Кодирование двоичной последовательности с использованием дискретных хаотических отображений

06, июнь 2012

DOI: 10.7463/0612.0402537

Митин С. В.

УДК 621.391

Россия, МГТУ им. Н.Э. Баумана

tician7506@gmail.com

Введение

Возможность использования хаотических сигналов для передачи информации впервые была продемонстрирована в 1993 году, после чего хаотические системы связи стали объектом пристального изучения [1-5]. Интерес к хаотическим системам связи связан с хорошими свойствами сигналов, создаваемых хаотическими системами с точки зрения разработки защищенных систем связи и систем множественного доступа. В случае защищенных систем связи, можно использовать некоррелированность и непредсказуемость хаотических сигналов для построения алгоритмов кодирования.

При разработке алгоритмов кодирования, основанных на дискретных хаотических отображениях, одной из основных задач является исследование взаимосвязи между функцией плотности вероятности полученных данных и значением отображения. Задача получения требуемого отображения начинается с необходимой функции плотности вероятности. Знание функции плотности вероятности помогает в оценке производительности возможных систем. Сложность состоит в практической разработке алгоритма кодирования, такого, чтобы получить реальную модель передатчика. Одной из возможностей является использование известного алгоритма кодирования основанного на отображении сдвига Бернулли и распространении на целый класс дискретных хаотических отображений. Разработка отображения требует некоторых ограничений, касающихся формы функции плотности вероятности и характеристик окончательного отображения, сопряженного отображению сдвига Бернулли.

Целью работы является разработка хаотического отображения с заданной функцией плотности вероятности и исследование алгоритма кодирования двоичных последовательностей с использованием полученного отображения.

Синтез кодирующего отображения

Для кодирования информационной двоичной последовательности $\{b_n\}$, где $b_n \in \{0,1\}$, $n = 1 \dots N$, будем использовать широко известный метод [10, 6, 7, 8], основанный на эффекте усечения.

Последовательность $\{b_n\}$ двоичная, независимая и равновероятная $p_0 = p_1 = 1/2$. Интересующие нас отображения ограничены интервалом $[0,1]$ и представляют собой отображение сдвига Бернулли

$$x_{n+1} = f(x_n) = \begin{cases} 2x_n, & \text{если } x_n < \frac{1}{2}, \\ 2x_n - 1, & \text{если } x_n \geq \frac{1}{2}, \end{cases}$$

и модифицированное логистическое отображение

$$x_{n+1} = f(x_n) = \begin{cases} 4x_n(1-x_n), & \text{если } x_n \in \left[0, \frac{1}{2}\right], \\ 1 - 4x_n(1-x_n), & \text{если } x_n \in \left[\frac{1}{2}, 1\right], \end{cases}$$

показанные на рисунке 1.

Рис. 1. Вид отображения сдвига Бернулли и модифицированного логистического отображения

Хорошо известным является следующее свойство отображения сдвига Бернулли [9]: если задать состояние системы r как

$$r = \sum_{n=1}^N b_n 2^{-n}$$

и взять $x_0 = r$ в качестве начального значения хаотической последовательности, то двоичная последовательность кодируется в хаотическую последовательность, генерируемую x_0 , значения которой определяются формулой

$$x_n = f(x_{n-1}) = f^n(x_0) = \sum_{m=n+1}^N b_m 2^{-m+n},$$

где $f^n(x)$ – результат применения отображения n раз. Информация из полученной последовательности может быть восстановлена в соответствии с выражением

$$b_n = \left[x_n + \frac{1}{2} \right], \quad (1)$$

где $[x]$ – максимальное целое, меньшее x .

Аналогично, если в случае модифицированного логистического отображения

$$x_0 = c \cdot 2 \left[\frac{\pi}{2} s(1-r) \right],$$

то имеет место то же свойство, определяемое формулой (1). Функция $x_0 = g(r)$, если она существует для определенного отображения, делает возможной передачу информации хаотической последовательностью, сгенерированной этим отображением, восстановление которой осуществляется в соответствии с формулой (1). Если отображения являются сопряженными, как в случае отображения сдвига Бернулли и модифицированного логистического отображения, функция $g(r)$ существует и связана с плотностью вероятности

$p(x)$ такого отображения как $g(r) = F^{-1}(r)$ [6], где $F(x) = \int_0^x p(x) dx$ – функция распределения плотности вероятности [6].

В реальной системе, где длина N сообщения может достигать тысяч бит, рассмотренный процесс кодирования не имеет практического применения, поскольку он подразумевает практически бесконечную точность вычислений. В этом случае, данный метод можно применять для кодирования блоками из $D \ll N$ бит за один раз. Если задать усеченную символьную последовательность как r'_n , соответствующее усеченное значение x'_n для отображения сдвига Бернулли

$$r'_n = \sum_{m=n}^{n+D-1} b_m 2^{-m+n-1}, \quad (2)$$

$$x'_n = g(r'_n),$$

где $g(r)$ определяется аналогично отображению сдвига Бернулли, для которого этот способ был впервые разработан [6-8, 10]. Однако можно распространить данный метод кодирования на широкий класс сопряженных отображений.

