Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

3. Дуб, Дж.Л. Вероятностные процессы / Дж. Л.Дуб. – М.: Издательство иностранной литературы, 1956. – 605 с.

4. Kharin Yu. Parsimonious models for high-order Markov chains and their statistical analysis / Yu. Kharin // VIII World Congress on Probability and Statistics. Publ. House of Koc. Univ.: Istanbul, 2012. – P. 168–169.

5. Raftery, A.E. A model for high-order Markov chains / A.E. Raftery // J. Royal Statistical Society. – 1985. – Vol. B-47, № 3. – P. 528–539.

6. Buhlmann, P. Variable length Markov chains / P. Buhlman, A. Wyner // The Annals of Statistics. – 1999. – Vol. 27, № 2. – P. 480–513.

7. Мальцев, М.В. О тестировании выходных последовательностей криптографических генераторов на основе цепей Маркова условного порядка / М.В. Мальцев, Ю.С. Харин // Информатика. – 2013. – № 4. – С. 104–111.

8. Харин, Ю.С. Цепь Маркова с частичными связями ЦМ(*s*, *r*) и статистические выводы о ее параметрах / Ю.С. Харин, А.И. Петлицкий // Дискретная математика. – 2007. – Т. 19, № 2. – С. 109–130.

9. Meier, W. The self-shrinking generator / W. Meier, O. Sta□elbach // Advances in Cryptology, Euro crypt-94. – 1995. – Vol. 950. – P. 205–214.

ШИФРОВАНИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКОЙ ДИНАМИКИ

А.В. СИДОРЕНКО

Белорусский государственный университет

Широкое распространение информационных технологий и Интернета вызывают проблемы обеспечения безопасного хранения и передачи данных в виде изображений. Одним из наиболее эффективных способов для решения этой задачи является шифрование информации. Стандартные методы шифрования, включая AES, DES или RSA, из-за особенностей, свойственных изображениям, для этого практически не дают эффекта.

В последние годы появилось ряд алгоритмов шифрования изображений, использующих для маскирования динамический хаос. Благодаря присущим динамическому хаосу особенностям, связанным с наличием чувствительности к начальным условиям и случайности, такие методы подходят для шифрования изображений с высокой степенью защиты. При этом шифрование, как правило, происходит с использованием перестановки и диффузии. При перестановке с помощью хаотического отображения производится перераспределение пикселей изображения без изменения уровня их яркости. На стадии диффузии путем применения хаотической последовательности к изображению изменяется значение каждого пикселя.

В данной работе предлагается генетический алгоритм шифрования изображений с использованием модели дезоксирибонуклеиновой кислоты (ДНК) и динамического хаоса. В схеме предложенного нами алгоритма шифрования выделяются три этапа: инициализация, генерация изображений-шифров и использование генетического алгоритма. Два последних этапа могут повторяться до тех пор, пока не будут удовлетворять выбранным критериям. В нашем случае в качестве критерия используется достижение соответствующего уровня информационной энтропии в зашифрованном изображении, что обусловлено необходимостью обеспечения лучшего быстродействия функционирования алгоритма. Рассмотрим подробнее этапы алгоритма.

Инициализация параметров алгоритма шифрования. Вводятся данные о необходимом значении энтропии, величине начальной популяции и значении процента мутирующих членов популяции. Производится вычисление хэш суммы для изображения по алгоритму SHA-256. Для этого хэш сумма разбивается на блоки, с помощью которых вычисляются начальные условия для хаотического отображения. Формирование начальной популяции производится при генерации хаотических последовательностей путем итерации логистического отображения. Она образуется за счет последовательностей, число которых равно размеру популяции, а размер каждой последовательности в три раза превышает количество пикселей шифруемого цветного изображения. Затем с помощью соответствующих кодировок начальная популяция и шифруемое изображение преобразуются в ДНК- последовательности. При этом получается ДНК- последовательность, соответствующая изображению, и некоторое количество ДНК- последовательностей, соответствующих начальной популяции (ДНК-маски).

Генерация изображений - шифров. На данном этапе происходит маскирование изображения ДНК-масками. После кроссовера для каждой ДНК-маски рассчитывается энтропия. Получаем несколько замаскированных ДНК – последовательностей, для которых рассчитывается энтропия замаскированных изображений.

Использование генетического алгоритма. После вычисления энтропии происходит кроссовер между парами ДНК-масок, которые выбираются случайным образом по правилу рулетки, размеры векторов которой пропорциональны энтропии каждого члена. Точка кроссовера выбирается посередине каждой ДНК-маски. Маски с минимальным значением энтропии проходят процесс мутации и заменяются на новые маски, генерируемые, как и члены начальной популяции. Рассчитывается энтропия. Если в популяции ДНК-масок есть хотя бы одна с энтропией, большей требуемого значения, то эта ДНК-маска используется для шифрования изображения, а соответствующие ей начальные условия – в качестве ключа расшифрования. При отсутствии этого популяция вновь проходит стадию кроссовера и мутации, пока не появится подходящая маска.

