СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ ДЕТЕРМИНИРОВАННОГО ХАОСА

УДК 003.26

Е.А. Дрыбин, В.С. Садов, БГУ, г. Минск;
О.М. Демиденко, УО ГГУ им. Ф. Скорины, г. Гомель

Аннотация

В работе представлены и исследованы подходы к формированию длинных воспроизводимых с требуемой точностью, хаотических последовательностей. Предложен стеганостойкий алгоритм кодирования конфиденциальной информации, использующий в качестве контейнера хаотическую последовательность, что позволяет скрыть как факт наличия секретного сообщения, так и факт передачи контейнера.

Введение

На протяжении нескольких десятилетий человечество переживает информационный взрыв, который характеризуется быстрым увеличением объема циркулирующей и хранящейся информации практически во всех сферах деятельности современного общества. В настоящее время информация играет ключевую роль в научно-техническом прогрессе и является ресурсом, не менее значимым и необходимым, чем энергетические, финансовые, трудовые и другие ресурсы. В таких условиях одной из наиболее актуальных задач в области информационных технологий является задача обеспечения конфиденциальной передачи и хранения информации.

В отличие от традиционных криптографических методов защиты информации, скрывающих содержимое сообщения, стеганография скрывает сам факт наличия секретного сообщения, тем самым, позволяя достичь наибольшей стойкости к атакам, направленным на выявление или разрушение скрываемой информации [1]. Получение случайных последовательностей чисел является краеугольным камнем многих прикладных задач современных крипто- и стеганографических систем защиты информации (генерация ключей, одноразовых шифроблокнотов, контейнеров и т.д.). Источниками настоящих случайных чисел могут служить физические шумы, как, например, дробовый шум в резисторе, детектор событий ионизирующей радиации. Однако случайные последовательности, полученные с помощью подобных устройств, невозможно воспроизвести, что делает их непригодными для решения ряда задач. В большинстве приложений информационной безопасности используются генераторы псевдослучайных чисел (ГПСЧ), формирующие выходную последовательность псевдослучайных чисел (ПСП) согласно заданному алгебраическому алгоритму. Хотя ПСП, как может показаться, лишена закономерностей, любой ГПСЧ с конечным числом внутренних состояний повторится после достаточно длинной последовательности чисел. Таким образом, для большинства ГПСЧ возможно вычислить всю ПСП, если их состояние в какой-то момент скомпрометировано, что позволит криптоаналитику получить доступ не только к будущим сообщениям, но и ко всем предыдущим [2].

Целью настоящей работы является разработка стеганостойкого алгоритма шифрования информации, использующего в качестве контейнера хаотическую последовательность, программная реализация стеганографической системы и разработка ГПСЧ на основе явления детерминированного хаоса, позволяющего получать сколь угодно длинные воспроизводимые выходные последовательности со статистическими свойствами, близкими к свойствам истинно случайных последовательностей.

Разработка стеганостойкого алгоритма сокрытия информации

Разрабатываемая стеганографическая система в качестве контейнера использует хаотическую последовательность, что позволяет скрыть как факт наличия секретного сообщения, так и факт передачи контейнера. Метод встраивания информации должен обеспечить качественное сокрытие, а также конфиденциальность данных в случае их обнаружения злоумышленником.

Отличительными особенностями хаотических последовательностей являются близость их свойств к истинно случайной последовательности и в то же время способность быть повторно воспроизведенными. Выбор типа генератора хаоса (ГХ) и его конкретной реализации является одной из важнейших задач данной работы.

Одним из самых известных алгоритмов для встраивания информации является метод LSB, однако, он является уязвимым для всех видов атак, суть которых заключается в обнаружении кодированного сообщения по аномальным статистическим характеристикам младших бит цифровых отсчетов [1]. С другой стороны, существует один из простейших алгоритмов криптографического шифрования информации – шифр Вернама (схема одноразового блокнота). Данный шифр является единственным, для которого доказана абсолютная криптографическая стойкость [3]. Идея разрабатываемого в работе метода заключается в объединении принципов этих двух простых методов для достижения высокого качества встраивания и криптографической стойкости стеганосистемы.