Рассмотрим процесс синтеза отображения, плотность вероятности которого имеет форму, как у модифицированного логистического отображения с максимумом в точке $1/2$:

$$p(x) = \frac{1}{\pi \sqrt{\left(x + \frac{1}{2}\right)\left(\frac{1}{2} - x\right)}}, \quad x \in \left[0, \frac{1}{2}\right),$$

$$p(x) = \frac{1}{\pi \sqrt{\left(x - \frac{1}{2}\right)\left(\frac{3}{2} - x\right)}}, \quad x \in \left(\frac{1}{2}, 1\right]. \quad (3)$$

Это отображение также является сопряженным отображению сдвига Бернулли. Будем называть его перевернутым логистическим отображением (ПЛО). Плотности вероятности всех трех отображений показаны на рисунке 2.

Рис. 2. Функции плотности вероятности для отображений Бернулли, модифицированного логистического и перевернутого логистического.

Функцию $g(r)$ получим из функции распределения отображения, используя соотношение $g(r) = F^{-1}(r)$. В случае отображения, сопряженного отображению сдвига Бернулли, если начальное состояние для отображения Бернулли $x_0^B = r$, а

начальное состояние для сопряженного отображения $x_0^C = g(r)$, то все члены хаотических последовательностей связаны выражением

$$f_C^n(x_0^C) = f_C^n[g(r)] = g[f_B^n(r)] = g[f_B^n(x_0^B)], \quad (4)$$

где $f_C^n(x)$ – n -я итерация сопряженного отображения, $f_B^n(x)$ – n -я итерация отображения сдвига Бернулли. Последнее выражение является прямым следствием определения сопряженных отображений f_1 и f_2 , $f_1(x) = \phi\{f_2[\phi^{-1}(x)]\}$, где $\phi(x)$ – функция, отображающая интервал $[0,1]$ в себя. Усеченный процесс кодирования (2) использует это свойство.

Таким образом, следующим этапом процесса синтеза отображения является нахождение выражения для $f_C(x)$, используя функцию плотности вероятности и свойство (4). Так как $g(r) = F^{-1}(r)$ и функция плотности вероятности симметрична относительно точки $\frac{1}{2}$, функция $g(r)$ обладает свойствами

$$g(0) = 0, \quad g\left(\frac{1}{2}\right) = \frac{1}{2}, \quad g(1) = 1,$$

$$g\left(\left[0, \frac{1}{2}\right]\right) = \left[0, \frac{1}{2}\right], \quad g\left(\left[\frac{1}{2}, 1\right]\right) = \left[\frac{1}{2}, 1\right],$$

а также является монотонно возрастающей функцией. Учитывая соотношение (4) и форму отображения Бернулли, новое отображение $f_C(x)$ будет обладать следующим свойством:

$$f_C[g(r)] = \begin{cases} g(2r), & \text{е с } r \leq \frac{1}{2}, \\ g(2r-1), & \text{е с } r > \frac{1}{2}. \end{cases}$$

Поскольку $g(r)$ обратимая функция, обозначая $g(r) = x$ и $r = g^{-1}(x)$, получим

$$f_C(x) = \begin{cases} g[2g^{-1}(x)], & \text{е с } x \leq \frac{1}{2} \\ g[2g^{-1}(x)], & \text{е с } x > \frac{1}{2} \end{cases}$$

что является основным выражением для нового отображения, при условии, что его функция плотности вероятности лежит в интервале $[0,1]$ и является симметричной относительно точки $\frac{1}{2}$.

Производя математические преобразования, можно получить $F(x)$, $g(r)$ и непосредственно отображение для функции плотности вероятности (3):

$$F(x) = \begin{cases} \frac{1}{2} - \frac{2}{\pi} \arcsin \left(\sqrt{x + \frac{1}{2}} \right), & \text{если } x \leq -\frac{1}{2}, \\ \frac{3}{2} - \frac{2}{\pi} \arcsin \left(\sqrt{x - \frac{1}{2}} \right), & \text{если } x \geq \frac{1}{2}, \end{cases}$$

$$g(r) = \begin{cases} \arcsin \left[\frac{\pi}{2} \left(\frac{1}{2} - r \right) \right] - \frac{1}{2}, & \text{если } x \leq \frac{1}{2}, \\ \arcsin \left[\frac{\pi}{2} \left(\frac{3}{2} - r \right) \right] + \frac{1}{2}, & \text{если } x \geq \frac{1}{2}, \end{cases}$$

