позволяет сделать вывод о нелинейном характере зависимости значений показателей S и R, а, следовательно, H и h, от продолжительности заболевания. Некоторые особенности динамики показателей S и R рассмотрены ниже.

Все значения информационных показателей маркеров синдрома холестаза в группе больных с хроническим активным гепатитом испытывают колебания на протяжении 12-и лет заболевания. Значения показателей S и R увеличиваются от начала заболевания (0,150 бит и 9,4%) до конца первого года заболевания (0,618 бит и 39,0%), затем они снова убывают к двум годам (0,362 бит и 22,9%), после чего наступает их рост на третий год заболевания (0,532 бит и 33,5%). Вследствие дальнейшего уменьшения H и h достигают минимума к шести годам заболевания (0,256 бит и 16,2%). Таким образом, к 6-8 годам заболевания коэффициент относительной организации системы R принимает очень низкие значения, что указывает на высокий уровень нестабильности функциональной системы.

Средние значения информационных показателей S и R маркеров синдрома холестаза в группе больных с хроническим персистирующим гепатитом испытывают колебания на протяжении 12-и лет заболевания, причём в период с 8-и до 12-и лет это скачкообразные колебания с большой амплитудой. Значения информационной организации системы S и коэффициента избыточности R увеличиваются от 0,5 лет заболевания (0,069 бит и 4,4%) до двух лет заболевания (0,566 бит и 35,7%), затем снова уменьшаются на третий год заболевания (0,305 бит и 19,2%). К восьми годам вновь происходит их увеличение (0,637 бит и 40,2%), а затем резкое уменьшение к девятому году заболевания (0,132 бит и 8,3%). От 9-и до 10-и лет средние значения S и R снова возрастают (0,614 бит и 38,8%), к 11-и годам заболевания уменьшаются до минимума (0,058 бит и 3,6%). К 12-и годам заболевания снова происходит повышение значений S и R до 0,427 бит и 26,9%, что указывает на стремление функциональной системы к стабильному состоянию.

В группе больных с циррозом печени средние значения информационной организации системы S и коэффициента избыточности R постепенно увеличиваются от 0,176 бит и 11,1% в первый год до максимальных значений к десятому году заболевания (0,590 бит и 37,2%). К 12 годам заболевания происходит уменьшение значений S и R до 0,435 бит и 27,5%.

Проведённый анализ позволяет сделать вывод о стремлении физиологических функций к устойчивому состоянию не только в норме, но и в условиях сформировавшегося патологического процесса для групп с хроническим персистирующим гепатитом и циррозом печени.

Список литературы

1. Исаева Н.М., Савин Е.И., Субботина Т.И. Исследование биохимических и иммунологических показателей крови при патологии печени с позиции теории информации // Международный журнал прикладных и фундаментальных исследований. – 2013. – №10-2. – С. 279-280.

2. Исаева Н.М., Савин Е.И., Субботина Т.И., Яшин А.А. Биоинформационный анализ биохимических и иммунологических показателей крови при хроническом вирусном поражении печени. // Международный журнал прикладных и фундаментальных исследований. – 2013. – №10-3. – С. 505-507.

3. Исаева Н.М., Савин Е.И., Субботина Т.И., Яшин А.А. Информационное состояние биохимических и иммунологических показателей крови при патологии печени // Международный журнал прикладных и фундаментальных исследований. – 2013. – №11-1. – С. 63-64.

«Технические науки и современное производство»
Франция (Париж), 14-23 октября 2014 г.

МЕТОДЫ И МОДЕЛИ ХАОТИЧЕСКИХ ПРОЦЕССОВ В СИСТЕМАХ СВЯЗИ

Когай Г.Д., Тен Т.Л.

Карагандинский государственный технический университет, Караганда, e-mail: tentl@mail.ru

Обилие работ, посвященных возможности применения хаотических процессов для передачи сообщений позволяет говорить о сложившемся направлении как в области телекоммуникаций, так и в области исследований динамического хаоса. Этим задачам посвящены специальные выпуски журналов IEEE Transactions on Circuits and Systems, International Journal of Circuit Theory and Applications, обзоры и монографии.

Цель. Исследовать и разработать методы и модели хаотических процессов в системах связи на основе отображения нелинейной динамической системы для шифрования и передачи информации. Провести исследования данного криптографического алгоритма по всем необходимым параметрам.