Так как замена младшего бита в контейнере на бит сообщения приводит к появлению статистических аномалий, которые могут быть легко выявлены (а сообщение прочитано), то вместо этого используем операцию сложения по модулю два (XOR) бита сообщения и соответствующего младшего бита контейнера. С точки зрения вероятности появления нуля или единицы в младшем бите отсчета хаотического сигнала (обладающего по сути характеристиками случайного сигнала) операция сложения по модулю два с битами сообщения ничего не меняет, поэтому статистические методы стеганографического анализа не могут выявлять наличие секретного сообщения в таком контейнере.

Кроме того, последовательность бит контейнера обладает характеристиками, близкими к истинно случайным, поэтому сложение по модулю два является,

Репозиторий ГГУ имени Ф. Скорины

по сути, применением шифра Вернона к сообщению. Так как шифр Вернона обладает абсолютной криптографической стойкостью, то в ситуации обнаружения наличия скрытого сообщения злоумышленником, он не сможет узнать его содержание, не имея ключа (исходной последовательности). Одним из условий успешного применения схемы одноразового блокнота является использование каждый раз различной последовательности, равной по длине сообщению. Для этой задачи хорошо подходят хаотические последовательности. Вместо длинного ключа необходимо знать лишь начальные условия и параметры генератора для получения хаотической последовательности произвольной длины. Так как хаотические процессы крайне чувствительны к начальным условиям, то достаточно лишь немного изменить их, чтобы получить совершенно другую выходную последовательность.

Таким образом, предложенный алгоритм сразу решает как задачу качественного скрытия сообщения, так и обеспечения абсолютной криптографической стойкости в случае его обнаружения. В качестве ключа в предложенном методе встраивания информации может выступать набор начальных условий для хаотического процесса.

Процесс извлечения информации представляет собой обратную встраиванию последовательность действий. Для прочтения сообщения необходимо воспроизвести исходную хаотическую последовательность, для чего требуется иметь идентичный ГХ и ключ (набор начальных условий и параметров генератора), а также иметь стеганофайл целиком. Ключ должен быть передан принимающей стороне заранее по надежному каналу передачи данных.

Генераторы хаотических последовательностей

Под ГХ будем понимать некоторую динамическую систему, в которой имеют место хаотические колебания, порождающие хаотическую последовательность чисел. ГХ, по сути, является разновидностью ГПСЧ и, в первую очередь, предназначен для решения тех же задач, то есть получения воспроизводимой последовательности чисел, наиболее приближенной по своим характеристикам к истинно случайной. Важным свойством истинно случайной последовательности является полное отсутствие корреляций, то есть сколь угодно большие знания о предыдущих значениях не могут повысить вероятность успешного предсказания следующего значения.

Согласно Шеннону, для защиты от статистического анализа зашифрованных данных, необходимо использовать два базовых метода сокрытия исходных статистических распределений: запутывание и распыление [2].

Запутывание обеспечивает сокрытие статистических свойств исходного сообщения для любого стороннего наблюдателя.

В смысле сообщения, распыление приводит к тому, что статистически близкие последовательности бит исходной информации преобразуются в совершенно различные последовательности стего (при шифровании одним ключом). В смысле ключа, распыление предполагает, что близкие ключи шифруют сообщение в совершенно разные стего. По сути, каждый бит ключа должен влиять на все стего сложным нелинейным образом. Это свойство особенно важно при дешифровании, так как в противном случае аналитик будет иметь возможность выявить тот факт, что некоторые биты ключа подобраны верно.

Исходя из вышеизложенного, для ГПСЧ можно выделить ряд существенных требований [4]:

– статистическая устойчивость: ПСП на выходе идеального ГПСЧ должна иметь равномерный закон распределения, а корреляция между значениями должна отсутствовать. Говоря проще, все подпоследовательности определенной длины должны иметь одинаковую вероятность появления в ПСП, выдаваемой генератором. Практически это означает, что ПСП должна пройти некоторый набор статистических тестов на равномерное распределение и независимость значений друг от друга;

– воспроизводимость: во многих задачах (в том числе часто в стеганографии и криптографии) необходимо иметь возможность воспроизвести одну и ту же ПСП неоднократно. Практически любой ГПСЧ (в отличие от последовательностей, генерируемых физическими устройствами) обладает данным свойством;

– длинный период: полный цикл генератора должен быть достаточно большим, чтобы невозможно было воссоздать его полностью в течение достаточно длинного периода компьютерного времени. В настоящие дни с увеличением вычислительных мощностей в геометрической прогрессии данная проблема обостряется;

– непредсказуемость: требование означает невозможность надежно предсказать будущие значения на выходе генератора, зная предыдущие, при помощи какого-либо полиномиального алгоритма. Данное требование особо важно в прикладных задачах стеганографии и криптографии;

– эффективность: конкретная реализация ГПСЧ должна быть как можно более эффективна с точки зрения использования вычислительных мощностей (потребления ресурсов процессора и оперативной памяти).

