УДК 004.93
doi:10.31799/1684-8853-2019-2-76-82

Научные статьи
Articles

Использование семейств ортогональных функций для кодирования данных в схеме хаотической маскировки

С. В. Белим[a], *доктор физ.-мат. наук, профессор, orcid.org/0000-0002-5785-5160, sbelim@mail.ru*
Ю. С. Ракицкий[a], *канд. техн. наук, доцент, orcid.org/0000-0001-9419-5424*
[a]*Омский государственный университет им. Ф. М. Достоевского, Мира пр., 55а, Омск, 644077, РФ*

Введение: *хаотическая маскировка сообщений применяется для скрытой передачи данных по каналам связи. Существующие схемы хаотической маскировки требуют сложной системы согласования хаотических генераторов и не устойчивы к передаче сигнала по зашумленному каналу связи. Одним из возможных путей решения данной проблемы является использование алгоритмов кодирования сообщений, позволяющих извлекать их из шумового контейнера без дополнительной информации о генераторе шума.* ***Цель:*** *разработка схемы хаотической маскировки, не требующей согласования генераторов шума и устойчивой к передаче по зашумленным каналам.* ***Методы:*** *представление передаваемого сигнала в виде суперпозиции ортогональных функций с весовыми коэффициентами, определяемыми битами передаваемого сообщения. Извлечение сообщения из хаотического сигнала путем вычисления проекции полученного сигнала на семейство ортогональных функций.* ***Результаты:*** *на базе метода кодирования сообщения с помощью семейства ортогональных функций разработана схема хаотической маскировки для скрытой передачи данных. Отличительной особенностью предложенной схемы является отсутствие необходимости синхронизации генераторов шума передающей и принимающей сторонами. Сокрытие сообщения происходит простым подмешиванием полезного сигнала к передаваемому хаотическому. Извлечение полезного сигнала осуществляется благодаря свойству ортогональности семейства функций, участвующих в кодировании сообщения. Предполагается, что проекция шума на ортогональные функции имеет малое значение. Для вычисления проекции сигнала на ортогональные функции выполнено численное интегрирование. Проведен компьютерный эксперимент для двух семейств простых тригонометрических функций. Определено, что при отношении уровня шума к полезному сигналу 38 дБ вероятность передачи одного байта сообщения без потерь превышает 0,95, что удовлетворяет требованиям к современным системам хаотической маскировки. Доказано, что результаты извлечения сообщения существенно зависят от точности численного интегрирования. Для повышения допустимого уровня шумового сигнала необходимо применять более точные методы интегрирования.* ***Практическая значимость:*** *на основе результатов исследования могут быть спроектированы и реализованы системы со скрытой передачей сообщений. Предложенный подход позволяет повысить устойчивость схемы хаотической маскировки к шумам в каналах связи.*

Ключевые слова *— хаотическая маскировка, ортогональные функции, скрытая передача сообщений, модуляция дифференциального хаоса.*

Для цитирования: Белим С. В., Ракицкий Ю. С. Использование семейств ортогональных функций для кодирования данных в схеме хаотической маскировки. *Информационно-управляющие системы*, 2019, № 2, с. 76–82. doi:10.31799/1684-8853-2019-2-76-82
For citation: Belim S. V., Rakitskiy Yu. S. Using families of orthogonal functions for coding messages in a chaotic masking scheme. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 2, pp. 76–82 (In Russian). doi:10.31799/1684-8853-2019-2-76-82

Введение

В последнее время получили развитие схемы использования динамического хаоса для сокрытия самого факта передачи содержательного сообщения. Полезный сигнал каким-либо образом подмешивается к хаотическому сигналу, для выработки которого применяются хаотические генераторы. Причем интенсивность хаотического сигнала значительно превышает интенсивность полезного сигнала. Основная проблема состоит в извлечении принимающей стороной полезной составляющей принятого сигнала. Для этого по каналу связи либо какими-то другими способами передается дополнительная информация о хаотическом генераторе. На основе дополнительной информации принимающая сторона самостоятельно генерирует хаотическую составляющую и вычитает ее из полученного сигнала. Данную ситуацию принято характеризовать как формирование двух связанных идентичных хаотичных генераторов. На сегодня получили развитие несколько различных подходов: хаотическая маскировка [1], переключение хаотических режимов [2], нелинейное подмешивание передаваемого сообщения к хаотическому сигналу [3], модулирование управляющих параметров хаотического генератора [4].

