния используется хаотическое тент-отображение

$$f(x_n) = \begin{cases} \mu x_n \quad \text{при } x_n < \frac{1}{2} \\ \mu(1 - x_n) \quad \text{при } \frac{1}{2} \le x_n \end{cases}$$

где мю – параметр отображения

Алгоритм шифрования изображений на основе хаоса

- В качестве ключа шифрования используется начальное условие

$x_0(-1) \subset (0, 1)$ для хаотического отображения.

Для обеспечения стойкости алгоритма к дифференциальному криптоанализу данное начальное условие модифицируется с помощью хеш-суммы, вычисляемой по алгоритму SHA-2.

На основе модифицированного начального условия *x*0(0) генерируются начальные условия для каждой строки и столбца согласно

$$x_0(n+1) = \sin(\pi \bullet x_0(n)) \quad n = \overline{0, M+N},$$

где *x*0(*n*) – начальные условия для строк и столбцов; *N* и *M* – число строк и столбцов соответственно.

Алгоритм шифрования изображений на основе хаоса

- Для сжатия изображения производится вложенное кодирование уточняющих вейвлет-коэффициентов с помощью алгоритма HBCT

(Hardware Block Cluster Tree).

- Данный метод использует построение кластерных деревьев в пределах квадратных блоков битовых плоскостей матрицы вейвлет-коэффициентов и прогрессивное вложенное кодирование.
- В процессе кодирования кодер проходит по пространственно-частотным диапазонам битовой плоскости, начиная с LHn и заканчивая HH1.

Алгоритм шифрования изображений на основе хаоса

- После сжатия уточняющие коэффициенты шифруются блочным алгоритмом шифрования на основе обратимых клеточных автоматов.
- Шифруемые данные делятся на блоки, каждый из которых шифруется независимо от остальных. Для каждого блока генерируется собственный ключ, формирование которого происходит с помощью кусочно-линейного отображения.

Алгоритм шифрования изображений на основе хаоса

- Сначала для каждого блока генерируется собственный ключ. Для этого с помощью кусочно-линейного отображения

$$f(x_n)=\begin{cases}\dfrac{x_n}{p}, & 0<x_n<p\\ \dfrac{x_n-p}{1/2-p}, & p<x_n<1/2\\ f(1-x_n), & 1/2<x_n<1\end{cases}.$$

где p – параметр отображения, для каждого блока генерируются четыре числа:

$$\begin{cases}x_1^1=f(x_0);\\ x_1^i=f(x_4^{i-1});\ x_2^i=f(x_1^i);\ x_3^i=f(x_2^i);\ x_4^i=f(x_3^{i-}),\end{cases}$$

Алгоритм шифрования изображений на основе хаоса

Данные четыре числа приводятся к целочисленному представлению

$$n_k^i = \left\lfloor 2^{32} \bullet x_k^i \right\rfloor$$

Из них строится маска для блока N_i. Затем формируется подключ Sk_i

Путем сложения по модулю два маски для блока N_i и общего ключа шифрования *K*

$$Sk_i = K \oplus N_i$$

Алгоритм шифрования изображений на основе хаоса

Шифруемый 256-битный блок данных делится на две равные части BL_i *и* BH_i Обе части складываются по модулю два с подключом Sk_i .

$$BL'_i = BL_i \oplus Sk_i$$

$$BH'_i = BH_i \oplus Sk_i$$

В качестве начальной конфигурации клеточного автомата *C*0 принимается BH'_i , а BL'_i принимается в качестве конфигурации, предшествующей начальной *C*–1.

В качестве эволюционной функции был использован циклический битовый сдвиг. Последние конфигурации *C*79 и *C*80 складываются по модулю два с подключом Sk_i, в результате чего получается блок зашифрованного текста.

