Хаотическая маршрутизация как метод преобразования информации

Ю.П. Шанкин

«Мир сложен – правила просты».

В настоящее время есть основания говорить о пересечении предметных областей общей теории нелинейных динамических систем, имеющей богатейший научный потенциал (со времен трудов Ляпунова и Пуанкаре), и традиционной криптографии, базирующейся на методах и инструментах дискретной математики, алгебры и теории чисел (примеры и список литературы можно найти, в частности, в работах [1, 2]). Собственно непредсказуемость хаотических систем может быть интерпретирована как наличие «криптосвязи» их поведения с простейшими физическими законами. Пример подобного подхода к преобразованию информации, несводящейся к традиционным способам модуляции или аддитивного сложения информационного и случайного сигналов, рассмотрен ниже.

Как известно [3], информационно – насыщенные символические последовательности могут генерироваться неравновесными системами в состоянии хаотического аттрактора (символическая динамика), что, в свою очередь, может рассматриваться в качестве текста из гиперсимволов, возникающих при соответствующем марковском разбиении множества возможных состояний системы. При определенных условиях символьный «текст» может быть взаимооднозначно увязан с исходным состоянием динамической системы, находящейся в режиме хаотического поведения.

Рассмотрим случай одномерного непрерывного кусочно-гладкого расширяющего (то есть с числом Ляпунова $\alpha \geqslant const > 1$) отображения f отрезка $A = [P_0, P_k]$ длины L на себя $(A \to A)$

Пусть: $P_0 < P_1 < ... < P_k$, $A_i = [P_{i-1}, P_i]$, $i = 1, 2, ..., k$ – растягивающее разбиение данного отрезка (одномерный аналог марковского разбиения). В этом случае справедлива теорема [4], согласно которой:

- любая возможная конечная символьная последовательность $A_1 \dots A_n$ взаимооднозначно соответствует некоторому подинтервалу отрезка A длины

$$\delta_n \leqslant \frac{L}{\alpha^{n-1}} \quad ; \tag{1}$$

- любая возможная бесконечная символьная последовательность $A_1 A_2 A_3 \dots$ соответствует единственной точке x_0 интервала A, генерирующей хаотическую орбиту $f(f...f(x)...)$ (в случае, если символьная последовательность не является периодической).

В соответствии с данной теоремой исходная информация, содержащаяся в дробной части числа $x_0 \in A$ (в общем случае – иррационального), задающего начальное состояние итерационного процесса

$$x_{n+1} = f(x_n), \quad n = 0, 1, 2, \dots, \tag{2}$$

взаимооднозначным образом преобразуется в «маршрут» (символьную последовательность) $\overrightarrow{I} = \{A_{i_n}\}$, такой, что $f(x_n) \in A_{i_n}$, $i_n \in [1, k]$.

Если положить $L = 1$, $\delta_n = 10^{-s_n}$, $\lambda = \ln \alpha$ – показатель Ляпунова, то можно записать:

$$S_n \geqslant \frac{(N-1)\lambda}{\ln 10}, \tag{3}$$

то есть N символов маршрута соответствует не менее, чем S_n символам «десятичного текста», записанного в начальном состоянии динамической системы.

Можно доказать, что любое возмущение маршрута $\overrightarrow{I}$ приводит к полной потере исходного десятичного текста, отвечающего той части маршрута, которая следует за внесенным возмущением (даже при полной ее тождественности первоначальному маршруту).

Действительно, пусть $L = 1$ и возмущение внесено в $(N+1)$ символ маршрута $\overrightarrow{I}$. Это означает, что на $(N+1)$ шаге итераций

$$f^{N+1}(x_0) = \underbrace{f(f(f...f}_{N+1}(x_0)...)$$

неправильно определен очередной элемент $A_{i_{N+1}}$ исходного марковского разбиения отрезка $A = [0,1]$. Предшествующие N «правильных» символов маршрута соответствуют, согласно (1), некоторому интервалу длиной δ^*:

$$\delta^* \sim \frac{1}{\alpha^{N-1}},$$

содержащему точку x_0, а дальнейший неправильный выбор $(N+1)$-го символа маршрута соответствует ошибочному выбору участка на оси x при последующем разбиении отрезка длины δ^* на составляющие меньшей длины, (в результате чего на $(N+1)$-м и дальнейших шагах итераций выбираются интервалы на оси x, фактически не содержащие точки x_0).