В данной работе проведена оценка стойкости шифра к статистическому и дифференциальному криптоанализам. При проведении статистического анализа шифрованного текста рассчитаны коэффициенты, позволяющие оценить стойкость шифра к статистическому криптоанализу: корреляция между соседними пикселями изображения и информационная энтропия. Как показали результаты проведенных вычислений, модуль коэффициента корреляции близок к нулевому значению, и не превосходит двух сотых. Энтропия же в зашифрованном изображении близка к своему максимальному значению. В совокупности с низким уровнем корреляции это означает хорошую стойкость алгоритма к статистическому анализу.

Дифференциальный криптоанализ заключается в следующем. В исходном изображении вносится небольшое изменение, затем производится шифрование исходного и измененного изображений, после чего определяют различия в двух рассматриваемых изображениях, чтобы найти закономерности между изменениями в зашифрованных изображениях и исходных изображениях.

Для оценки стойкости к данному типу анализа открытый текст изображения зашифровывается, получаем изображение-шифр C1. Затем в открытом тексте изображения произвольно меняется один пиксель. Это измененное изображение зашифровывается тем же ключом, получаем изображение-шифр C2. С помощью коэффициентов NPCR (Number of Pixel Change Rate) и UACI (Unified Averaged Changed Intensity) проводим сравнительный анализ полученных C1 и C2.

Тестирование проводилось с использование изображений “Лена“ и “Бабуин” с различным разрешением. Полученные результаты показывают, что и коэффициент

NPCR и коэффициент UACI стремятся к своим идеальным значениям, что свидетельствует о хорошей стойкости к дифференциальному криптоанализу.

В данной работе проведена оценка производительности предложенного алгоритма. Оценка производительности осуществлялась с помощью процессора Intel Core i5-3230M 2,4 GHz с 6 GB RAM. Результаты приведены на рисунках 1, 2, 3.

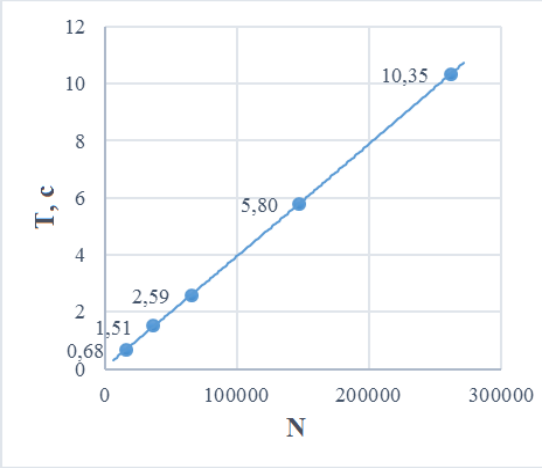

Рис. 1 – График зависимости времени шифрования T (в секундах) от размера изображения N (в пикселях)

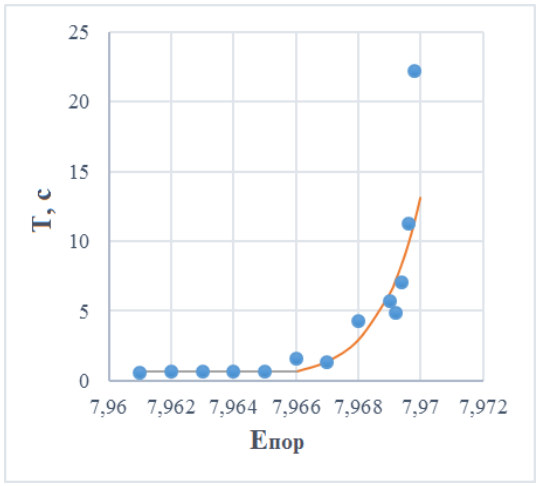

Рис. 2 – График зависимости времени шифрования T (в секундах) от порогового значения энтропии $E_{пор}$

Как видно из рисунка 1, время шифрования растет по линейному закону в зависимости от количества пикселей изображения при постоянных остальных параметрах. Приведенная на рисунке 2 зависимость времени шифрования от заданного значения энтропии показывает, что при малых значениях энтропии время шифрования практически остается постоянным. Это связано с тем, что для достижения данного уровня достаточно одной итерации генетического алгоритма. Далее по графику происходит экспоненциальный рост времени шифрования от заданного значения энтропии. Приведенный на рисунке 5 график зависимости времени шифрования от заданного процента мутаций показывает, что существует минимум при 30% уровне мутаций.