Алгоритм шифрования изображений на основе хаоса

- Одной из основных проблем, присущих алгоритмам шифрования изображений, является большое время шифрования. Включенный в алгоритм метод вейвлет-сжатия HBCT не всегда позволяет добиться необходимого уровня производительности. Нами предлагается применение параллельных вычислений как способа, позволяющего повысить производительность.
- Описанный алгоритм разрабатывался так, чтобы максимизировать использование параллельных вычислений. Дискретное вейвлет-преобразование каждого столбца производится независимо, что позволяет осуществлять эти вычисления в несколько потоков. При шифровании LL-поддиапазона обработка строк и столбцов производится параллельно в пределах одного раунда. Кодирование и шифрование вейвлет-коэффициентов происходят в блоках фиксированного размера, причем каждый блок обрабатывается независимо от других, что позволяет производить данные вычисления параллельно.

Алгоритм шифрования изображений на основе хаоса

- В настоящей работе для параллельных вычислений используются неспециализированные вычисления на графическом процессоре или GPGPU (General-purpose computing for graphics processing units) с применением фреймворка OpenCL.

Оценка стойкости алгоритма

- Для оценки стойкости предложенного алгоритма к различным видам криптоанализа разработана программа на языке C++.
- Алгоритм шифрования LL - поддиапазона был протестирован на устойчивость к статистическому и дифференциальному криптоанализу.
- Блочный алгоритм шифрования вейвлет-коэффициентов был протестирован с помощью набора тестов SP 800-22. В тестах использовались изображения «Лена», «Мандрил» и «Перцы», которые

являются стандартными тестовыми изображениями для проверки работы алгоритмов обработки изображений.

Оценка стойкости алгоритма

- Для оценки стойкости алгоритма к статистическому криптоанализу были вычислены коэффициенты корреляция между соседними пикселами по горизонтали, вертикали и диагонали, а также информационная энтропия.
- Для оценки стойкости к дифференциальному криптоанализу производятся следующие действия. Открытый текст изображения зашифровывается и получается изображение-шифр С1. Затем выбирается произвольный пиксел в открытом тексте, чтобы обеспечить небольшое изменение, которое добавляется/вычитается к его десятичному значению, или переключается младший значащий бит. Измененное изображение шифруется с использованием того же ключа для получения нового изображения-шифра С2. Эти два изображения-шифра сравниваются с помощью следующих критериев: процента измененных пикселов (NPCR – Near Pixel Change Rate) и среднего изменения интенсивности (UACI – Unified Averaged Changed Intensity) – меры различия средней интенсивности между двумя шифрами.

Оценка стойкости алгоритма

- Процент измененных пикселов рассчитывается следующим образом

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

$$D(i,j) = \begin{cases} 1 & C1(i,j) = C2(i,j) \\ 0 & C1(i,j) \neq C2(i,j) \end{cases}$$

Чем ближе данный коэффициент к 100 %, тем большую стойкость имеет алгоритм к дифференциальному криптоанализу.

Оценка стойкости алгоритма

- Среднее изменение интенсивности (UACI – Unified Averaged Changed Intensity) – мера различия средней интенсивности между двумя шифрами определяется по формуле

$$UACI = \frac{1}{M \times N} \sum_{i=1,\, j=1}^{M,N} \frac{C1(i,j) - C2(i,j)}{L} \times 100\,\%$$

L – число возможных уровней яркости.

Чем ближе данный показатель к 33 %, тем больше стойкость к дифференциальному криптоанализу.