Таким образом, величина δ^* может рассматриваться как погрешность в определении начального состояния системы x_0 при возмущении маршрута на $(N+1)$-м шаге:

$$\Delta x_0 = \delta^*.$$

С другой стороны, скорость разбегания траекторий динамических систем характеризуется показателем Ляпунова $\lambda = \ln \alpha$, в силу чего погрешность в определении положения через M шагов может быть записана в виде:

$$\Delta x_M = \Delta x_0 e^{\lambda M} = \delta^* e^{\lambda M} \approx e^{\lambda M - \lambda(N-1)}, \quad (\lambda > 0)$$

При $M > N$ погрешность Δx_M становится больше длины исходного интервала, то есть теряется какая-либо связь участка маршрута при $N > M$ с реальным начальным положением системы.

Упростим задачу еще раз, полагая, что исходное марковское разбиение сводится к выбору либо правого (R), либо левого (L) подинтервала исходного отрезка $[0,1]$ при некотором его разбиении, анало-

гичном изображенному на рис. 1 (где в качестве линейного отображения f приведено отображение типа «tent–map»). Появление «буфера» (B) перед «текстовой» частью (T) обусловлено необходимостью выхода системы на хаотический режим (формирование предельного цикла).

Нетрудно показать, что «размер» (число десятичных разрядов – B) буфера перед информационным текстом определяет верхнюю оценку размерности «ключевого пространства» рассматриваемого нелинейного преобразования. Объем «ключевого пространства» определяется числом параметрических кластеров, задаваемых порогом дискретизации допустимого вида преобразования или его основных параметров (при выполнении условий «марковского разбиения»). Восстановление текста возможно только в случае использования (при решении прямой и обратной задачи) исходных данных, принадлежащих одному кластеру. Число кластеров N (длина «ключа») существенным образом зависит от числа степенной свободы (числа независимых параметров – P) системы и длины «буфера» (B):

$$N \leqslant 10^{PB}$$

Собственно восстановление текста ($\overrightarrow{x}$) по заданному маршруту ($\overrightarrow{I}$) при заданной функции отображения f возможно при чтении маршрута (I) как слева направо, так и справа налево, однако алгоритм чтения и его основные параметры (трудоемкость и устойчивость) при этом существенно различны.

В случае обратного («арабского» – то есть справа налево) чтения маршрута I строится обратное отображение f^{-1}, неоднозначность которого устраняется выбором правой или левой его ветви в соотношении с заданным маршрутом ($\overrightarrow{I}$). Это отображение легко реализуемо, однако весьма чувствительно к точному значению размерности «блока» информационного текста, определяемого разрядностью используемой вычислительной системы или прецезионной точностью приборов в случае аналоговой реализации преобразования (2).

При «латинском» (слева направо) чтении маршрута ($\overrightarrow{I}$) для восстановления исходного текста ($\overrightarrow{x}$) по заданной функции f алгоритм существенно более трудоемкий, так как связан с вычислением корней уравнений типа

$$f(f...f(x_0)...) - x = 0 \tag{4}$$

с предельной точностью, определяемой разрядностью вычислительной системы (в целях достоверного определения границ интервала для поиска корней уравнения (4) на последующем этапе итераций). Вместе с тем «латинское» чтение маршрута инвариантно к длине исходного информационного блока.

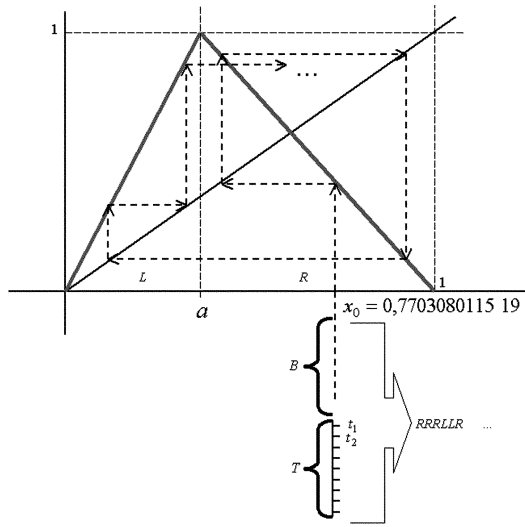

Рис. 1.

Задача однозначного восстановления неизвестной функции f по известным начальным данным $\overrightarrow{x}$ и маршруту $\overrightarrow{I}$ («атака по открытому тексту») является некорректно поставленной и ее решение не представляется возможным при отсутствии априорной информации о виде отображения f.