$$f(x_n) = \begin{cases} 4x_n \sqrt{\frac{1}{4} - x_n^2}, & \text{если } 0 \leq x_n < \frac{1}{2\sqrt{2}}, \\ 1 - 4x_n \sqrt{\frac{1}{4} - x_n^2}, & \text{если } \frac{1}{2\sqrt{2}} \leq x_n < \frac{1}{2}, \\ 4(1 - x_n) \sqrt{\frac{1}{4} - (1 - x_n)^2}, & \text{если } \frac{1}{2} \leq x_n < 1 - \frac{1}{2\sqrt{2}}, \\ 1 - 4(1 - x_n) \sqrt{\frac{1}{4} - (1 - x_n)^2}, & \text{если } 1 - \frac{1}{2\sqrt{2}} \leq x_n \leq 1. \end{cases} \quad (5)$$

Функции $g(r)$ для трех отображений иллюстрирует рисунке 3.

Рис. 3. Различные функции $g(r)$ для отображений Бернулли, модифицированного логистического и перевернутого логистического.

Отображение ПЛО (5) показано на рисунке 4.

Рис. 4. Перевернутое логистическое отображение

Можно использовать эти три отображения для кодирования двоичной последовательности, применяя формулу (2). Необходимо отметить, что для процесса кодирования требуется только функция $g(r)$, но для процесса декодирования потребуется и само отображение $f(x)$.

Результирующая усеченная последовательность x'_n близка к оригинальной последовательности x_n , когда число бит D достаточно велико, и этот процесс эквивалентен добавлению шума $x'_n = x_n + \eta_n$.

Значение $\eta_n = - \sum_{m=n+D+1}^N b_m 2^{-m+n}$ можно приближенно рассматривать как шумовую последовательность, влияние которой уменьшается с увеличением D . Заметим также, что метод усечения – это пример квантизации x_n с точностью D бит, поэтому существует всего 2^D различных значений для x'_n . Поэтому полученная последовательность соответствует дискретному хаотическому отображению. Таким образом, получаем пару кодирующих функций

$$r_n = \sum_{m=n+1}^{n+D} b_m 2^{-m+n},$$

$$x_n = g(r_n),$$

которые можно использовать для кодирования данных с помощью отображения сдвига Бернулли или других сопряженных отображений.

Закодированная последовательность передается по каналу связи, где к ней добавляется шум, а затем принимается и декодируется на принимающей стороне. Модель коммуникационной системы можно представить в виде схемы, изображенной на рисунке 5.

Рис. 5. Схема системы связи с хаотическим кодированием

Шум в канале связи можно представить в виде гауссовского белого шума с нулевым математическим ожиданием и мощностью σ^2 . Плотность вероятности такого шума

$$p(n) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{n^2}{2\sigma^2}}.$$

Эта хорошо известная в телекоммуникациях модель, которая позволяет абстрагироваться от различных влияний, вносимых обычными каналами. Наличие шума необходимо учитывать в процессе декодирования.

Заключение

В данной статье рассмотрен метод кодирования двоичной последовательности с использованием дискретных хаотических отображений. Показано, что в реальных системах необходимо применять метод усечения для кодирования сообщения блоками бит. Проведен синтез хаотического отображения с заданной функцией плотности вероятности, приведены графики отображений и функций, при помощи которых производится кодирование двоичной последовательности.

Литература

1. Дмитриев А.С. Динамический хаос как носитель информации // Новое в синергетике: Взгляд в третье тысячелетие : монография / РАН.- М.: Наука.- 2002. – С. 82-122. (Информатика: неограниченные возможности и возможные ограничения).
2. Волковский А. Р., Рульков Н. В. Синхронный хаотический отклик нелинейной системы передачи информации с хаотической несущей // Письма в ЖТФ. – 1993. – № 3. – С. 71–75.
3. Дмитриев А.С., Кузьмин Л.В., Панас А.И., Старков С.О. Эксперименты по передаче информации с использованием хаоса через радиоканал // Радиотехника и Электроника. – 1998. – Т.43. – №9. – С. 1115–1128.
4. Дмитриев А.С., Кузьмин Л.В., Панас А.И. Схема связи с суммированием по модулю хаотического и информационного сигналов // Радиотехника и электроника. – 1999. – Т. 44. – № 8. – С. 988–996.
5. Хаслер М. Передача информации с использованием хаотических сигналов // Зарубежная радиоэлектроника. – 1998. – № 11. – С. 33–43.
6. Kozic S., Schimming T. Coded Modulation Based on Higher Dimensional Chaotic Maps // Proc. of the International Symposium on Circuits and Systems (ISCAS 2005) (23-26 May 2005, Japan, Kobe). IEEE. 2005. Vol. 2. PP. 888-892.
7. Baptista M., Lopez L. Information transfer in chaos-based communication // Physical Review E - Statistical, Nonlinear and Soft Matter Physics, 2002. vol 65. no. 5. PP. 0552011-0552014.
8. Kozic S., Oshima K., Schimming T. Minimum Distance Properties of Coded Modulations Based on Iterated Chaotic Maps // Proc. of the 11th International IEEE Workshop on Nonlinear Dynamics of Electronic Systems (NDES 2003) (Scuol/Schuls, Switzerland, 18-21 May 2003). 2003. PP.141–144.
9. Chen B., Wornell G. W. Analog Error-Correcting Codes Based on Chaotic Dynamical Systems // IEEE Trans. Commun., July 1998, vol. 46, no. 7, pp. 881-890.
10. Kozic S., Oshima K., Schimming T. How to repair CSK using small perturbation control - Case study and performance analysis // Proc. of the European Conference on Circuit Theory and Design 2003 (ECCTD 2003) (Cracow, Poland, 1-4 September 2003). Krakow, Poland. 2003. Vol. 3. PP. 249-252.