Исторически одним из первых и наиболее простых в реализации является метод хаотической маскировки сообщения [1]. Передаваемое сообщение $m(t)$ складывается с хаотическим сигналом $x(t)$. Полученный смешанный сигнал $m'(t) = m(t) + x(t)$ передается принимающей стороне.

Основная задача, которая стоит перед принимающей стороной, заключается в синхронизации своего хаотического генератора $u(t)$ с хаотическим генератором передающей стороны: $u(t) = x(t)$. После этого передаваемое сообщение может быть получено путем простого вычитания $m(t) = m'(t) - u(t)$. В разработанных в настоящее время схемах хаотической маскировки уровень шума по сравнению с уровнем полезного сигнала составляет 35–65 дБ [5]. Схема хаотической маскировки эффективна, если уровень шума в канале связи достаточно низок, в противном случае резко снижается качество передачи информации. Также к значительному снижению качества полученного сигнала приводит рассинхронизация управляющих параметров генераторов шума [6–8].

Одним из возможных подходов к вычитанию шума из передаваемого сигнала является ортогонализация хаотических сигналов. Такие схемы нашли развитие в рамках общего подхода к модуляции сигналов, получившего название Differential Chaos Shift Keying (DCSK) [9]. Одной из проблем подобных систем является построение ортогональных хаотических сигналов. Для ее решения используются обычные генераторы шума с последующим применением к ним преобразования Гильберта [10–12], преобразования Грамма — Шмидта [13–15], кодов Уолша [16–18]. Также следует отметить, что для схем на основе ортогональных хаотических сигналов характерна низкая пропускная способность. Каждый ортогональный хаотический фрейм несет один бит информации.

В данной статье предложена схема хаотической маскировки сигнала, не требующая синхронизации генераторов шума. Основная идея состоит в кодировании сообщения на основе семейства ортогональных функций, которое позволяет в дальнейшем извлекать его без синхронизации хаотических генераторов передающей и принимающей сторонами. Данное кодирование было ранее применено для шифрования сообщений [19] и формирования устойчивых цифровых водяных знаков [20].

Кодирование сообщения

Пусть сообщение представлено в виде конечной последовательности битов $C = c_1c_2...c_N$.

Разобьем сообщение на подпоследовательности C_j длиной n ($j = 1, ..., M$, $M = [N/n]$) и представим каждую такую подпоследовательность в виде вектора

$$\mathbf{C}_j = (c_{jn}, ..., c_{(j+1)n-1}).$$

Выберем систему ортогональных на отрезке $[0, b]$ функций $f_i(t)$, $i = 1, ..., n$, где t — временная ось. Пусть для данного семейства функций условие ортогональности имеет вид

$$\int_0^b w(t) f_i(t) f_j(t) \mathrm{d}t = \delta_{ij},$$

где $\delta_{ij} = \begin{cases} 0, & i \neq j; \\ 1, & i = j. \end{cases}$

Построим вектор-функцию в n-мерном пространстве, координатами которой служат ортогональные функции из выбранного семейства:

$$\mathbf{f}(t) = (f_1(t), f_2(t), ..., f_n(t)).$$

Сопоставим каждой подпоследовательности исходного сообщения функцию $F_j(x)$, вычисляемую как скалярное произведение:

$$F_j(t) = \mathbf{c}_j\mathbf{f}(t).$$

Тогда все сообщение представимо в виде вектор-функции

$$\mathbf{F}(t) = (F_1(t), F_2(t), ..., F_M(t)).$$

Если исходное сообщение представить в виде матрицы, строками которой служат векторы подпоследовательностей:

$$\mathbf{MC} = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_M \end{pmatrix},$$

то вектор $\mathbf{F}(t)$ может быть получен как

$$\mathbf{F}(t) = \mathbf{MC} \cdot \mathbf{f}(t).$$

Сформируем функцию $F_c(t)$ на отрезке $[0, Mb]$, соответствующую сообщению, для передачи по каналу связи:

$$F_c(t) = \begin{cases} F_1(t), & t \in [0, b); \\ F_2(t-b), & t \in [b, 2b); \\ \vdots & \vdots \\ F_M(t-Mb), & t \in [(M-1)b, Mb]. \end{cases}$$

Функция $F_c(x)$ несет в себе полную информацию об исходном сообщении.

После получения функции $F_c(t)$, определенной на отрезке $[0, Mb]$, для извлечения сообщения необходимо выполнить следующие действия.

