Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

Аль-Асади
МохайманСалах

Методика тестирования хаотических генераторов псевдослучайных последовательностей для систем защиты информации

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

_____

Научный руководитель
Борискевич Анатолий Антонович
д.т.н., доцент

_____

Минск 2016

ВВЕДЕНИЕ

Развитие телекоммуникационных мультимедийных технологий способствует увеличению потоков информации и вызывает необходимость в создании новых алгоритмов защиты информации от несанкционированного доступа. Поиск новых технологий защиты обусловлен не стремлением увеличения криптостойкости традиционных схем шифрования, а необходимостью не зависеть от существующих стандартов и нерешённых математических проблем, которые могут перестать быть препятствием перед злоумышленником.

Одним из решений данной проблемы является использование алгоритмов хаотического шифрования, которые строятся на основе генераторов псевдослучайных чисел (ГПСЧ). ГПСЧ являются связующим звеном в обеспечении информационной безопасности. Такие генераторы применяются во многих криптографических задачах, например, при формировании случайных параметров и ключей систем шифрования, поэтому требования, предъявляемые к ним, оказываются достаточно высокими. В частности, одним из критериев абсолютно произвольной двоичной последовательности, получаемой на выходе генератора, является невозможность её предсказания в отсутствии какой-либо информации о данных, подаваемых на вход генератора. Поэтому на практике необходимо проводить тестирование для проверки случайного характера бинарной последовательности, формируемой ГПСЧ, что в свою очередь позволяет выявить генераторы, заранее удовлетворяющие требованиям конкретной криптографической задачи.

Целью дипломного проекта является исследование ГПСЧ с помощью существующих методов тестирования, программная реализация алгоритмов генерации хаотических последовательностей с улучшенными свойствами (одномерныеидвумерные генераторы), которые позволяют эффективно защищать передаваемые данные и восстанавливать их на приемной стороне получателю, владеющему начальными значениями генератора (управляющий параметр и начальное состояние последовательности), а также тестирование полученных результатов.

Для достижения данной цели были решены следующиезадачи:

–классификация генераторов псевдослучайных чисел;

– анализ методики тестирования генераторов псевдослучайных чисел на основе графических и статистических тестов;

– анализ основных характеристик одномерных ГПСЧ (показатель Ляпунова, пространственная траектория, бифуркационная диаграмма, плотность распределения состояний, чувствительность к начальным параметрам);

– программная реализация алгоритмов шифрования с улучшенными характеристиками на основе двумерных ГПСЧ, тестирование полученных результатов;

Результаты проведенного исследования являются необходимыми во многих приложениях, например, в медицине, информационных системах, космических системах, науке.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является исследование ГПСЧ с помощью существующих методов тестирования, программная реализация алгоритмов генерации хаотических последовательностей с улучшенными свойствами (одномерные, двумерные и трехмерные генераторы), которые позволяют эффективно защищать передаваемые данные и восстанавливать их на приемной стороне получателю, владеющему начальными значениями генератора (управляющий параметр и начальное состояние последовательности), а также тестирование полученных результатов

Для достижения данной цели были решены следующие задачи:

- проведена классификация генераторов псевдослучайных чисел;
- проведен анализ методики тестирования генераторов псевдослучайных чисел на основе графических и статистических тестов;
- проведен анализ основных характеристик одномерных генераторов псевдослучайных чисел;
- осуществлена программная реализация в среде моделировании Matlabалгоритмов шифрования на основе двумерных генераторов псевдослучайных чисел.

Результаты проведенного исследования являются необходимыми во многих приложениях, например, в медицине, информационных системах, космических системах, науке.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении и общей характеристике работы обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются цель и задачи, указывается теоретико-методологическая основа, формулируются основные положения диссертации, выносимые на защиту.

Первая глава носит теоретический характер, состоит из 6 разделов. В ней определяется следующее:

Вторая глава носит теоретический характер, состоит из 3 разделов. В ней представлена классификация генераторов псевдослучайных чисел. Было выделено три основные типа: конгруэнтные, криптографические и хаотические генераторы. Последние могут иметь одномерное, двумерное и трехмерное представление. Данные генераторы используются в схемах поточного шифрования мультимедийной информации с минимальным коэффициентом размножения ошибок.

Третья глава носит практико-ориентированныйхарактер, состоит из 3 разделов. В ней представлены модели динамического хаоса. В данном разделе рассмотрены одномерные однопараметрические хаотические генераторы

Четвертая глава носит практико-ориентированный характер, состоит из 2 разделов. В данном разделе рассмотрен метод шифрования изображений на основе улучшенного варианта ГПСЧ, а именно двумерного хаотического генератора, который основан на формировании хаотических матриц перестановок. Формирование двумерных генераторов производилось в среде программирования Matlab. Программа предусматривает следующие возможности:

– открытие изображения в формате bmp;

– возможность синтезировать матрицы хаотических значений и перестановок;

– применение полученных матриц для шифрования изображения.

По полученным данным произведено тестирование чувствительности генераторов на основе логистической хаотической функции, хаотической функции Тент, рекурсивной функции, хаотической функции приподнятый Тент к изменению начального параметра x(0).

ЗАКЛЮЧЕНИЕ

Произведена классификация генераторов, выделено три основных класса генераторов: криптографические, конгруэнтные, хаотические.

Проведен анализ графических тестов: гистограмма распределения элементов последовательности, распределение на плоскости, проверка серий, проверка на монотонность, автокорреляционная функция, профиль линейной сложности, графический спектральный тест.

Проведено тестирование генератора Blum-Blum-Shum, линейного конгруэнтного генератора (CG), криптографического генератора на регистрах сдвига с линейной обратной связью (LFSR), криптографического генератораAES-128.

Проанализированы основные характеристики одномерных хаотических генераторов: бифуркационная диаграмма, показатель Ляпунова, пространственная траектория, чувствительность к начальным параметрам, плотность распределения состояний.

Проведен анализ методики статистического тестирования (пакет НИСТ – национальный институт стандартов и технологий), основанной на генерации множества псевдослучайных последовательностей определенной длины по критерию уровня значимости для каждого из 16 тестов, вычисления значений вероятностей P-value, вычислении гистограммы P-value, определении равномерности гистограмм, вычислении критерия Хи-квадрат, сравнении пересчитанного значения P-valueco значением доверительного интервала.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Аль-АсадиМохайман Салах АбдулмахдиКомбинированное маркирование мультимедийной информации на основе триангуляционных ключевых точек // Аль-АсадиМохайман Салах Абдулмахди,А.А. Борискевич, П.М. Никуленко, Технические средства защиты информации: тез.докл. XIII Белорус.-рос. науч.-техн. конф. – Минск – Минск: БГУИР, 2015. –С. 35.