Большинство современных ГПСЧ базируется на двух основных методах: линейно-конгруэнтном и методе сдвиговых регистров [4]. Каждый из базовых методов имеет свои принципиальные недостатки [5, 6, 7], не позволяющие им в полной мере соответствовать вышеизложенным требованиям. Существует также схема Макларена-Марсальи, использующая два ГПСЧ и вспомогательную матрицу, с помощью которой происходит перемешивание двух последовательностей, полученных от двух генераторов [8], однако, на сегодняшний день в ней выявлено четыре тесно связанных друг с другом недостатка при использовании в криптографических задачах [9].

Хаотические последовательности теоретически обладают [3]:

– качественными характеристиками, идентичными характеристикам истинно случайной последовательности (получаемых, например, с использованием физических устройств генерирования случайных чисел);

– в отличие от истинно случайных последовательностей их возможно воспроизвести на протяжении некоторого интервала времени (на некотором протяжении

Репозиторий ГГУ имени Ф. Скорины

траектории системы в фазовом пространстве), после чего исходная и повторенная последовательности начинают расходиться.

Совершенно очевидно, что такая последовательность лишена всех недостатков ПСП, однако, возникает ряд вопросов [3]:

– практическая реализация ГХ, управление хаотическими процессами и порождаемой им выходной последовательности;

– длительность интервала времени, на котором возможно воспроизвести хаотический процесс с требуемой точностью, а, значит, и максимальная длина воспроизводимой последовательности, порождаемой ГХ;

– формирование сколь угодно длинной последовательности на выходе ГХ, не изменяя ее качественных характеристик.

Классической задачей стеганографии является оценка качества используемого генератора, считающегося псевдослучайным. Для проверки последовательности порождаемой ГПСЧ на статистическую устойчивость, например, в набор NIST (Национальный Институт Стандартов и Технологий США) входит 16 различных тестов [10].

Для проверки выходной последовательности ГПСЧ на непредсказуемость можно использовать статистический критерий, предназначенный для нахождения автокорреляции временных рядов, так называемый тест Льюнга-Бокса. Этот тест проверяет на отличие от нуля сразу несколько коэффициентов автокорреляции [11].

В дальнейшем, именно эти четыре теста будут использоваться для оценки качества порождаемой ГПСЧ последовательности. Кроме того, если классические ГПСЧ в большинстве случаев позволяют воспроизвести всю длину выходной ПСП, то ГХ нуждаются в дополнительном анализе этого критерия. Актуальной длиной ПСП для ГХ можно считать именно то количество битов, которое при необходимости возможно воспроизвести. Таким образом, эти два требования оказываются взаимосвязаны друг с другом и должны рассматриваться вместе.

Одним из важнейших свойств хаотических процессов является возможность их воспроизведения. Насколько бы точно не были заданы начальные условия со временем, исходная и повторенная последовательности начнут расходиться. Также стоит понимать, что при программной реализации нелинейной системы с хаотическими режимами свои коррективы в возможность воспроизведения внесет точность вычислений (например, ограничение представления числа с плавающей запятой), а при аппаратной реализации – шумы физических элементов. Эти «погрешности» реализации системы невозможно просчитать теоретически, поэтому длина выходной последовательности ГХ, которая может быть воспроизведена, должна определяться экспериментально для каждой конкретной модели. Тем не менее, выявить некоторые теоретические зависимости, общие для всех систем, можно [12]. Данные закономерности носят скорее не абсолютный, а оценочный или относительный характер, но с их помощью можно теоретически сравнить ГХ без учета «погрешностей» практической реализации и оценить наиболее «перспективный».