1. Разделить отрезок, на котором определена функция $F_c(t)$, на M частей. Данный отрезок определяется длительностью передачи сообще-

ния. Число M является параметром системы обмена сообщениями и известно обеим сторонам.

2. Определить координаты вектор-функции

$$\mathbf{F}(t) = (F_1(t), F_2(t), \ldots, F_M(t)).$$

Все функции $F_j(t)$, $j = 1, \ldots, M$ определяются на отрезке $[0, b]$ с помощью соотношения

$$F_j(t) = F_c(t + (j - 1)b).$$

3. Для каждой функции $F_j(t)$ вычислить набор величин

$$a_{ij} = \int_0^b w(t) f_i(t) F_j(t) \mathrm{d}t, \ i = 1, \ldots, n.$$

4. Сформировать последовательность

$$C_j = c_1^{(j)} c_2^{(j)} \ldots c_n^{(j)}, \ c_i^{(j)} = \begin{cases} 1, & a_{ij} \geq 0{,}5; \\ 0, & a_{ij} < 0{,}5. \end{cases}$$

5. Объединить подпоследовательности C_i в одну последовательность с помощью конкатенации:

$$C = C_1 C_2 \ldots C_M.$$

Полученная последовательность C будет совпадать с исходной, переданной по каналу связи. В идеальной системе величины a_{ij} должны принимать только единичные и нулевые значения. Однако даже в отсутствие помех в канале связи на третьем шаге необходимо вычислять интегралы, значение которых в общем случае может быть определено только численно. Для вычисления величин a_{ij} необходимо выполнить дискретизацию функции $F_c(x)$ с некоторым шагом x:

$$F_{ci} = F_c(ix), \ i = 0, \ldots, Mb/x - 1.$$

Дискретизация функции может использоваться не только на этапе вычисления интегралов, но и при отправке сообщения. Тогда правильный выбор параметра b влияет на работоспособность схемы в целом.

Схема скрытой передачи сообщения

Общая схема системы скрытой передачи сообщений на основе хаотической маскировки представлена на рис. 1.

Для скрытой передачи сообщения используем схему хаотической маскировки, сложив передаваемое сообщение $F_c(t)$ с хаотическим шумом. Пусть генератор шума вырабатывает сигнал $H(t)$. Тогда по каналу связи будет передаваться сигнал

$$S(t) = F_c(t) + H(t),$$

причем интенсивность хаотического сигнала I_H превышает интенсивность полезного сигнала I_F. Соотношение сигнал/шум принято измерять в децибелах, т. е. вычислять величину $k = 10\log_{10}(I_H/I_F)$.

Для извлечения передаваемого сообщения из сигнала $S(t)$ необходимо выполнить те же преобразования, что и для извлечения сообщения из функции $F_c(t)$:

1) разделить отрезок, на котором определена функция $S(t)$, на M частей;

2) определить координаты вектор-функции

$$\mathbf{S}(t) = (S_1(t), S_2(t), \ldots, S_M(t));$$

все функции $S_j(t)$, $j = 1, \ldots, M$ определяются на отрезке $[0, b]$ с помощью соотношения

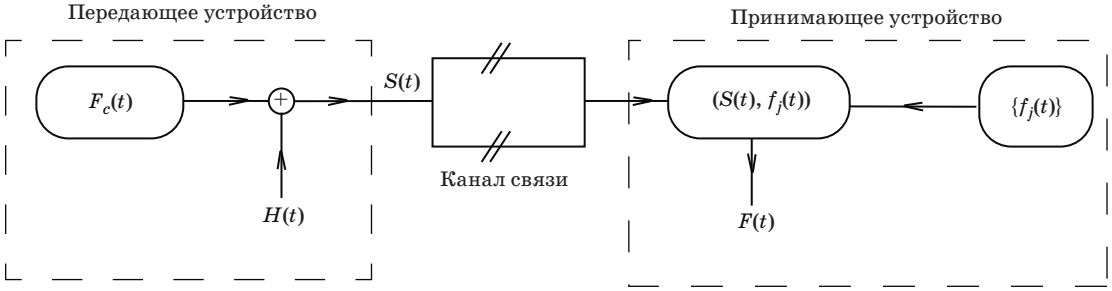
$$S_j(t) = S(t + (j - 1)b);$$

3) для каждой функции $S_j(x)$ вычислить набор величин

$$d_{ij} = \int_0^b w(t) f_i(t) S_j(t) \mathrm{d}t, \ i = 1, \ldots, n;$$

4) сформировать последовательность

$$E_j = e_1^{(j)} e_2^{(j)} \ldots e_n^{(j)}, \ e_i^{(j)} = \begin{cases} 1, & d_{ij} \geq 0{,}5; \\ 0, & d_{ij} < 0{,}5; \end{cases}$$



