

Схема хаотической маскировки сообщений на основе ортогональных функций

С.В. Белим
sbelim@mail.ru

Ю.С. Ракицкий
yrakitsky@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

В статье предложен метод хаотической маскировки дискретного сигнала. Предложенный подход не требует синхронизации хаотических генераторов и устойчив к шумам в канале связи. Эти свойства снимают основную проблему хаотической маскировки, связанную с рассинхронизацией управляющих параметров. Основная идея состоит в использовании кодирования сообщения с помощью ортогональных функций. Далее применяется простое суммирование скрытого сообщения с хаотическим сигналом. Извлечение сообщения может быть выполнено на основе свойства ортогональности без вычитания хаотической составляющей.

Введение

Для скрытой передачи сообщений могут использоваться различные подходы на основе стеганографических алгоритмов, электронной цифровой подписи [1, 2], динамического хаоса [3] и т.д. Эти методы отличаются друг от друга, прежде всего контейнером, используемым для встраивания сообщения. Контейнер служит для маскировки факта передачи сообщения. В данной статье предложен алгоритм, основанный на маскировке сообщения с помощью динамического хаоса, получивший название хаотической маскировки.

Использование динамического хаоса для сокрытия передаваемого сообщения предполагает наличие двух связанных идентичных хаотических генераторов. Разработаны несколько способов использования динамического хаоса в таких задачах: хаотическая маскировка [4], переключение хаотических режимов [5] нелинейное подмешивание передаваемого сообщения к хаотическому сигналу [6], модулирование управляющих параметров хаотического генератора [7]. На основе этих методов разработан ряд алгоритмов передачи данных.

Одним из первых методов использования динамического хаоса для сокрытия сообщения является хаотическая маскировка [4]. Схема использования хаотической маскировки для скрытой передачи сообщения приведена на рис. 1. Абонент, передающий сообщение $m(t)$ добавляет его в сумматоре к хаотическому сигналу $x(t)$. Далее сумма двух сигналов $m'(t) = m(t) + x(t)$ передается по каналу связи. Принимающий абонент синхронизирует свой хаотический генератор $u(t)$ с помощью принимаемого сигнала. В результате синхронизации хаотические генераторы у передающего и принимающего абонента становятся идентичными $u(t) = x(t)$. Переданное сообщение восстанавливается с помощью вычитания из полученного сигнала $m'(t)$ синхронизированного хаотического сигнала $u(t)$.

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2018 (DMS-2018), Omsk, Russia, October 2018, published at <http://ceur-ws.org>

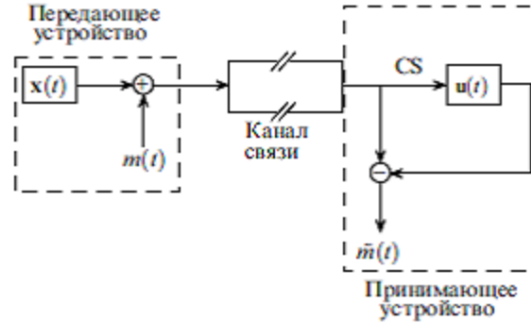


Рис. 1: Схема использования хаотической маскировки для скрытой передачи сообщения