Одной из наиболее значимых и информативных характеристик хаотических процессов является энтропия Колмогорова, обратно пропорциональная времени предсказуемости системы [13]:

$$K \approx \frac{1}{T}.$$

При цифровой обработке хаотических колебаний происходит дискретизация параметра времени и поэтому можно говорить об эквивалентности интервала времени длине выходной последовательности ГХ в отсчетах. Таким образом, одна из теоретических зависимостей может быть описана отношением:

$$L \approx \frac{1}{K}.$$

Другими словами, длина воспроизводимости обратно пропорциональна энтропии Колмогорова системы. Это является закономерным следствием того факта, что K-энтропия является мерой непредсказуемости или нашего незнания о системе [13].

С одной стороны, для выполнения требования воспроизводимости энтропия Колмогорова системы должна быть как можно меньше, с другой стороны, для выполнения требования непредсказуемости энтропия Колмогорова должна быть как можно больше. С точки зрения использования ГХ в качестве ГПЧС, в прикладных задачах информационных технологий единственным вариантом является компромисс между требованиями воспроизводимости и непредсказуемости. При этом для достижения наилучших результатов целесообразно для различных задач применять различные модели ГХ с требуемым «балансом».

K-энтропия определяется свойствами и внутренним устройством самой нелинейной системы и поэтому не зависит от численных параметров, используемых в описывающих модель дифференциальных уравнениях, и которые, в свою очередь, определяют режим возникающих в системе колебаний [12, 13].

Точность задания начальных условий в любой практической модели конечна и, безусловно, прямым образом влияет на возможность предсказать состояние системы через некоторое время. Экспериментально была выявлена зависимость степени воспроизведения хаотического движения от порядка величины флуктуации начальных условий от их абсолютного значения [12]:

$$L = k(\alpha)\cdot\varepsilon,$$

где L – количество воспроизводимых отсчетов выходной последовательности, k – коэффициент воспроизводимости, зависящий от набора параметров α, описывающих хаотическую систему, ε – порядок флуктуации начальных условий относительно своей абсолютной величины. Коэффициент воспроизводимости зависит как от внутреннего устройства и непредсказуемости самой нелинейной системы (что описывает K-энтропия), так и от реализации его конкретной модели. Коэффициент воспроизводимости позволяет принять однозначное решение: совпадает ли данный повторенный отсчет с исходным и может ли считаться успешно воспроиз-

Репозиторий ГГТУ им. П.О. Сухого

веденной вся последовательность. На коэффициент воспроизводимости не оказывают влияния параметры дифференциальных уравнений и конкретные начальные условия.

Наиболее значимым фактором, влияющим на возможности воспроизведения выходной последовательности ГХ, является его конкретная реализация и используемые в ней методы получения хаотических последовательностей. Для программной реализации наибольшее значение имеет метод решения дифференциальных уравнений, описывающих хаотическую систему. Рассмотреть все методы не представляется возможным, однако, понятно, что чем выше точность решения, предоставляемая тем или иным методом, тем более длинную выходную последовательность можно повторить и тем больше вычислительных ресурсов потребуется для моделирования такой системы. Для решения практических задач наиболее целесообразно найти некоторый баланс между точностью решения, а соответственно воспроизводимостью, и вычислительной эффективностью.

Так как воспроизвести больше, чем определенное количество отсчетов невозможно, то единственным способом продлить последовательность будет перезапуск генератора. Для того, чтобы качественные свойства последовательности не нарушились, необходимым условием, очевидно, является «нераздельность» всей «длинной последовательности» на отдельные подпоследовательности, из которых она была получена. То есть граница «сшивки» подпоследовательностей должна отсутствовать. Для выполнения этого требования очередной перезапуск ГХ необходимо осуществлять с $nL+1$-го отсчета, где L – длина воспроизводимой подпоследовательности [12]. Таким образом, при перезапуске генератора мы продолжаем двигаться по аттрактору, не нарушая статистических характеристик выходной последовательности и скрывая места «сшивки». С помощью такого приема можно получить сколь угодно длинную хаотическую последовательность на выходе генератора без существенного увеличения сложности технической реализации и затрат на требуемые вычислительные мощности. Обратной стороной данного метода является необходимость сохранять или передавать все наборы начальных условий для перезапуска ГХ.

При выборе ГХ и его конкретной реализации целесообразно стремиться к компромиссу между характеристиками и подбирать их в соответствии с требованиями прикладной задачи и техническими возможностями. Для более детального изучения и анализа этого вопроса в работе были рассмотрены известные динамические системы с хаотическими режимами [13]: Лоренца, Рёсслера, Чуа.