Описание алгоритма

В работе [1] указаны три отличительные черты хаотических процессов, благодаря которым перспективно применение динамического хаоса для передачи информации:

1) Широкополосность. Хаотические сигналы непериодичны и обладают непрерывным спектром. Для многих типов хаотических сигналов этот спектр занимает весьма широкую полосу и, кроме того, вид спектральной характеристики можно задавать. В системах связи широкополосные сигналы используются для борьбы с искажениями в каналах распространения сигнала, в частности, с такими эффектами, как затухание сигнала в некоторой полосе частот или с узкополосными возмущениями. Таким образом, хаотические сигналы потенциально применимы для систем связи, использующих широкий диапазон частот;

2) Сложность. Хаотические сигналы имеют сложную структуру и весьма нерегулярны. Один и тот же хаотический генератор может создавать совершенно разные процессы при весьма незна-

чительном изменении начальных условий. Это значительно затрудняет определение структуры генератора и предсказание процесса на какое-нибудь длительное время. Сигналы сложной формы и непредсказуемого поведения являются классическими видами сигналов, используемых в криптографии, что дает еще одну возможность применения хаоса;

3) Ортогональность. В силу нерегулярности хаотических сигналов, их автокорреляционная функция обычно весьма быстро затухает. Поэтому сигналы от нескольких генераторов вполне можно считать некоррелированными, ортогональными. Это свойство указывает на применимость хаотических сигналов для многопользовательских систем связи, в которых один и тот же диапазон частот используется несколькими пользователями одновременно.

Исследования в области применения хаоса в системах связи открывают широкие возможности для практических применений в таких направлениях как: синхронизация приемника и передатчика [2-4]; фильтрация шумов [5]; восстановление информационных сигналов [5], а также разработка алгоритмов кодирования-декодирования, позволяющих представить произвольное цифровое сообщение через символическую динамику хаотической системы [4, 5].

В настоящее время известно, что хаотические сигналы, генерируемые нелинейными детерминированными динамическими системами, так называемый динамический хаос, обладают целым рядом свойств, способствующих применению этих сигналов для передачи информации. Предложен ряд конкретных схем передачи информации, использующих динамический хаос, в частности, схема хаотической маскировки информационного сигнала [4]; схемы с нелинейным подмешиванием информационного сигнала в хаотический [4] и др. Обсуждаются возможности создания прямохаотических систем связи, в которых хаотические колебания выступают в качестве носителя информации, генерируемого непосредственно в области частот, где происходит передача информации [5].

В работе [6] приводится классификация динамических систем с точки зрения возможности их использования в качестве источников хаотического сигнала, содержащего кодированную информацию, который может быть передан и подвергнут дешифрованию в приемнике с малыми искажениями. Основной результат работы состоит в том, что передача информации с очень малой вероятностью ошибки может быть выполнена в том случае, если скорость генерирования информации хаотической системой, т.е. топологическая энтропия системы не меньше, чем скорость выработки информации источником сообщения (т.е. шенноновской энтропии) за вычетом условной энтропии, вызванной ограничениями в канале связи (например, шумовые искажения).

Многие статьи посвящены передаче сообщений с помощью модулированного хаотического сигнала. Такой способ модуляции имеет ряд преимуществ по сравнению с традиционно используемой модуляцией гармонического сигнала. Действительно, если в случае гармонических сигналов управляемых характеристик всего три (амплитуда, фаза и частота), то в случае хаотических колебаний даже небольшое изменение параметра дает надежно фиксируемое изменение характера колебаний [5]. Это означает, что у источников хаоса с изменяемыми параметрами имеется широкий набор схем ввода информационного сигнала в хаотический (т.е. модуляции хаотического сигнала информационным). Кроме того, хаотические сигналы принципиально являются широкополосными. В системах связи широкая полоса частот несущих сигналов используется как для увеличения скорости передачи информации, так и для повышения устойчивости работы систем при наличии возмущений. Шумоподобность и самосинхронизируемость систем, основанных на хаосе, дают им потенциальные преимущества и над традиционными системами с расширением спектра, базирующимися на псевдослучайных последовательностях.

Рассмотрим подробнее некоторые схемы применения хаоса для передачи сообщений. К первым и, пожалуй, наиболее часто цитируемым публикациям по передаче сообщений с помощью хаотических сигналов относятся статьи [2, 3]. В этих статьях передатчик строится как система Лоренца, уравнения которой после масштабирования приводятся к виду:

$$\begin{cases} u = \sigma(v-u), \\ v = ru - v - 20uw, \\ w = 5uv - bw. \end{cases} \quad (1)$$

В соответствии с построена аналоговая электронная цепь, имеющая параметры $\sigma = 16$, $r = 45.6$, $b = 4.0$ (переменные *u, v, w* отвечают напряжениям на выходах операционных усилителей). Уравнения приемника взяты в виде:

$$\begin{cases} u_s = \sigma(v_s - u_s), \\ v_s = ru - v_s - 20uw_s, \\ w_s = 5uv_s - bw_s. \end{cases} \quad (2)$$

