Применение детерминированного хаоса в информационных технологиях

Шилин Д.Л.
ВМиП, ФИТиУ
Белорусский государственный университет информатики и радиоэлектроники
Республика Беларусь, Минск, ул. П. Бровки, 6
dimashilin@gmail.com

***Аннотация* — В этом докладе автор предлагает ознакомиться с системой шифрования на базе устройства фазовой синхронизации и приводит результаты статистического анализа такой системы.**

Ключевые слова: детерминированный хаос, устройство фазовой синхронизации, шифование.

I. Введение

Явлению нерегулярного движения в нелинейных системах был присвоен термин – детерминированный хаос, который возникает не из-за внешнего источника шума, не из-за большого числа степеней свободы, а определяется динамикой нелинейной системы. Причиной нерегулярного поведения является свойство нелинейных систем экспоненциально быстро разводить первоначальные траектории в области фазового пространства [1]. Предсказать поведение траекторий хаотических систем невозможно, поскольку чувствительность к начальным условиям высока, а начальные условия могут быть заданы только с конечной точностью.

Автор предлагает использовать системы фазовой синхронизации (СФС) в режиме детерминированного хаоса для синхронной засекреченной передачи информации или для зашифровывания и хранения информации на электронных носителях.

II. Моделирование

Остановимся на основных свойствах СФС, позволяющих реализовать поставленную задачу.

Во-первых: поведение хаотических траекторий не может быть предсказано; прогноз движения вдоль траекторий становится все более и более неопределённым, по мере удаления от начальных условий.

Во-вторых: при одинаковых начальных условиях и одинаковых значениях параметров СФС система генерирует непредсказуемые, но одинаковые траектории.

В-третьих: СФС обладают уникальной возможностью синхронной работы по стартовому импульсу.

Основываясь на этих свойствах автором разработана система засекречивания в режиме реального времени, которая может быть использована при передаче информации и ее хранении. Основным блоком системы является устройство фазовой синхронизации, которое работает в режиме детерминированного хаоса. Достижение требуемого режима обеспечивается выбором соответствующих параметров устройства и начальной расстройкой частоты. Устройство фазовой синхронизации (УФС) является системой автоматического регулирования, частота настройки которой в синхронном режиме определяется частотой управляющего сигнала и коэффициентом деления цепи обратной связи, а сигналом рассогласования является разность фаз управляющего сигнала и сигнала цепи обратной связи. Структурная схема УФС приведена на рис. 1.

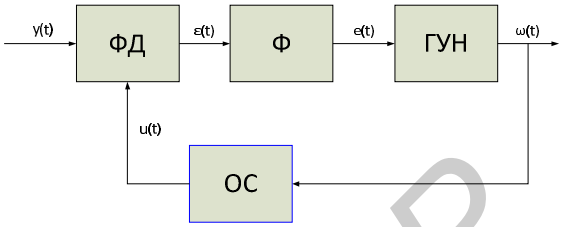

Рис. 1. Структурная схема УФС

Где: ФД – фазовый детектор; Ф – фильтр корректор; ГУН генератор, управляемый напряжением; ОС – цепь обратной связи; $y(t)$ – входной сигнал; $u(t)$ – сигнал обратной связи; $\varepsilon(t)$ – сигнал рассогласования; $e(t)$ – управляющий сигнал; $\omega(t)$ – выходной сигнал устройства.

Для УФС характерны различные режимы работы. Синхронные режимы: однократный синхронный режим; кратные захваты; *NT*-периодические режимы. Асинхронные режимы: режим биений; режим хаоса и режим детерминированного хаоса[1]. В данном докладе под рабочим режимом подразумевается режим детерминированного хаоса, который отличается невозможностью предсказания поведения выходного сигнала устройства.

Основной трудностью в достижении этого режима является определение параметров устройства и начального рассогласования частоты[1].