Для математического моделирования и анализа хаотических процессов использован пакет программ MATLAB, в котором действительное число представляется восемью байтами. Таким образом, максимальная точность вычислений составляет порядка 10^{-16}. Для решения системы дифференциальных уравнений, описывающих хаотический процесс, выбран численный метод Дорманда-Принса (разновидность метода Рунге-Кутты четвертого порядка точности), который сочетает достаточно высокую точность и быстродействие. Особенности этого метода и необходимость хранения промежуточных данных позволяют достичь максимальной точности вычислений порядка 10^{-14}.

Результаты экспериментального исследования представлены в виде графиков зависимостей длины воспроизводимости от заданного порядка точности вычислений и затраченного времени на вычисления с заданной точностью от воспроизводимой длины при этой точности (рисунок 1 и рисунок 2 соответственно).

Исходя из графика зависимости длины воспроизводимости от заданного порядка точности вычислений, можно сказать, что система Рёсслера обладает наибольшей воспроизводимостью. В то время, как системы Лоренца и Чуа практически идентичны по этому показателю и более чем в два раза уступают системе Рёсслера.

Время, потраченное на вычисления, нельзя считать абсолютной мерой быстродействия ГХ, однако, так как все эксперименты проводились в одинаковых условиях, его с успехом можно использовать как относительную

Рисунок 1 – График зависимости длины воспроизводимости от заданного порядка точности вычислений

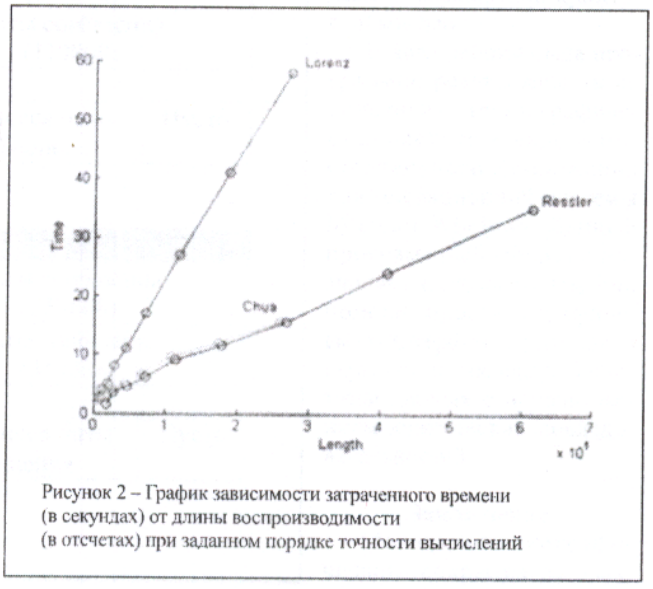

Рисунок 2 – График зависимости затраченного времени (в секундах) от длины воспроизводимости (в отсчетах) при заданном порядке точности вычислений

Репозиторий ГГТУ им. П.О. Сухого

величину для сравнения генераторов между собой. Анализируя график зависимости затраченного времени от длины воспроизводимости можно сравнить исследуемые ГХ по относительному показателю эффективности с точки зрения затрат вычислительного времени:

$$Q = \frac{количество\ отсчетов}{затраченное\ время}.$$

Практически одинаково эффективными ГХ являются система Рёсслера и схема Чуа, существенно уступает им в этом показателе модель Лоренца.

Для проверки статистических свойств выходной последовательности на соответствие выдвигаемых к ней требований необходимо использовать какой-либо алгоритм хеширования, так как все числа представлены с использованием МПЗ-аппроксимации. Каждый отсчет генератора представляет собой 64 бита (8 байт), которые представляют собой десятичное число в определенном формате и потому распределены не случайно. Используем следующий простой и эффективный способ хеширования: каждый отсчет преобразовывается в 8-битный путем сложения между собой всех байт 64-битного числа по модулю 255 (соответствующему максимальному значению 8-битного числа).

Для проверки выходной последовательности на соответствие требованию статистической устойчивости для каждого ГХ были проведены монобитный тест и тест пробегов; непредсказуемость генераторов проверялась с помощью теста Льюнга – Бокса. Для каждого из исследуемых ГХ более 95 % порождаемых последовательностей успешно проходили все тесты.