Encoding of the binary sequence with the use of discrete chaotic maps

06, June 2012

DOI: 10.7463/0612.0402537

Mitin S.V.

Russia, Bauman Moscow State Technical University

tician7506@gmail.com

This article presents a method of encoding of the binary sequences with the use of discrete chaotic maps. It was shown that in real systems the method of truncation to encode a message by blocks of bits should be used. The synthesis of a chaotic map with the specified probability density function was carried out. Maps and functions' graphs, which are using for encoding of the binary sequence, are also included in the article.

Publications with keywords: [encoding](#), [chaos](#), [chaotic communication](#)**Publications with words:** [encoding](#), [chaos](#), [chaotic communication](#)

References

1. Dmitriev A.S. Dinamicheskii khaos kak nositel' informatsii [Dynamic chaos as a carrier of information]. In book: *Novoe v sinergetike: Vzgliad v tret'e tysiacheletie* [New in synergy: A Look into the third millennium]. Moscow, Nauka, 2002, pp. 82-122. (*Informatika: neogranichennye vozmozhnosti i vozmozhnye ogranicheniia* [Informatics: unlimited possibilities and possible limitations]).
2. Volkovskii A. R., Rul'kov N. V. Sinkhronnyi khaoticheskii otklik nelineinoi sistemy peredachi informatsii s khaoticheskoi nesushchei [Synchronous chaotic response of a nonlinear system of information transmission with the chaotic carrier]. *Pis'ma v Zhurnal Tekhnicheskoi Fiziki* [Letters to Journal of Technical Physics], 1993, no. 3, pp. 71–75.
3. Dmitriev A.S., Kuz'min L.V., Panas A.I., Starkov S.O. Eksperimenty po peredache informatsii s ispol'zovaniem khaosa cherez radiokanal [Experiments on the transmission of information using chaos via a radio channel]. *Radiotekhnika i Elektronika*, 1998, vol. 43, no. 9, pp. 1115–1128.
4. Dmitriev A.S., Kuz'min L.V., Panas A.I. Skhema svyazi s summirovaniem po moduliu khaoticheskogo i informatsionnogo signalov [The scheme of connection with the summation modulo of the chaotic and information signals]. *Radiotekhnika i elektronika*, 1999, vol. 44, no. 8, pp. 988–996.
5. Khasler M. Peredacha informatsii s ispol'zovaniem khaoticheskikh signalov [The transmission of information using chaotic signals]. *Zarubezhnaia radioelektronika*, 1998, no. 11, pp. 33–43.

6. Kozic S., Schimming T. Coded Modulation Based on Higher Dimensional Chaotic Maps. *Proc. of the International Symposium on Circuits and Systems (ISCAS 2005)*, 23-26 May 2005, Japan, Kobe. IEEE, 2005, vol. 2, pp. 888-892.
7. Baptista M., Lopez L. Information transfer in chaos-based communication. *Physical Review E - Statistical, Nonlinear and Soft Matter Physics*, 2002, vol. 65, no. 5, pp. 0552011-0552014.
8. Kozic S., Oshima K., Schimming T. Minimum Distance Properties of Coded Modulations Based on Iterated Chaotic Maps. *Proc. of the 11th International IEEE Workshop on Nonlinear Dynamics of Electronic Systems (NDES 2003)*. Scuol/Schuls, Switzerland, 2003, pp.141–144.
9. Chen B., Wornell G. W. Analog Error-Correcting Codes Based on Chaotic Dynamical Systems. *IEEE Trans. Commun.*, 1998, vol. 46, no. 7, pp. 881-890.
10. Kozic S., Oshima K., Schimming T. How to repair CSK using small perturbation control - Case study and performance analysis. *Proc. of the European Conference on Circuit Theory and Design 2003 (ECCTD 2003)*. Krakow, Poland, 2003, vol. 3, pp. 249-252.