Уравнения (2) похожи на (1), за исключением того, что правая часть (2) зависит не от своей переменной состояния u_s, а от переменной u, которая таким образом может рассматриваться как поступающий на приемник выходной сигнал передатчика. Методом функций Ляпунова в работах [2, 3] показано, что системы (1) и (2) синхронизируются, т.е. невязка между их соответствующими переменными состояния асимптотически стремится к нулю. Другими словами, (2) является асимптотическим наблю-

дателем для (1). Для передачи двоичного сигнала коэффициент в передатчика (1) изменялся, принимая значение $b = 4.4$, соответствующее двоичной «единице», тогда как исходное значение $b = 4.0$ означало двоичный «ноль». При изменении величины в (1) до $b = 4.4$ в системе (2) резко возрастает уровень сигнала рассогласования $e = u - u_s$ (т.к. параметр в наблюдателя (2) отличается от значения в системе (1)). Усреднением $e^2(t)$ определялось, какой из сигналов был передан.

В работе [3-4] продемонстрирована и возможность применения хаоса для защиты информации. Предложенный там подход известен под названием «хаотического маскирования» (chaotic masking) и состоит в том, что в передатчике к информационному полезному сигналу добавляется хаотический, а в приемнике происходит восстановление полезного сигнала из смеси. Для выделения полезного сигнала использовано свойство робастности процесса синхронизации систем (2), (1). Система (2) может, тем самым, рассматриваться как фильтр, настроенным, нестрого говоря, в резонанс к хаотическому генератору (1). Поскольку полезный сигнал $m(t)$ имеет принципиально другую форму, чем хаотический, его можно восстановить, подавая на вход приемника (2) смешанный сигнал $s(t) = m(t) + u(t)$, а затем на выходе приемника восстановить по оценке $u_r(t)$ переменной $u(t)$ по формуле $m'(t) = s(t) - u_r(t)$.

К настоящему времени предложены различные методы использования хаотических процессов для хранения и кодирования информации. Начинают развиваться принципиально новые системы обработки информации – хаотические процессоры. Возможности таких процессоров продемонстрированы разработкой программного комплекса «Associative Memory for Pictures», предназначенного для записи и извлечения изображений, а также систему управления факсимильными документами «FacsDataWizard». Развитием этой системы явился программный комплекс «Незабудка», защищенный патентами Российской Федерации и США. Задачей комплекса является поиск документов (с идентификацией места в документе) при запросах на естественном языке. Информация запоминается и хранится в виде траекторий дискретной хаотической системы. Соответствующее хаотическое отображение строится в процессе кодирования информации. При старте с произвольных начальных условий траектория после переходного процесса притягивается к одному из имеющихся циклов и воспроизводит соответствующую информацию.

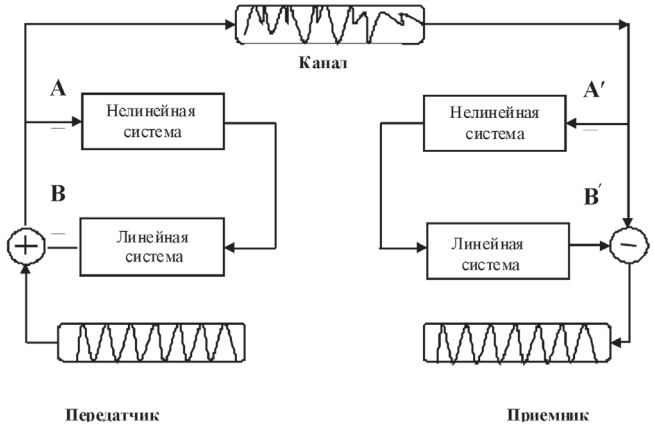
В большинстве современных систем связи в качестве носителя информации используются гармонические колебания. Информационный сигнал в передатчике модулирует эти колебания по амплитуде, частоте или фазе, а в приемнике информация выделяется с помощью обратной операции – демодуляции. Модуляция носителя может осуществляться либо за счет модуляции уже сформированных гармонических колебаний, либо путем управления параметрами генератора в процессе формирования колебаний.

Аналогичным образом можно производить модуляцию хаотического сигнала информационным сигналом. Однако возможности здесь значительно шире. Действительно, если в случае гармонических сигналов управляемых характеристик – всего три (амплитуда, фаза и частота), то в случае хаотических колебаний даже небольшое изменение параметра дает надежно фиксируемое изменение характера колебаний. Это означает, что у источников хаоса с изменяемыми параметрами, имеется широкий набор схем ввода информационного сигнала в хаотический (т.е. модуляции хаотического сигнала информационным). Кроме того, хаотические сигналы принципиально являются широкополосными, интерес к которым в радиотехнике связан с большей информационной емкостью. В системах связи широкая полоса частот несущих сигналов используется как для увеличения скорости передачи информации, так и для повышения устойчивости работы систем при наличии возмущений.

