УДК 514.765
А.В. Токарев[1]
Использование детерминированного хаоса при шифровании сигнала

Использование детерминированного хаоса при шифровании сигнала.

Детерминированный хаос это нерегулярное или хаотическое движение, порожденное нелинейными системами, для которых динамические законы однозначно определяют эволюцию во времени состояния системы при известной предыстории.

Критерии хаотичности системы:

1. сигнал “выглядит случайным”;

2. в спектре мощности наблюдается широкополосный шум на низких частотах;

3. автокорреляционная функция быстро спадает;

4. сечение Пуанкаре состоит из точек, заполняющих пространство.

На данный момент разработаны методы классификации различных типов хаоса, найдены закономерности его развития, созданы техники, позволяющие отличить хаос от белого шума, и т.п. Более того, было обнаружено и строго обосновано, что сложное пространственно-временное поведение распределенных сред с громадным числом степеней свободы может быть адекватно описано нелинейными системами небольшой размерности.

Одним из направлений применения хаоса является защита информации. 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.

Главной проблемой при шифрации сигнала является создание неповторяющейся гаммы - последовательности длиной близкой или равной длины сигнала, генерируемой неким достаточно устойчивым ключом, с использованием быстрого и простого в реализации алгоритма. Данную проблему легко решить с помощью детерминированного хаоса.

Пусть имеется сигнал S длиной n s_i, где $i = 1, 2, .., n$ элемент сигнала S.

Выберем дискретную динамическую систему $x \to f_\lambda(x)$, где λ- некоторая постоянная величина, с наложенными на функцию $f(x)$ следующими ограничениями:

1. функция непрерывна, выпукла вверх на отрезке $(0, 1)$;

2. $f(0) = f(1) = 0$;

3. функция имеет непрерывную производную в точке максимума.

Выберем $x_0 \in (0, 1)$ - начальное значение, необходимое для создания траектории. С помощью дискретной динамической системы $x \to f_\lambda(x)$, используя итеративное отображение, строится траектория точки x_0 - $x_1, x_2, ..., x_n$. Данная последовательность $\{x_i\}_n$ является гаммой и равна длине самого сигнала. Если произвести слияние последовательностей $\{s_i\}_n$ и $\{x_i\}_n$ неким методом, то полученная последовательность $\{c_i\}_n$ является закодированным сообщением.

Для восстановления информации обязательно необходимо иметь саму последовательность $\{c_i\}_n$ иметь x_0 и знать использованную при шифрации дискретную динамическую систему $x \to f_\lambda(x)$. Восстановление заключается в воссоздании хаотической траектории $\{x_i\}_n$ и выделении из $\{c_i\}_n$ обратной операцией $\{s_i\}_n$.

При использовании компьютера с операционной системой Windows 9x была реализована программа, позволяющая зашифровать и восстановить исходное сообщение или файл. В ней в качестве дискретной динамической системы была применена система вида:

$$x \to 4 \cdot x \cdot (1 - x)$$

и для слияния двух сигналов $\{s_i\}_n$ и $\{x_i\}_n$ вначале они нормировались, а затем применялось, для слияния, обычное алгебраическое сложение.

Результаты работы кодирующей программы представлены на рисунке, на нем графически представлена закодированная последовательность 30 повторяющихся символов "c"

Полученный сигнал невозможно отличить от шума, к тому же для расшифровки необходимо знать конкретный вид динамической системы и начальный параметр x_0

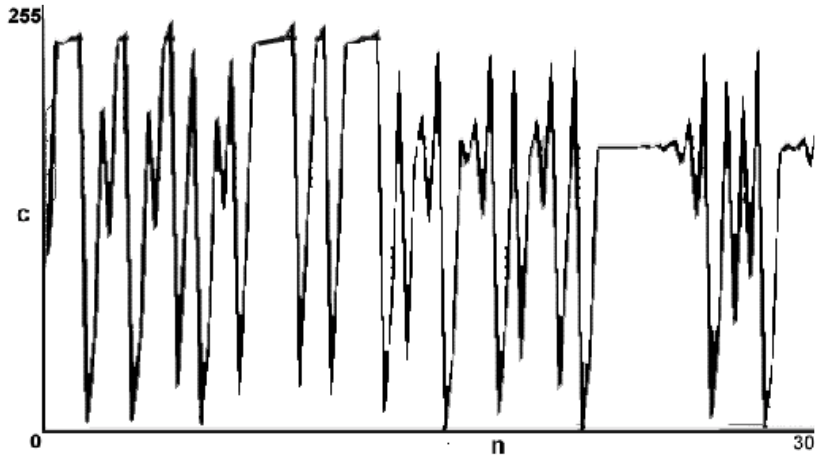

Рис. 1

Список литературы

[1] Шустер Г. Детерминированный хаос. Введение. - М. "Мир", 1988
[2] Шарковский А.Н., Коляда С.Ф., Сивак А.Г., Федоренко В.В. Динамика одномерных отображений. - Киев Наукова думка 1989