Хаотическая маскировка сообщения эффективна при низком уровне шума в канале связи. При этом уровень шума превышает скрытый сигнал на 35-65 дБ [8]. Наличие шума в канале связи резко снижает качество передаваемой информации. Также к ухудшению качества приема сообщения приводит рассинхронизация управляющих параметров генераторов шума. Кроме того хаотическая маскировка характеризуется низким уровнем конфиденциальности [9, 10, 11]. Эти недостатки делают метод хаотической маскировки малоприменимым для практического применения. Следует отметить, что влияние шумов в канале связи является одной из основных проблем реализации устойчивых систем передачи информации. Достаточно большое количество работ посвящено реализации источников хаотического сигнала. Классификация динамических систем, которые могут быть использованы при генерации хаотического сигнала, несущего встроенное сообщение приведена в работе [12]. В данной статье приведено условие на скорости выработки полезного сигнала и генерации хаотической несущей, позволяющей снизить вероятность искажения скрытого сообщения. Для них используется понятие оптимальных кодирующих систем. Получен критерий определения таких систем. Кроме хаотической маскировки разработаны системы передачи сообщений на основе модуляции хаотического сигнала [13]. Информационный сигнал используется для изменения параметров хаотического генератора. Такой подход позволяет существенно повысить скорость передачи информации и является устойчивым к шумам в канале связи. В данной статье предложена схема формирования передаваемого скрытого сообщения, которая позволяет не проводить синхронизацию хаотических генераторов передающей и принимающей стороны.

1 Кодирование на основе ортогональных функций

Построим схему передачи скрытого цифрового сообщения, замаскированного в аналоговом шуме. Для этого на основе цифрового сигнала построим непрерывную функцию, по которой однозначно восстанавливается исходное сообщение. Используем семейство ортогональных функций — множество функций $\{f_i(x) | i \in N\}$ таких, что существует весовая функция $w(x)$ и интервал $[a, b]$, для которых

$$\int_a^b f_i(x)f_j(x)w(x)dx = \delta_{ij},$$

где δ_{ij} — символ Кронекера.

Пусть информация, которую необходимо закодировать, представляет собой последовательность вещественных чисел $k_i (i = 1, \dots, n)$. Построим функцию

$$F(x) = \sum_{i=1}^n k_i f_i(x).$$

Исходные числа k_i могут быть восстановлены из $F(x)$ на основе свойства ортогональности с помощью простого соотношения:

$$k_i = \int_a^b f_i(x)F(x)w(x)dx.$$

Описанный подход позволяет на основе взвешенной суммы функций и самих функций легко найти коэффициенты при слагаемых этой суммы. Кроме того, даже при искажении взвешенной суммы весовые коэффициенты могут быть восстановлены с удовлетворительной точностью.

В качестве примера рассмотрим семейство ортогональных тригонометрических функций

$$f_n(x) = \sqrt{2}\sin(\pi nx)$$

Ограничим множество возможных весовых коэффициентов двумя значениями: $\{0, 1\}$. Определим функцию $F(x) = f_1(x) + f_3(x) + f_7(x) + f_8(x)$. Возьмем 100 значений функции $f(x)$ с равным шагом в интервале $[0, 1]$. Искзим каждое значение функции равномерным шумом в диапазоне $[-2; 2]$. На рис. 2 представлен график оригинальной и искаженной функций.