На рисунке показана простейшая схема связи с использованием хаоса. Передатчик и приемник включают в себя такие же нелинейные и линейные системы, как источник. Дополнительно в передатчик включен сумматор, а в приемник – вычитатель. В сумматоре производится сложение хаотического сигнала источника и информационного сигнала, а вычитатель приемника предназначен для выделения информационного сигнала. Сигнал в канале хаосоподобный и не содержит видимых признаков передаваемой информации, что позволяет передавать конфиденциальную информацию. Сигналы в точках A и A', B и B' попарно равны. Поэтому при наличии входного информационного сигнала S на входе сумматора передатчика такой же сигнал будет выделяться на выходе вычитателя приемника.

Сфера применения хаотических сигналов не ограничивается системами с расширением спектра. Они могут быть использованы для маскировки передаваемой информации и *без* расширения спектра, т.е. при совпадении полосы частот информационного и передаваемого сигналов.

Все это стимулировало активные исследования хаотических коммуникационных систем. К настоящему времени на основе хаоса предложено несколько подходов для расширения спектра информационных сигналов, построения самосинхронизующихся приемников и развития простых архитектур передатчиков и приемников (рисунок).



Пример схемы связи с использованием хаоса

Вывод

Идея большинства предложенных решений базируется на синхронизации приемником исходного невозмущенного хаотического сигнала, генерируемого передатчиком. С помощью таких схем связи может передаваться как аналоговая, так и цифровая информация с различными скоростями информационных потоков и разной степенью конфиденциальности. Еще одним потенциальным достоинством схем связи с использованием хаоса является возможность реализации новых методов разделения каналов, что особенно важно в многопользовательских коммуникационных системах [7- 8].

Шумоподобность и самосинхронизируемость систем, основанных на хаосе, дают им потенциальные преимущества над традиционными системами с расширением спектра, базирующимися на псевдослучайных последовательностях. Кроме того, они допускают возможность более простой аппаратной реализации с большей энергетической эффективностью и более высокой скоростью операций.

Список литературы

1. Тайлак Б.Е. Модель псевдослучайного генератора, построенного на базе хаотической системы: // Труды международной научной конференции «Наука и образование – ведущий фактор стратегии «Казахстан – 2030». – Караганда:

2. Изд-во КарГТУ, 2009. – С. 353-355.

3. Тайлак Б.Е. Генератор псевдослучайных последовательностей на базе хаотической системы // Материалы международной научно-практической конференции. – Омск – 2009.

4. Д. Кнут. Искусство программирования.– СПб.: Питер, 2000. – Т.2.

5. Marsaglia G. DIEHARD Statistical Tests.

6. Menezes A., van Oorshot P., Vanstone S. Handbook of Applied Cryptography / CSR Press. 1997.

7. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

8. Когай Г.Д., Тайлак Б.Е., Томилова Н.И., Спанова Б.Ж. Методические основы применения хаотической динамики к криптографическому преобразованию информации. «Наука и образование – ведущий фактор стратегии «Казахстан – 2030». – Караганда: КарГТУ, – Сагиновские чтения № 5. – 2013. – Часть III.

9. Бейсенби М.А., Тен Т.Л., Когай Г.Д., Тайлак Б.Е. Управление детерминированным хаосом в распределенных сетях. Учебное пособие – Караганда: КарГТУ, 2012.

АНАЛИЗ ГЕНЕРАТОРА ПСП НА ОСНОВЕ СВОЙСТВ ХАОТИЧЕСКИХ СИСТЕМ

Когай Г.Д., Тен Т.Л.

Карагандинский государственный технический университет», Караганда, e-mail: tentl@mail.ru

Существует множество алгоритмов, обеспечивающих различные уровни криптографической защищенности, основанные на различных принципах защиты, от применения секретных алгоритмов, до использования математических методов, основанных на вычислительной сложности. Одно из современных перспективных направлений криптографической защиты информации в распределенных компьютерных сетях есть применение алгоритмов, основанных на поведенческих свойствах нелинейных динамических систем, так называемых «детерминированном хаосе».

Цель – разработать метод генерации псевдослучайных чисел на основе свойств хаотических систем. Провести анализ статистической безопасности работы генератора, используя различные методики оценки качества работы генератора. От качества работы ГСЧ зависит качество работы всей системы и точность результатов. Поэтому случайная последовательность, порождаемая ГСЧ, должна удовлетворять целому ряду критериев.

Описание алгоритма

Для исследования ПСП применяются две группы тестов [1]:

Графические тесты – статистические свойства последовательностей отображаются в виде графических зависимостей, по виду которых делают выводы о свойствах исследуемой последовательности.

Оценочные тесты – статистические свойства последовательностей определяются число-