■ ***Рис. 1***. Структурная схема системы скрытой передачи сообщений

■ ***Fig. 1***. The structure scheme of a system for the hidden messages transmission

5) объединить подпоследовательности E_i в одну последовательность с помощью конкатенации:

$$E = E_1 E_2 ... E_M.$$

В силу аддитивного подхода к формированию сигнала $S(x)$ над хаотическим сигналом $H(x)$ выполняются те же самые преобразования. Хаотический сигнал $H(t)$ будет представлен в виде вектор-функции

$$\mathbf{H}(t) = (H_1(t), H_2(t), ..., H_n(t)).$$

Каждая функция $H_j(t)$, $j = 1, ..., n$ определена на отрезке $[0, b]$. Для величин d_{ij} можем записать

$$d_{ij} = \int_0^b w(t) f_i(t) \left(F_j(t) + H_j(t) \right) \mathrm{d}t = a_{ij} + h_{ij},$$

где $h_{ij} = \int_0^b w(t) f_i(t) H_j(t) \mathrm{d}t.$

Для правильного декодирования сообщения, в идеальном случае, необходимо выполнение требования $d_{ij} = a_{ij}$, т. е. $h_{ij} = 0$. Однако в силу того, что при вычислении $e_i^{(j)}$ используется пороговая схема, достаточно выполнения условия $|h_{ij}| < 0{,}5$. Данное ограничение накладывает условия как на выбор семейства ортогональных функций, так и на соотношение интенсивностей сигнала и шума. В идеальном случае при равномерном распределении случайных величин $H_j(t)$ и интегрировании на бесконечном интервале ($b \to \infty$) все $h_{ij} = 0$. В реальных системах приходится работать с конечными интервалами ($b < \infty$). В результате чего статистические характеристики случайных функций $H_j(t)$ отличаются от идеальных, и интегралы принимают ненулевые значения ($|h_{ij}| > 0$).

Сформулируем основные требования к семействам ортогональных функций, которые могут быть использованы в предложенной схеме.

1. Интервал ортогональности должен быть конечным. В противном случае невозможно сформировать кадры закодированного сообщения.

2. Ни одна из функций, в том числе весовая, не должна иметь особенностей на интервале ортогональности и ограниченную область допустимых значений. Это требование необходимо для эффективной реализации численного интегрирования.

3. Вычисление значений функции должно иметь низкую трудоемкость.

4. Определенный интеграл от функций в интервале ортогональности с учетом весовой функции должен быть равен нулю. Это требование позволит минимизировать значения величин h_{ij}.

Следующие факторы могут приводить к ненулевому значению величин h_{ij}:

1) выбор семейства ортогональных функций $f_i(t)$, $i = 1, ..., n$;

2) ограниченная длина отрезка b;

3) погрешности численного интегрирования, связанные с выбором численного метода и шага дискретизации.

Компьютерный эксперимент

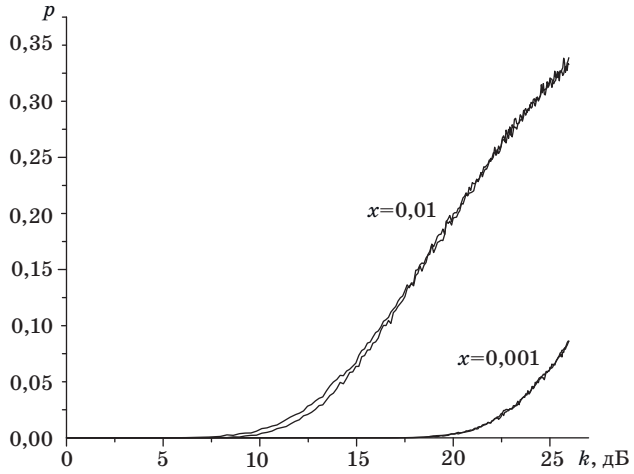
В рамках компьютерного эксперимента протестируем предложенную схему хаотической маскировки. Для тестирования было использовано два семейства простых тригонометрических функций, ортогональных на отрезке $[0, 1]$:

$$f_j(t) = \sqrt{2}\cos(\pi j t),\ j = 1, ..., 8;$$

$$g_j(t) = \sqrt{2}\sin(\pi j t),\ j = 1, ..., 8.$$

Весовая функция для этих семейств ортогональных функций $w(t) = 1$. Интегралы вычислялись методом трапеций. Для выявления влияния точности численного интегрирования на результаты извлечения полезного сигнала рассматривалось два случая с шагом дискретизации $x = 0{,}01$ и $x = 0{,}001$. Интенсивность полезного сигнала $I_F = 1$. Интенсивность хаотического сигнала I_H менялась от 0 до 20 с шагом 0,1. В качестве генератора шума использовался линейный конгруэнтный генератор с равномерным распределением. В качестве скрытого сообщения использована битовая последовательность длиной 2048 символов, которая формировалась из последовательно записанных чисел от 0 до 255 в однобайтовом представлении. Для каждого семейства ортогональных функций производилось кодирование сообщения, зашумление и извлечение 100 раз. В каждом эксперименте генератор псевдослучайной последовательности инициализировался различными зернами, что обеспечивало различные сигналы $H(t)$. В каждом эксперименте определялось количество неверно извлеченных битов. После этого значения, полученные в различных экспериментах, усреднялись, и вычислялась вероятность потери отдельного бита при передаче сообщения по предложенной схеме. На рис. 2 приведены графики зависимости вероятности неверного извлечения бита от соотношения сигнал/шум k для семейств ортогональных функций $f_j(t)$ и $g_j(t)$ при различных шагах численного интегрирования.

Из рисунка можно сделать несколько выводов. Во-первых, оба семейства ортогональных функций $f_j(t)$ и $g_j(t)$ обеспечивают мало отличимые друг от друга результаты. Во-вторых, точность вычисления интегралов, выражающаяся в выборе шага дискретизации, существенно влияет



■ ***Рис. 2.*** Зависимость вероятности p неверного определения одного бита передаваемого сообщения от соотношения сигнал/шум

■ ***Fig. 2.*** Dependence of insecure determination probability for one bit of the transferred message p on a ratio signal/noise

на результаты извлечения сообщения. При шаге дискретизации $x = 0{,}001$ для уровня шума 25 дБ вероятность неверного определения значения одного бита составляет $p = 0{,}08$. Вероятность передачи одного байта сообщения без потерь может быть определена по формуле $P = 1 - (1 - p)^8$.

Отсюда следует, что вероятность передачи одного байта сообщения без потерь при $k = 28$ дБ для $x = 0{,}01$ составляет $P = 0{,}96$, а для $x = 0{,}001$ получаем значение $P = 0{,}49$. Введем верхнюю границу пороговой вероятности передачи одного байта сообщения без потерь P_0. Согласно работе [5], рекомендуемым значением является $P_0 = 0{,}95$. В этом случае совместное использование методов хаотической маскировки и алгоритмов помехоустойчивого кодирования позволяет передавать сообщение без потерь [5]. Значение верхней границы вероятности передачи одного байта сообщения без потерь достигается при вероятности неверного определения одного бита $p_0 = 0{,}31$. При шаге дискретизации $x = 0{,}01$ верхняя граница передачи одного байта сообщения без потерь достигается при отношении уровня шума к уровню сигнала $k = 25{,}2$ дБ, что заметно ниже уровня, приемлемого для современных систем хаотической маскировки. Для шага дискретизации $x = 0{,}001$ аналогичный уровень шума составляет $k = 38{,}3$ дБ, что сопоставимо с результатами, использующими схему синхронизации генераторов шума [5]. Из этого можно сделать вывод, что шаг дискретизации $x = 0{,}001$ позволяет построить схему скрытой передачи сообщений, обеспечивающую устойчивость передачи сообщений при более высоких значениях интенсивности шума. Устойчивость схемы может быть повышена с помощью уменьшения шага дискретизации и использования более точных методов интегрирования.

Заключение

Предложенный в данной статье метод кодирования сообщений позволяет реализовать схему хаотической маскировки сигнала, не требующую согласования генераторов хаоса отправляющей и принимающей сторон. В результате существенно повышается устойчивость схемы к случайным шумам, присутствующим в каналах передачи информации. Основной проблемой построения предложенной схемы является обеспечение высокой точности численного интегрирования, влияющей на правильность извлечения передаваемого сообщения. Величина ошибки при вычислении интегралов может варьироваться с помощью шага дискретизации функции, кодирующей сообщение. Уменьшение шага дискретизации приводит к снижению количества ошибочно извлекаемых битов. Как следствие, появляется возможность увеличить интенсивность маскирующего хаотического сигнала. При значениях шага дискретизации 0,001 удается построить систему, сопоставимую по уровню хаотического сигнала с актуальными на данный момент системами хаотической маскировки.