В качестве примера рассмотрим слово «CHAOS», десятичная запись которого в виде начального состояния $\overrightarrow{x_0}$ имеет вид:

$$x_0 = 0,770308011519 \tag{5}$$

Здесь две семерки (77) выполняют роль буфера, а последующие цифры соответствуют порядковому номеру букв английского алфа-

вита в слове «CHAOS». В случае ранее упомянутого преобразования f в виде «tent–map» (рис. 1) и параметре $a = 0,3$ начальному значению (5) преобразования (2) отвечает маршрут:

$$\overrightarrow{I} = RRRLLRRRRRRRLRRRR\ldots, \tag{6}$$

общая длина которого, однозначно соответствующая начальному значению (5), в соответствии с оценкой (3) составляет примерно 55 символов. (Один и тот же вид маршрута (6) при различных значениях параметра «a» может соответствовать совершенно разным начальным «текстам»).

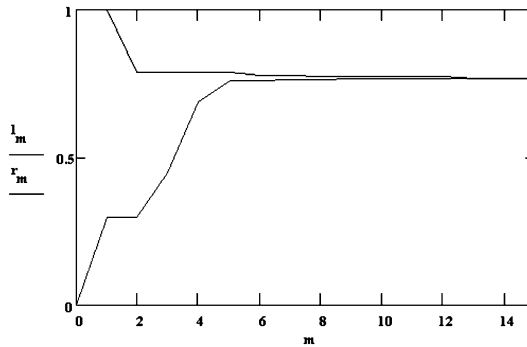

Рис. 2.

На рис. 2 приведены результаты «латинского» чтения маршрута (6) при заданном виде преобразования f. По оси абсцисс отложены порядковые номера отдельных символов маршрута (6). Ось ординат отвечает исходному отрезку $[0, 1]$ оси x. При этом верхняя кривая на рис. 2 отвечает верхней границе подинтервала, содержащего исходное значение x_0, а нижняя кривая – нижней границе этого же подинтервала. Как видно из рисунка, эти границы последовательно сближаются при чтении маршрута, приводя в конечном итоге к полному восстановлению начального значения (5), а значит и восстановлению исходного слова «CHAOS».

Более сложный вид отображения f (например, в случае нелинейного вида ребер в отображении «tent–map» или при увеличении числа «структурных параметров» отображения) существенно осложня-

ет решение обратной задачи посторонним лицом, не имеющим информации о виде отображения f. При этом, однако, как прямое («латинское»), так и обратное («арабское») чтение маршрута «доверенным лицом» (при известной функции f) однозначно восстанавливает исходный текст при обязательном выполнении условий марковского разбиения исходного отрезка $[0, 1]$, соответствующего виду отображения f. В случае нарушения условий марковского разбиения строгое решение обратной задачи формально остается возможным, но приводит к численному значению $\overline{x_0}$, отличному от исходного значения x_0.

Описанный метод преобразования информации на основе хаотической маршрутизации исходного текста обеспечивает строгое взаимооднозначное соответствие:

$$(f, \overrightarrow{I}) \to x_0$$
$$(f, x_0) \to I$$

между элементами триады

$$(f/\{A\}, \overrightarrow{I}, x_0),$$

включающей в себя собственно нелинейное отображение f с соответствующим марковским разбиением $\{A\}$, вектор маршрута $\overrightarrow{I}$ и начальное состояние x_0.

Как прямое ($x_0 \to \overrightarrow{I}$), так и обратное ($\overrightarrow{I} \to x_0$) преобразование легко реализуемо численно или в аналоговом виде, при этом объем одноактно передаваемой информации определяется разрядностью ЭВМ или прецензионной точностью физических систем, реализующих заданное нелинейное отображение f.

Отображение ($x_0 \to \overrightarrow{I}$) и ($\overrightarrow{I} \to x_0$) являются последовательными отображениями с последствиями: предшествующие элементы отображений существенным образом влияют на формирование последующих.

В случае численной реализации алгоритма хаотической маршрутизации (при конечной разрядности представления данных) или с учетом ограниченной приборной точности соответствующих аналоговых физических систем возможно поблочное разбиение исходного

текста на подсистемы конечной длины, отвечающие самостоятельным (независимым) начальным значениям хаотического маршрутизатора.

Список литературы

[1] Gutowitz H. Cryptography with Dynamical Systems. 1995. (http://www.santafe.edu/~had/crpto.html).

[2] Андреев Ю.В. и др. Стратегии использования динамического хаоса в коммуникационных системах и компьютерных сетях // Зарубежная радиоэлектроника. 2000. №11. С. 4-26.

[3] Николис Г., Пригожин И. Познание сложного. М.: Мир, 1990.

[4] Alligood K.T., Sauer T.D., Yorke I.A. CHAOS. Springer, 1996.