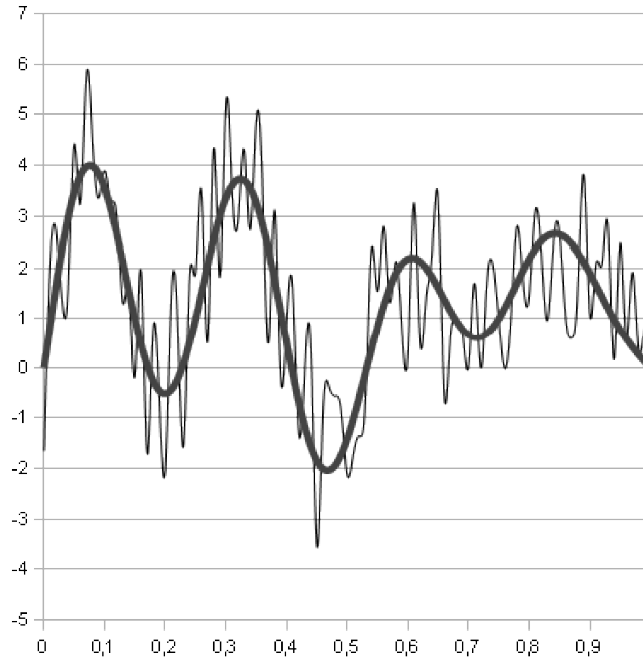


Рис. 2: Пример малого искажения передаваемого сообщения

Результаты восстановления коэффициентов показаны на рис. 3, где восстановленные значения коэффициентов отмечены меньшими повернутыми квадратами. Из рисунка видно, что, несмотря на значительный по сравнению с диапазоном значений уровень шума, восстановленные коэффициенты имеют значения, близкие к исходным, а при округлении до ближайшего порогового значения (0 или 1) полностью с ними совпадают.

На основе рассмотренного выше подхода кодирование n -битовой строки $(b_1, b_2, \dots, b_n)$ сообщения состоит из двух шагов:

1. Выбрать n функций: $f_1, f_2, \dots, f_k$ из семейства ортогональных функций;
2. Построить на отрезке ортогональности $[a, b]$ функцию

$$F(x) = \sum_{i=1}^n b_i f_i(x).$$

Процедура извлечения скрытого сообщения состоит из последовательного вычисления интегралов

$$d_i = \int_a^b f_i(x) F(x) w(x) dx \quad i = (1, \dots, n)$$

Если $d_i > 0.5$, то соответствующий бит b_i выходного сообщения равен единице, в противном случае ноль.

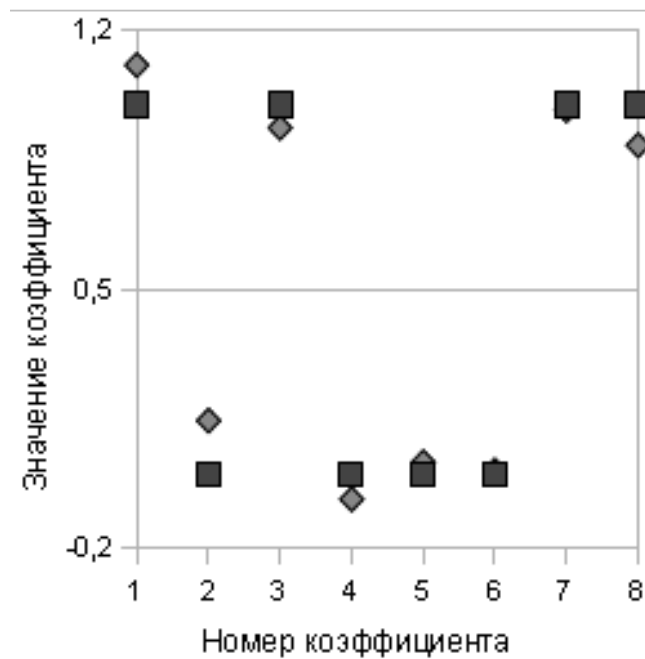


Рис. 3: Исходные и восстановленные коэффициенты

2 Компьютерный эксперимент

В компьютерном эксперименте было использовано семейство простых тригонометрических функций, обладающих свойством ортогональности на отрезке $[0, 1]$:

$$\{f_n(x) = \sqrt{2}\cos(\pi nx) | n \in N\}$$

Весовая функция для такого семейства ортогональных функций $w(x) = 1$. Для вычисления интегралов использовался численный метод трапеций. При дискретизации сигнала интервал ортогональности разбивался на 100 частей. Интенсивность скрываемого сигнала выбиралась равной единице. Интенсивность шума варьировалась, начиная от нуля до значений, не позволяющих извлечь скрытое сообщение с шагом 0.1. Хаотический сигнал моделировался с помощью генератора псевдослучайной последовательности с равномерным распределением. В качестве скрытого сообщения передавались все возможные значения, кодируемые 8 битами. Для всех значений передаваемого сообщения вычислялось максимальное количество неверно извлеченных битов при заданной интенсивности хаотического сигнала. График полученной зависимости представлен на рис. 4.