Также следует отметить более высокую пропускную способность предложенной схемы по сравнению с результатами, полученными в работах [10–18], в которых свойства ортогональности используются для формирования хаотической составляющей сигнала. Схемы, предложенные в этих статьях, позволяют в одном фрейме кодировать не более двух бит исходного сообщения. В разработанном в настоящей статье подходе в одном фрейме передается восемь бит исходного сообщения.

Конфиденциальность передачи информации в предложенной схеме может быть обеспечена с помощью введения дополнительных параметров в ортогональные функции. Например, в рассмотренной схеме на основе простых тригонометрических функций может быть выбрано семейство ортогональных функций

$$f_j(t) = \sqrt{2}\cos(\omega\pi jt),\ j = 1, \ldots, N.$$

Два параметра, ω и N, известны только передающей и принимающей сторонам. До начала сеанса принимающая и передающая стороны по защищенному каналу обмениваются информацией об используемой частоте ортогональных функций ω и их количестве N. Без знания этих параметров извлечение сообщения невозможно.

В данной статье в качестве маскировки использован хаотический сигнал. Однако может быть использован и любой белый шум, что не скажется на работоспособности схемы в целом. Выбор той или иной маскировки может осуществляться исходя из конкретной реализации.

Литература

1. **Cuomo K. M., Oppenheim A. V., Strogatz S. H.** Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 1993, vol. 40, iss. 10, pp. 626–633. doi:10.1109/82.246163
2. **Dedieu H., Kennedy M. P., Hasler M.** 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*, 1993, vol. 40, iss. 10, pp. 634–642. doi:10.1109/82.246164
3. **Dmitriev A. S., Panas A. I., Starkov S. O.** Experiments on speech and music signals transmission using chaos. *International Journal of Bifurcation and Chaos*, 1995, vol. 5, no. 4, pp. 1249–1254. doi:10.1142/S0218127495000910
4. **Yang T., Chua L. O.** Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 1996, vol. 43, iss. 9, pp. 817–819. doi:10.1109/81.536758
5. **Downes P. T.** Secure communication using chaotic synchronization. *SPIE*, 1993, vol. 2038, pp. 227–234.
6. **Perez G., Cerderia H. A.** Extracting messages masked by chaos. *Phys Rev Lett*, 1995, vol. 74, pp. 1970–1973. doi:10.1103/PhysRevLett.74.1970
7. **Short K. M.** Unmasking a modulated chaotic communication scheme. *International Journal of Bifurcation and Chaos*, 1996, vol. 6, no. 2, pp. 367–375. doi:10.1142/S0218127496000114
8. **Ponomarenko V. I., Prokhorov M. D.** Extracting information masked by the chaotic signal of a time-delay system. *Phys Rev E*, 2002, vol. 66, pp. 026215. doi: 10.1103/PhysRevE.66.026215
9. **Kolumban G., Vizvari G. K., Schwarz W., Abel A.** Differential chaos shift keying: a robust coding for chaos communication. *Proc. Intern. Workshop on Non-linear Dynamics of Electronic Systems (NDES)*, 1996, pp. 92–97.
10. **Galias Z., Maggio G. M.** Quadrature chaos-shift keying: theory and performance analysis. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2001, vol. 48, no. 12, pp. 1510–1519. doi:10.1109/TCSI.2001.972858
11. **Kaddoum G.** Design and performance analysis of a multiuser OFDM based differential chaos shift keying communication system. *IEEE Trans. Commun.*, 2016, vol. 64, no. 1, pp. 249–260. doi:10.1109/TCOMM.2015.2502259
12. **Yang H., Tang W. K. S., Chen G.** System design and performance analysis of orthogonal multi-level differential chaos shift keying modulation scheme. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2016, vol. 63, no. 1, pp. 146–156. doi:10.1109/TCSI.2015.2510622
13. **Wren T. J., Yang T. C.** Orthogonal chaotic vector shift keying in digital communications. *IET Communications*, 2010, vol. 4, no. 6, pp. 739–753. doi:10.1049/iet-com.2009.0122
14. **Wang L., Cai G., Chen G.** Design and performance analysis of a new multiresolution M-ary differential chaos shift keying communication system. *IEEE Transaction on Wireless Communications*, 2015, vol. 14, no. 9, pp. 5197–5208. doi:10.1109/TWC.2015.2434820
15. **Kaddoum G., Soujeri E., Arcila C., Eshteiwi K.** I-DCSK: An improved noncoherent communication system architecture. *IEEE Transactions on Circuits and Systems II: Exp. Briefs*, 2015, vol. 62, no. 9, pp. 901–905. doi:10.1109/TCSII.2015.2435831
16. **Xu W. K., Wang L., Kolumban G.** A novel differential chaos shift keying modulation scheme. *International Journal of Bifurcation and Chaos*, 2011, vol. 21, no. 3, pp. 799–814. doi:10.1142/S0218127411028829
17. **Huang T., Wang L., Xu W., Lau F. C.** A multilevel code-shifted differential chaos-shift-keying system. *IET Communications*, 2016, vol. 10, no. 10, pp. 1189–1195. doi:10.1109/TCSII.2017.2764916
18. **Escribano F. J., Kaddoum G., Wagemakers A., Giard P.** Design of a new differential chaos-shift-keying system for continuous mobility. *IEEE Trans. Commun.*, 2016, vol. 64, no. 5, pp. 2066–2078. doi:10.1109/TCOMM.2016.2538236
19. **Белим С. В., Белим С. Ю.** Шифрование сообщений на основе собственных функций операторов. *Математические структуры и моделирование*, 2008, вып. 18, с. 95–97.
20. **Белим С. В., Илюшечкин Е. А.** Применение семейств ортогональных функций для построения устойчивых цифровых водяных знаков. *Математические структуры и моделирование*, 2014, вып. 32, с. 225–231.