С точки зрения «качества» выходной последовательности и близости ее статистических характеристик к характеристикам истинно случайной, наилучшим вариантом является ГХ на основе системы Лоренца. Наилучшей воспроизводимостью и вычислительной эффективностью обладает генератор Рёсслера, существенно превосходящий по этим показателям системы Лоренца и Чуа.

Структура и анализ стеганографической системы

Для практического построения стеганографической системы использованы два альтернативных ГХ, основанных на системах Лоренца и Рёсслера соответственно. Первый генератор позволяет более качественно скрыть встраиваемое сообщение, в то время как второй обладает большей вычислительной эффективностью.

В качестве ключа выберем набор начальных условий (192 бита) генератора. Если ключ будет отличаться хотя бы на 1 бит, на выходе ГХ будет совершенно другая последовательность. Таким образом, общее количество всех возможных последовательностей в построенной стеганосистеме будет порядка $2^{192} \sim 10^{57}$.

Для генератора Лоренца длину одного цикла перезапуска из соображений надежности выберем равной $L_L = 120\,000$ отсчетов (соответствует точности вычислений $\sim 10^{-12}$ при реальной точности $\sim 10^{-14}$). Для генератора на основе системы Рёсслера аналогичная длина составит $L_R = 360\,000$. Встраивание сообщения производится в соответствии с разработанным выше алгоритмом – сложением по модулю два младшего бит контейнера с соответствующим битом сообщения. Для каждого ГХ схема встраивания приведена на рисунке 3.

Для проверки стего на отсутствие статистических аномалий были проведены монобитный тест, тест пробегов и тест Льюнга-Бокса. По результатам экспериментального исследования статистические свойства стего идентичны свойствам пустого контейнера (хаотической последовательности).

120000 бит			
Условия перезапуска генератора (192 бит)		Биты сообщения (119808)	
Условия перезапуска генератора (192 бит)		Биты сообщения (119808)	
…		…	
Стоп-сигнал (24 бита)	Количество оставшихся бит (16 бит)	Оставшиеся биты сообщения	Пусто

360000 бит			
Условия перезапуска генератора (192 бит)		Биты сообщения (359808)	
Условия перезапуска генератора (192 бит)		Биты сообщения (359808)	
…		…	
Стоп-сигнал (24 бита)	Количество оставшихся бит (16 бит)	Оставшиеся биты сообщения	Пусто

Рисунок 3 – Схема встраивания битов сообщения в контейнер:
а) генератор Лоренца, б) генератор Рёсслера

Таким образом, можно говорить о том, что разработанная стеганографическая система обладает высокой стеганографической стойкостью и абсолютной криптостойкостью.

В ходе работы была программно реализована выше описанная стеганографическая система в виде самостоятельного приложения для операционной системы Microsft Windows. Данный программный продукт позволяет пользователям при помощи простого графического интерфейса (рисунок 4) скрывать и извлекать любые типы данных с использованием хаотических последовательностей.

Заключение

Методы стеганографического сокрытия данных,

Репозиторий ГГУ имени Ф. Скорины

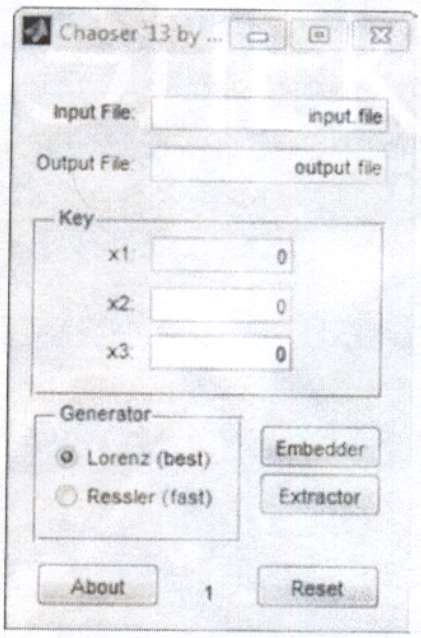

Рисунок 4 – Внешний вид интерфейса приложения Chaoser '13

использующих в качестве контейнера хаотическую последовательность, обеспечивают высокую стеганостойкость и абсолютную криптостойкость. Извлечение данных представляет собой обратный сокрытию процесс и требует наличия исходной (немодифицированной) хаотической последовательности. Чувствительность хаотических процессов к сколь угодно малым изменениям начальных условий и затратность воспроизведения хаотических последовательностей с точки зрения вычислительных мощностей исключают возможность подбора ключа методом «грубой силы».