Режим детерминированного хаоса характеризуется построением странных аттракторов в области фазового пространства (рис. 2)

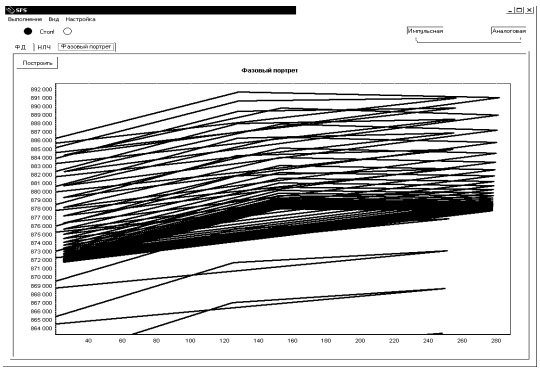

Рис. 2. Фазовый портрет системы в режиме хаоса

Таким образом, значения фазы и частоты на выходе фазового детектора представляют собой некоторую случайную последовательность. В целях оценки “степени случайности” данной последовательности, был проведен ряд тестов — статистических и теоретических. Предполагается равномерное распределение последовательностей. Тестирование проводилось по критериям сериальной корреляции, частот, интервалов, серий, максимум-t и монотонности. Все статистические тесты были успешно пройдены. Последовательности достаточно случайны для

применения в любых приложениях, использующих случайные и псевдослучайные последовательности.

Прежде всего, рассматривается возможность использования системы в криптографии (шифровании информации).

III. Анализ системы

Разработанная система представляет собой симметрично − поточную криптосистему, в которой шифрование проводится над каждым байтом исходного текста с использованием гаммирования. Источником гамма – последовательности является УФС, работающая в режиме детерминированного хаоса[2,4,5]. С точки зрения шифрования процесс генерации необходимых последовательностей лучше представить следующим образом. На вход подаётся некоторый ключ, представляющий собой конечное множество чисел $\{a1,a2,...,ak\}$. На выходе получаем последовательность $\{x1,x2,...,xn\}$, которую можно использовать, например, для сложения с открытым текстом. В качестве ключевого пространства используется множество $A=A1\times A2\times...\times Ak$, представляющее собой множество ключей, при которых выходная последовательность случайна. При использовании системы для шифрования файлов мощность этого множества имеет большое значение, поскольку, чем она больше, тем меньше вероятность узнать ключ методом перебора. Необходима случайность используемой гамма – последовательности, чтобы скрывать статистические свойства открытого текста и сделать невозможной статистическую атаку.

Последовательности чисел, получаемые при помощи генератора на основе УФС в режиме детерминированного хаоса, были протестированы на случайность. Поскольку равномерное распределение последовательности, то для того, чтобы выдвинуть гипотезу, необходимо было рассмотреть вначале группированный статистический ряд, построенный по выборке случайных чисел. Построение проводилось, как и принято в математической статистике, на основе подсчета частот встречаемости чисел, принадлежащих каждому из интервалов. Из гистограммы (рис. 3) мы смогли предположить, что функция распределения является равномерной.

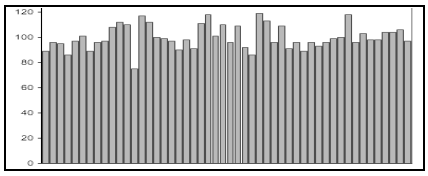

Рис. 3. Гистограмма последовательности

Тестирование последовательности проводилось по критериям сериальной корреляции, частот, интервалов, серий, максимум t и монотонности[2]. Для анализа численных значений также применялась программа–анализатор значений статистики (”хорошими” считались значения, лежащие между 25 – й и 75 – й процентными точками для статистик K^+ (K^-) и χ^2).

Тест сериальной корреляции пройден последовательностью успешно, поскольку значение вычисленной статистики (коэффициента сериальной корреляции C=–0,00360991) принадлежит определенному диапазону и указывает на практическое отсутствие линейной зависимости каждого следующего элемента последовательности от предыдущих. Для критериев частот, серий и монотонности значения статистик χ^2лежат между 25 й и 75 й процентными точками, что указывает на достаточную случайность тестируемой последовательности. Все другие использованные тесты были также успешно пройдены.

Таким образом, есть основания утверждать, что разработанная система кодирования является практически стойкой, обладает высокой скоростью работы, и в тоже время, выделяется простотой реализации, т. к. используется симметрично − поточная криптосистема.

[1] Дмитриев А.С., Смирнов С.О.Передача сообщений с использованием хаоса и классическая теория информации.// Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1998, №11, с. 4-32

[2] Кузнецов А.П., Батура М.П., Шилин Л.Ю. Анализ и параметрический синтез импульсных систем с фазовым управлением. Минск, 1993.

[3] Кнут Д. Искусство программирования, том 2 // М. Наука, 2001, -788 с.

[4] Шахгильдян В.В., Ляховкин А.А. Системы фазовой автоподстройки частоты // М.: Связь, 1972. -447 с.

[5] Акимов В.Н., Белюстина Л.Н., Белых В.Н. Системы фазовой синхронизации // М.: Радио и связь, 1982. -288 с