UDC 004.93
doi:10.31799/1684-8853-2019-2-76-82

Using families of orthogonal functions for coding messages in a chaotic masking scheme

S. V. Belim[a], Dr. Sc., Phys.-Math., Professor, orcid.org/0000-0002-5785-5160, sbelim@mail.ru
Yu. S. Rakitskiy[a], PhD, Tech., Associate Professor, orcid.org/0000-0001-9419-5424
[a]F. M. Dostoevskiy Omsk State University, 55a, Mira Pr., 644077, Omsk, Russian Federation

Introduction: Chaotic masking of messages is used for hidden data transfer over a communication channel. The existing chaotic masking schemes require a sophisticated system to coordinate the chaotic generators. These systems are not stable in the case of a noisy communication channel. One of the ways to solve this problem is using coding algorithms which allow you to extract messages from a noisy container without any extra information about the chaotic generator. **Purpose:** Development of a chaotic masking scheme which does not need the noise generators to be coordinated and which is immune to transfer over noisy channels. **Methods:** The signal is represented as a superposition of orthogonal functions with weighting coefficients determined by the bits in the message being transferred. A message is extracted from the chaotic signal by calculating its projection on a family of orthogonal functions. **Results:** Based on the proposed method, a chaotic masking scheme is constructed for hidden data transfer. It does not need the chaotic generators of the transmitter and receiver to be synchronized. Messages are concealed by mixing the useful and chaotic signals. The useful signal can be extracted because the functions used for the coding are orthogonal. It is assumed that noise projection on orthogonal functions is very small. To calculate this projection, digital integration was used. A computer experiment was performed for two families of simple trigonometric functions. It showed that the proposed scheme allows you to recover the signal with a high precision for noise-to-signal ratio 38 dB (the probability of a correct byte transfer is more than 0.95). The success of recovering strongly depends on the digital integration precision. To increase the allowable noise level, you need to use more precise integration methods. **Practical relevance:** The results of the study can be used for developing systems with hidden message transmission. The proposed approach allows you to improve the stability of a chaotic masking scheme to the noise in communication channels.

Keywords — chaotic masking, orthogonal functions, hidden transmission of messages, differential chaos shift keying.