В настоящей работе показано, что ГХ могут успешно использоваться в задачах, требующих «качественных» случайных последовательностей чисел, а также предложен метод получения длинных хаотических последовательностей путем перезапуска ГХ с nL=1-го отсчета, где n –номер перезапуска, L – длина воспроизводимой подпоследовательности. Таким образом, возможно получить сколь угодно длинную воспроизводимую хаотическую последовательность, не изменяя ее статистических свойств. По результатам экспериментальных исследований в ходе работы установлено, что максимальная длина воспроизведения хаотического процесса обратно пропорциональна энтропии Колмогорова и прямо пропорциональна точности вычислений и определения начальных условий. Для исследованных в работе хаотических систем Лоренца, Рёсслера и Чуа при точности вычислений порядка 10^{-16} (64-битное представление числа) длины воспроизводимости соответственно равны $L_{Lmax} = 2{,}7 \cdot 10^5$, $L_{Rmax} = 6{,}2 \cdot 10^5$ и $L_{Cmax} = 2{,}6 \cdot 10^5$ отсчетов (по 64 бита).

Литература:

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

2. Shannon, C.E. A mathematical theory of communication / C.E. Shannon // Bell System Technical Journal. – 1948. – № 4. – P. 379–423, 623–526.

3. Дрыбин, Е.А. Получение длинных хаотических последовательностей / Е.А. Дрыбин, В.С. Садов // Материалы международной научной конференции ITS 2013. – 2013. – С. 254–255.

4. Бараш, Л.Ю. Генерация случайных чисел и параллельных потоков случайных чисел для расчетов Монте-Карло / Л.Ю. Бараш, Л.Н. Щур // Модел. и анализ информ. систем. – 2012. – № 2. – С. 145–162.

5. Шнайер, Б. Прикладная криптография / Б. Шнайер. – Триумф, 2002. – 275 с.

6. Ferrenberg, A.M. Monte Carlo simulations: hidden errors from «good» random number generators / A.M. Ferrenberg, D.P. Landau, Y. Wong // J. Phys. Rev. Lett. – 1992. – № 69 (23). – 3382–3384.

7. MacLaren, M.D. Uniform Random Number Generators / M.D. MacLaren, G. Marsaglia // Journal of the ACM. – 1965. – P. 83–89.

8. Кнут, Д.Э. Искусство программирования / Д.Э. Кнут. – 3-е изд. – М. : Вильямс, 2000. – Т. 2: Получисленные алгоритмы. – 832 с.

9. Retter, C.T. Cryptanalysis of a MacLaren – Marsaglia system / C.T. Retter // Cryptologia. – 1984. – № 8. – P. 97–108.

10. Rukhin A. A statistical test suite for random and pseudorandom number generators for cryptographic applications / A. Rukhin, J. Soto, J. Nechvatal and the oth. // NIST Special Publication. – 2001. – 800-22. – P. 153.

11. Эконометрика. Учебник / отв. ред. : И.И. Елисеева. – 2-е изд. – М. : Финансы и статистика, 2006. – 576 с.

12. Садов, В.С. Исследование хаотических процессов на примере математической модели системы Лоренца в пакете программ MATLAB R2011b / В.С. Садов, Е.А. Дрыбин // Материалы международной научной конференции ITS 2012. – 2012. – С. 270–271.

13. Шустер Г. Детерминированный хаос: введение / Г. Шустер. – М. : Мир, 1988. – 240 с.

Abstract

In the work presented and investigated approaches to the formation of long reproducible, with the required accuracy, chaotic sequences. Steganostable encoding algorithm confidential information, using as a container chaotic sequence that allows you to hide the fact of how a secret message, and the fact of the transfer container proposed.

Поступила в редакцию 07.08.2014 г.

Программаторы для любых микросхем
SEPROM EEPROM EPROM FLASH PIC MCU PAL
+375 (17) 266-32-09 www.chipstar.ru

Репозиторий ГГТУ им. П.О. Сухого