Оценка стойкости алгоритма

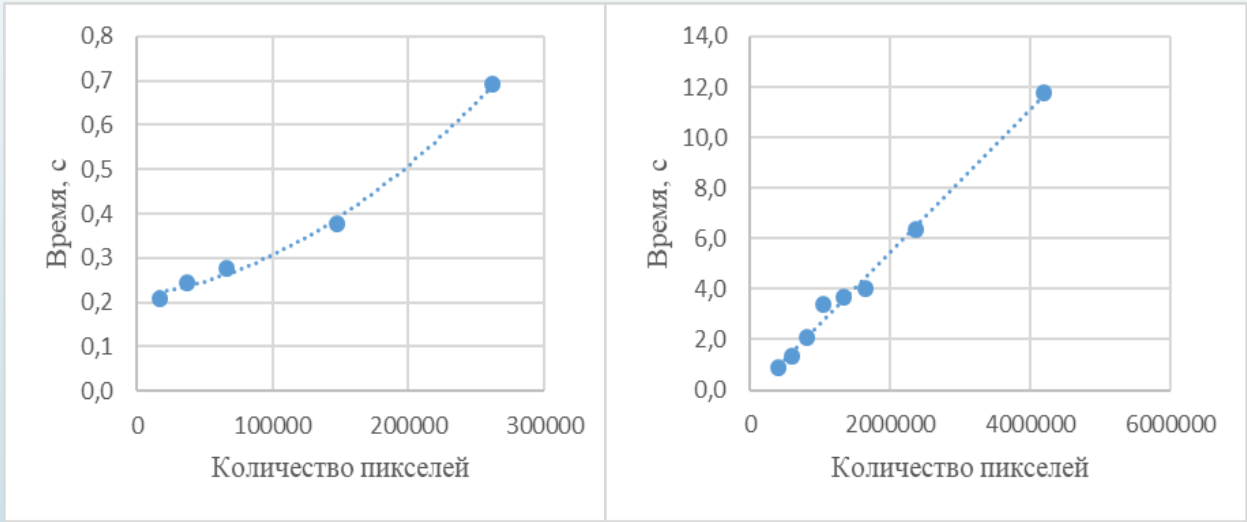
- Проведенная оценка стойкости алгоритма шифрования данных к статистическому и дифференциальному криптоанализу показала высокий уровень стойкости к данным видам криптоанализа.

Оценка производительности алгоритма

- Для осуществления тестирования производительности алгоритма было зашифровано с использованием сжатия без потерь тестовое изображение “Мандрил“ в различных разрешениях.
- Тестирование проводилось с помощью интегрированного графического процессора Intel(R) HD Graphics 4000 и центрального процессора Intel Core i5-3230M.
- На рис. 1, *а* показана зависимость времени шифрования от количества пикселов для изображений малого размера (разрешение до 512×512 пикселов). Из графика видно, что зависимость имеет экспоненциальный характер. Однако для большого размера шифруемого изображения (разрешение более 512×512 точек) зависимость имеет линейный характер (рис. 1, *б*).

Оценка производительности алгоритма

- На рис. 1 показана зависимость времени шифрования от количества пикселов для изображений



а) *б)*

Рис. 1. Зависимость времени шифрования от количества пикселов в изображении:
а) для изображений малого размера; *б)* для изображений большого размера

Оценка производительности алгоритма

- Из графика видно, что зависимость имеет экспоненциальный характер для малых изображений. Однако для большого размера шифруемого изображения (разрешение более 512×512 точек) зависимость имеет линейный характер (рис. 1, б).
- Скорость шифрования при сжатии без потерь находится на уровне 8 Мбит/с.

Заключение

- Разработан алгоритм шифрования изображений с использованием хаотической динамики, оптимизированный для параллельных вычислений. В качестве хаотических отображений для перестановочно-рассеивающего алгоритма используется тент-отображение, а для шифрования уточняющих вейвлет-коэффициентов – хаотическое кусочно-линейное отображение.
- Проведена оценка стойкости алгоритма шифрования LL-поддиапазона вейвлет-коэффициентов к статистическому и дифференциальному криптоанализу. Оценка показала высокий уровень стойкости этой части алгоритма к данным видам криптоанализа.

Заключение

- Протестирован алгоритм шифрования уточняющих вейвлет-коэффициентов с использованием набора статистических тестов SP 800-22. Оценка показала схожесть генерируемого алгоритмом выходного битового потока со случайным потоком по большинству критериев, что означает высокую стойкость данной части алгоритма к статистическому криптоанализу.
- Тестирование производительности разработанного алгоритма показало его высокий уровень. Средняя скорость шифрования с использованием сжатия без потери качества составляет 8 Мбит/с.

Спасибо за внимание