Как видно из рис. 4, если интенсивность хаотического сигнала превышает интенсивность скрытого сигнала не более, чем в 8 раз, то сообщение восстанавливается без потерь. Если интенсивность хаотического сигнала превышает интенсивность сигнала сообщения не более, чем в 18 раз, то неверно определяется не более 2 бит. Следует отметить, что 2 бита – это максимальное значение. Часть сообщений восстанавливается без потерь, а часть с одним измененным битом. Пример общего вида сигнала, кодирующего сообщение, и его суммы с хаотическим сигналом при отношении интенсивностей, равной 18 представлены на рис. 5.

Предложенная схема обладает низкой конфиденциальностью. Злоумышленник, зная общий вид используемого семейства ортогональных функций, легко может определить как факт наличия скрытого сообщения, так и его содержимое. Данная проблема может быть решена с помощью использования семейства ортогональных функций с параметром. Причем параметр должен быть вещественным. Например, может быть использовано семейство функций:

$$\{f_n(x) = \sqrt{2}\cos(\pi nax) | n \in N\},$$

где a — вещественный параметр, который держится в секрете обоими абонентами. Как показал компьютерный эксперимент, изменение a на 10% приводит в среднем к замене 12% битов в извлекаемом на выходе сообщении. Прямой перебор практически невозможен.

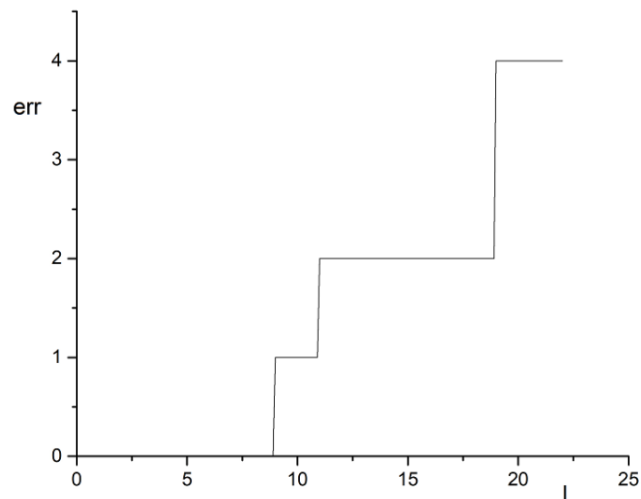


Рис. 4: Зависимость количества измененных битов в извлеченном сообщении err в зависимости от интенсивности хаотического сигнала I .

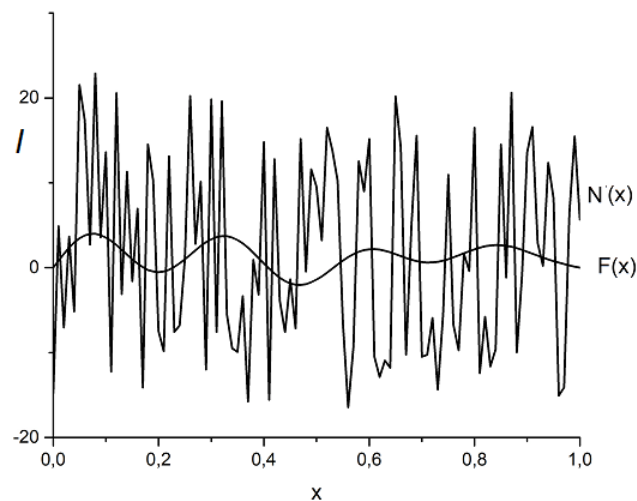


Рис. 5: Сигнал скрытого сообщения $F(x)$ и его сумма с хаотическим сигналом $N(x)$.