For citation: Belim S. V., Rakitskiy Yu. S. Using families of orthogonal functions for coding messages in a chaotic masking scheme. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 2, pp. 76–82 (In Russian). doi:10.31799/1684-8853-2019-2-76-82

References

1. Cuomo K. M., Oppenheim A. V., Strogatz S. H. Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 1993, vol. 40, iss. 10, pp. 626–633. doi:10.1109/82.246163
2. Dedieu H., Kennedy M. P., Hasler M. 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*, 1993, vol. 40, iss. 10, pp. 634–642. doi:10.1109/82.246164
3. Dmitriev A. S., Panas A. I., Starkov S. O. Experiments on speech and music signals transmission using chaos. *International Journal of Bifurcation and Chaos*, 1995, vol. 5, no. 4, pp. 1249–1254. doi:10.1142/S0218127495000910
4. Yang T., Chua L. O. Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 1996, vol. 43, iss. 9, pp. 817–819. doi:10.1109/81.536758
5. Downes P. T. Secure communication using chaotic synchronization. *SPIE*, 1993, vol. 2038, pp. 227–234.
6. Perez G., Cerderia H. A. Extracting messages masked by chaos. *Phys Rev Lett*, 1995, vol. 74, pp. 1970–1973. doi:10.1103/PhysRevLett.74.1970
7. Short K. M. Unmasking a modulated chaotic communication scheme. *International Journal of Bifurcation and Chaos*, 1996, vol. 6, no. 2, pp. 367–375. doi:10.1142/S0218127496000114
8. Ponomarenko V. I., Prokhorov M. D. Extracting information masked by the chaotic signal of a time-delay system. *Phys Rev E*, 2002, vol. 66, pp. 026215. doi: 10.1103/PhysRevE.66.026215
9. Kolumban G., Vizvari G. K., Schwarz W., Abel A. Differential chaos shift keying: a robust coding for chaos communication. *Proc. Intern. Workshop on Non-linear Dynamics of Electronic Systems (NDES)*, 1996, pp. 92–97.
10. Galias Z., Maggio G. M. Quadrature chaos-shift keying: theory and performance analysis. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2001, vol. 48, no. 12, pp. 1510–1519. doi:10.1109/TCSI.2001.972858
11. Kaddoum G. Design and performance analysis of a multiuser OFDM based differential chaos shift keying communication system. *IEEE Trans. Commun.*, 2016, vol. 64, no. 1, pp. 249–260. doi:10.1109/TCOMM.2015.2502259
12. Yang H., Tang W. K. S., Chen G. System design and performance analysis of orthogonal multi-level differential chaos shift keying modulation scheme. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2016, vol. 63, no. 1, pp. 146–156. doi:10.1109/TCSI.2015.2510622
13. Wren T. J., Yang T. C. Orthogonal chaotic vector shift keying in digital communications. *IET Communications*, 2010, vol. 4, no. 6, pp. 739–753. doi:10.1049/iet-com.2009.0122
14. Wang L., Cai G., Chen G. Design and performance analysis of a new multiresolution M-ary differential chaos shift keying communication system. *IEEE Transaction on Wireless Communications*, 2015, vol. 14, no. 9, pp. 5197–5208. doi:10.1109/TWC.2015.2434820
15. Kaddoum G., Soujeri E., Arcila C., Eshteiwi K. I-DCSK: An improved noncoherent communication system architecture. *IEEE Transactions on Circuits and Systems II: Exp. Briefs*, 2015, vol. 62, no. 9, pp. 901–905. doi:10.1109/TCSII.2015.2435831
16. Xu W. K., Wang L., Kolumban G. A novel differential chaos shift keying modulation scheme. *International Journal of Bifurcation and Chaos*, 2011, vol. 21, no. 3, pp. 799–814. doi:10.1142/S0218127411028829
17. Huang T., Wang L., Xu W., Lau F. C. A multilevel code-shifted differential chaos-shift-keying system. *IET Communications*, 2016, vol. 10, no. 10, pp. 1189–1195. doi:10.1109/TCSII.2017.2764916
18. Escribano F. J., Kaddoum G., Wagemakers A., Giard P. Design of a new differential chaos-shift-keying system for continuous mobility. *IEEE Trans. Commun.*, 2016, vol. 64, no. 5, pp. 2066–2078. doi:10.1109/TCOMM.2016.2538236
19. Belim S. V., Belim S. Yu. Encrypting massage on based eigenfunction of operators. *Matematicheskie struktury i modelirovanie* [Mathematical Structures and Modeling], 2008, iss. 18, pp. 95–97 (In Russian).
20. Belim S. V., Ilushechkin E. A. Applying families of orthogonal function to building resistant digital watermarks. *Matematicheskie struktury i modelirovanie* [Mathematical Structures and Modeling], 2014, iss. 32, pp. 225–231 (In Russian).