КОДИРОВАНИЕ И СЖАТИЕ ДАННЫХ С ПРИМЕНЕНИЕМ ХАОСА

Андреев В.В., Степанова М.В.

ФГОУ ВПО «Чувашский государственный университет имени И.Н.Ульянова», кафедра «Телекоммуникационные системы и технологии», Россия, 428015, г. Чебоксары, Московский пр., 15, E-mail: andreev_vsevolod@mail.ru

В связи с бурным развитием компьютерных сетей, интернет-технологий и беспроводных систем связи появляется все больше задач, которые трудно решить, используя только традиционные подходы. Одним из альтернативных подходов является применение теории динамического хаоса. Здесь есть два аспекта, на которых следует заострить внимание: 1) интенсивный рост производительности процессоров, сводящий на нет многие традиционные криптографические решения, стимулирует разработку новых принципов кодирования информации; 2) схемы кодирования, основанные на хаосе, в большинстве случаев оказываются более медленными и криптографически более слабыми, чем их традиционные аналоги. Следует отметить, что хаотические системы по своей природе, как правило, непрерывны. Поэтому многие методы шифрования, разработанные в традиционной криптографии, не применимы для хаотической.

В данной работе исследованы методы шифрования и сжатия информации, основанные на применении хаоса. В качестве генератора хаоса использован аттрактор Лоренца:

$$\frac{dx}{dt} = a(y - x), \quad \frac{dy}{dt} = x(b - z) - y, \quad \frac{dz}{dt} = xy - cz.$$

Здесь были заданы следующие значения параметров: $a = 10$, $b = 27.7$, $c = 8/3$. С помощью аттрактора Лоренца был получено цветное изображение, представленное на рис.1.

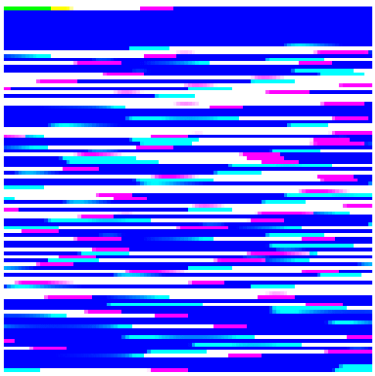

Рис. 1

Подбором параметров и начальных условий аттрактора Лоренца можно добиться совпадения в достаточной степени отдельных фрагментов шифруемого образа с образами, генерируемыми с помощью аттрактора Лоренца. Тогда объём зашифрованной информации существенно уменьшится, так как достаточно сложный образ кодируется относительно небольшим количеством наборов параметров и начальных условий аттрактора Лоренца. Кроме того, учитывая, что аттрактор Лоренца очень чувствителен к малым изменениям параметров и начальных условий, исследованный метод проявляет высокую устойчивость к несанкционированным попыткам дешифрования информации. Недостатком метода является то, что значительно увеличивается время, необходимое для шифрования. Проведённый анализ показал эффективность исследованного метода кодирования.