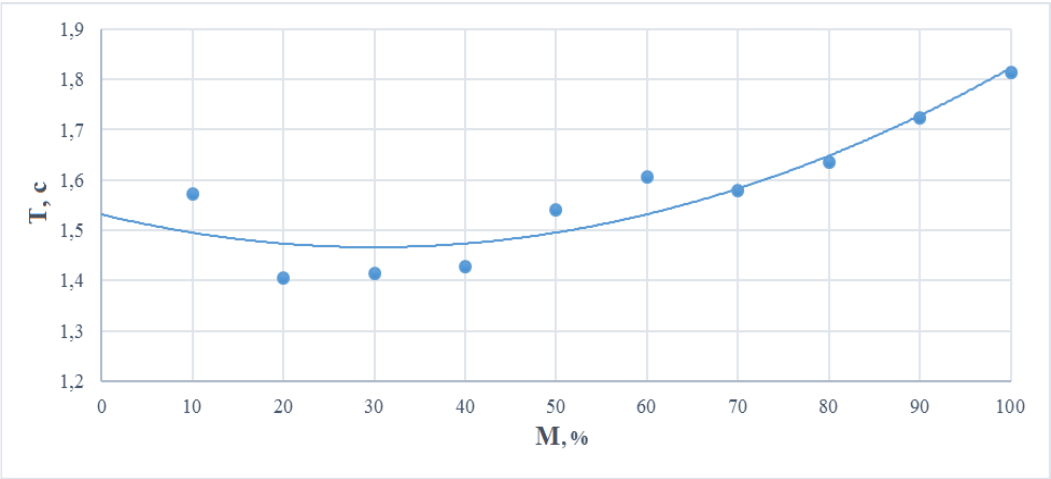

Рис. 3 – График зависимости времени шифрования T (в секундах) от заданного процента мутаций M

Предложенный алгоритм шифрования изображений позволяет повысить степень защиты информации, стойкость к различным атакам и может быть интегрирован в аппаратуру. Преимуществами данного алгоритма является его гибкость, а также возможность обеспечения шифрования с необходимым уровнем безопасности.

ОЦЕНКА УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ФИЗИЧЕСКОГО ДАТЧИКА СЛУЧАЙНЫХ ЧИСЕЛ

А. И. ТРУБЕЙ, И.К. ПИРШТУК, В.Ю. ПАЛУХА, М.В. МАЛЬЦЕВ

НИИ прикладных проблем математики и информатики БГУ

Функционирование физического датчика случайных чисел (ФДСЧ) основано на преобразовании случайного физического процесса в случайную последовательность с равномерным распределением на интервале [0, 1]. Основным недостатком данного метода является возможная нестабильность вероятностных характеристик случайной величины используемого процесса. Поэтому необходимо оценить стабильность функционирования параметров ФДСЧ, то есть рассмотреть гипотезу о том, что распределение вероятностей случайной величины физического процесса зависит от времени, и определить статистическую значимость отклонений данных параметров. Для подтверждения стабильности эмпирического закона распределения необходимо осуществлять проверку устойчивости работы ФДСЧ в течение определенного времени.

1. Формулировка гипотезы об однородности выборок

Предположим, что имеем комплект, состоящий из $M \geq 2$ двоичных последовательностей, выработанных датчиком в промежутки времени $t_1,...,t_M$. Из комплекта сформируем M независимых выборок, полученных в результате статистического анализа последовательностей. Каждая из выборок есть реализация полиномиальной схемы с N исходами. Объемы выборок равны $n_1,...,n_M$. Обозначим $n = \sum_{k=1}^{M} n_k$, $n_0 = min\{n_1,...,n_M\}$, $\nu_{k,i}$ – частота символа i. В качестве выборок можно рассматривать, например, частоты встречаемости пересекающихся (непересекающихся) l-грамм, гистограммы частот F_k попадания вероятностей p_{ij} матрицы статистического портрета датчика в каждый из 10 подинтервалов, на которые разбивается интервал [0; 1]. Гипотеза однородности предполагает, что вероятностные свойства наблюдаемой последовательности не изменяются во времени. Это означает, что возможные изменения внешних условий и отклонения параметров физического датчика не являются статистически значимыми.

Полагаем, что выборки статистически однородны и для них выполняется гипотеза H_0, если $p_{1,i} = ... = p_{M,i}$; $i = 1,..., N$. В противном случае будем говорить, что выполняется альтернатива H_1. При альтернативе вероятности исходов могут быть постоянными или изменяться с ростом объемов выборок.

Для проверки однородности используем статистику хи-квадрат:

$$\chi^2 = n\sum_{k=1}^{M}\sum_{k=1}^{N}\frac{1}{n_k m_i}\left(\nu_{k,i} - m_i\frac{n_k}{n}\right)^2, \text{ где } m_i = \sum_{k=1}^{M}\nu_{k,i}.$$