Заключение

В данной статье показана возможность реализации метода хаотической маскировки скрытого сообщения без синхронизации генераторов, передающей и принимающей сторон. Рассмотренный пример простых тригонометрических функций не обеспечивает достаточного уровня целостности сообщения и конфиденциальности. Однако эти проблемы могут быть решены при дальнейшем развитии предложенного метода. Прежде всего, при кодировании сообщения могут быть использованы коды, исправляющие ошибки, что существенно повысит устойчивость метода к уровню шума. Во-вторых, вместо тригонометрических функций могут быть использованы другие семейства ортогональных функций. Проблема конфиденциальности также может быть решена с помощью выбора семейства ортогональных функций с параметрами. В этом случае, для обнаружения и извлечения скрытого сообщения необходимо знать набор параметров, которые играют роль ключевых материалов, и держаться в секрете. Предложенный метод хаотической маскировки обладает тремя существенными преимуществами перед остальными. Во-первых, не требуется синхронизация генераторов динамического хаоса передающей и принимающей сторон. Во-вторых, может быть использован любой генератор хаотического сигнала. В-третьих, схема устойчива к зашумлению в канале связи, что является большой проблемой для всех предложенных ранее схем.

Список литературы

- [1] S.V. Belim, A.M. Fedoseyev. Issledovaniye skrytykh kanalov peredachi informatsii v algoritme tsifrovoy podpisi GOST R34.10-2001. *Izvestiya ChNTs*, 36(2):20–23, 2007.
- [2] M.I. Atmashkin, S.V. Belim. Skrytyye kanaly peredachi informatsii v algoritme elektronnoy tsifrovoy podpisi GOST R 34.10-2001. *Problemy informatsionnoy bezopasnosti. Kompyuternyye sistemy*, 4:26–35, 2010.
- [3] A.S. Dmitriyev, A.I. Panas. *Dinamicheskiy khaos: novyye nositeli informatsii dlya sistem svyazi*. M.: Fizmatlit, 2002.
- [4] K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz. Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 40(10):626–633, 1993.
- [5] H. Dedieu, M.P. Kennedy, M. Hasler. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 40(10):634–642, 1993.
- [6] A.S. Dmitriyev, A.I. Panas, S.O. Starkov. Experiments on speech and music signals transmission using chaos. *Int. J. Bifurcation and chaos*, 5(4):1249–1254, 1995.
- [7] T. Yang, L.O. Chua. Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 43(9):817–819, 1996.
- [8] P.T. Downes. Secure communication using chaotic synchronization. *SPIE*, 2038:227–234, 1993.
- [9] G. Perez, H.A. Cerderia. Extracting Messages Masked by Chaos. *Phys Rev. Lett.*, 74:1970–1973, 1995.
- [10] K.M. Short. Unmasking a modulated chaotic communication scheme. *Int. J. Bifurcation and chaos*, 6(2):367–375, 1996.
- [11] V.I. Ponomarenko, M.D. Prokhorov. Extracting information masked by the chaotic signal of a time-delay system. *Phys. Rev. E.*, 66:026215, 2002.
- [12] M.S. Baptista, E.E. Macau, C. Grebogi. Conditions for efficient chaos-based communication. *Chaos*, 145–150, 2003.
- [13] A.S. Dmitriyev, A.I. Panas, S.O. Starkov. Dinamicheskiy khaos kak paradigma sovremennykh sistem svyazi. *Zarubezhnaya radioelektronika. Uspekhi sovremennoy radioelektroniki*, 10:4–26, 1997.

Scheme of Chaotic Masking Messages Based on Orthogonal Functions

Sergey V. Belim, Yuriy S. Rakitskiy

The method of chaotic masking a discrete signal is proposed in the article. The proposed approach does not require the synchronization of chaotic generators and is resistant to noise in the communication channel. These properties remove the main problem of chaotic masking associated with the desynchronization of control parameters. The basic idea is to use message coding using orthogonal functions. Next, a simple summation of a hidden message with a chaotic signal is applied. The extraction of the message can be performed on the basis of the orthogonality property without subtraction of the chaotic component.