В. В. Андреев, Ю. В. Сапожникова, А. И. Фомичев

Детерминированный хаос и кодирование информации

В работе разработаны и исследованы два алгоритма кодирования информации на основе детерминированного хаоса. В качестве генератора хаоса использован аттрактор Лоренца. Найдены оптимальные параметры кодирования.

В связи с бурным развитием компьютерных сетей, интернет-технологий и беспроводных систем связи появляется все больше задач, связанных с кодированием информации, которые трудно решить, используя только традиционные подходы.

Например, интенсивный рост производительности процессоров, сводящий на нет многие традиционные криптографические решения, стимулирует разработку новых принципов кодирования.

Одним из альтернативных подходов здесь является применение теории динамического детерминированного хаоса. В системах с динамическим хаосом наблюдается, в частности, сильная чувствительность к изменению начальных данных. Поведение таких систем невозможно предсказать на достаточно длительных временных интервалах.

Следует отметить, что в настоящее время большое внимание уделяется разработке алгоритмов шифрования, основанных на хаосе [1, 2]. В работе [2] был предложен новый метод кодирования графической информации с использованием хаотического генератора. Метод основан на изменении цвета каждого образа символа согласно псевдослучайному закону.

В настоящей работе, как и в [3], в качестве генератора хаоса использован аттрактор Лоренца, описываемый системой дифференциальных уравнений [4]:

$$\begin{cases} -\dfrac{dX}{dt} = -\sigma X + \sigma Y, \\ \dfrac{dY}{dt} = -XZ + rX - Y, \\ \dfrac{dZ}{dt} = XY - bZ. \end{cases} \qquad (1)$$

Здесь $r = 28, \sigma = 10, b = \dfrac{8}{3}$, t — время. На рис. 1 и 2 изображены кривые, полученные из решений системы уравнений Лоренца следующим образом:

$$f(t) = AX(t) + BY(t) + CZ(t). \qquad (2)$$

Здесь $A = B = C = 0{,}016$. Для указанных на рис. 1 и 2 кривых начальные условия $X(0)$ отличаются на одну миллионную долю. Видно (см. рис. 1, 2), что при временах t, больших двадцати условных единиц, траектории систем становятся совершенно непохожими.

В работе были разработаны и исследованы два алгоритма кодирования данных на основе динамического детерминированного хаоса.

Способ I

Для шифрования сигнала использован следующий алгоритм.

1. Отсчеты исходного звукового сигнала $s(t)$ (см. рис. 3) сортируем по возрастанию. При этом, если среди отсчетов встречается несколько одинаковых, оставляем только один из них. В результате получаем массив m1unique (см. рис. 4 и 5).

2. В массиве n_1 запоминаем номера отсчетов исходного сигнала, совпадающих по уровню с каждым из элементов массива m1unique (см. рис. 5). Таким образом, размерность массива n_1 равна размерности массива $s(t)$.

3. В массиве n_2 запоминаем количество повторений в исходном сигнале каждого из отсчетов, записанных в массив m1unique (см. рис. 5). Следовательно, массивы m1unique и n_2 имеют одинаковую размерность.

4. Умножаем каждый элемент массива m1unique на постоянный коэффициент k,