СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2020. – № 1–2 (97).** – 67–76

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И УСТРОЙСТВ

УДК 004.93 DOI: 10.17212/2307-6879-2020-1-2-67-76

МОДЕЛЬ ХАОТИЧЕСКОЙ МАСКИРОВКИ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ОРТОГОНАЛЬНЫХ ФУНКЦИЙ*

С.Ю. БЕЛИМ[1], С.В. БЕЛИМ[2]

[1] *644050, РФ, г. Омск, пр. Мира, 11, Омский государственный технический университет, кандидат педагогических наук, доцент кафедры прикладной математики и фундаментальной информатики. E-mail: svbelim@gmail.com.*
[2] *644050, РФ, г. Омск, пр. Мира, 11, Омский государственный технический университет, доктор физико-математических наук, профессор кафедры физики. E-mail: sbelim@mail.ru.*

В статье предложена модель хаотической маскировки сигнала. Цифровой сигнал в битовом представлении кодируется с помощью семейства ортогональных функций. На полученный аналоговый сигнал накладывается случайный белый шум. Амплитуда белого шума значительно превышает амплитуду сигнала. Для извлечения полезного сигнала используется свойство ортогональности функций. Преимуществом предложенной модели является отсутствие необходимости согласования генераторов шума источника и получателя сообщения. Для извлечения сообщения необходима операция интегрирования. Рассмотрен случай использования простой схемы прямоугольников. Проведен сравнительный компьютерный эксперимент на основе двух семейств ортогональных функций: простых тригонометрических функций и ортогональных полиномов Лагранжа. Показано, что использование семейства тригонометрических функций приводит к меньшему количеству ошибок при извлечении сообщения.

Ключевые слова: хаотическая маскировка, ортогональные функции, белый шум

ВВЕДЕНИЕ

Основная цель хаотической маскировки сигналов состоит в сокрытии факта передачи сообщения. При передаче по каналам связи сигнал помещается в хаотический контейнер. Хаотическая составляющая вычитается при приеме сигнала. В простейшем случае к передаваемому сообщению $m(t)$ добавляется хаотический шум $x(t)$. Результатом является смешанный сигнал $m'(t) = m(t) + x(t)$. Хаотический шум $u(t)$ вычитается после приема смешанно-

* Статья получена 12 мая 2020 г.

го сигнала. Результатом является полученное сообщение $m(t) = m'(t) - u(t)$. Полученное сообщение совпадает с передаваемым, если $u(t) = x(t)$. Сообщение передается без ошибок, если два генератора шума согласованы и генерируют одинаковый хаотический сигнал. Основной проблемой схем хаотической маскировки является протокол согласования генераторов шума. Интенсивность сигнала шума значительно превышает интенсивность полезного сигнала. В современных системах хаотической маскировки уровень шума превышает уровень сигнала на 35…60 дБ [1].

Для согласования генераторов шума используется передача дополнительных параметров. При этом необходимо осуществить согласование параметров генераторов шума для их синхронизации. Качество передачи сигнала значительно снижается при передаче по зашумленным каналам. Случайный шум невозможно вычесть из смешанного сигнала. Второй значительной проблемой является рассинхронизация генераторов при возникновении ошибок [2–4]. Рассинхронизация возникает при нарушении протокола обмена параметрами. В схеме хаотической маскировки сообщение передается в виде аналогового сигнала. Это связано с тем, что цифровые сигналы легко обнаруживаются в схеме хаотической маскировки.

Одним из возможных подходов к схеме хаотической маскировки является использование ортогональных хаотических сигналов. Этот подход называется DCSK (Differential Chaos Shift Keying) [5]. Ортогональные хаотические сигналы производятся обычными генераторами шума. К этим сигналам применяются различные ортогональные преобразования: Гильберта [6–8], Грамма–Шмидта [9–11] или Уолша [12–14]. Этот подход характеризуется низкой пропускной способностью: один кадр переносит один бит.

В настоящей статье предложена схема хаотической маскировки с кодированием сигнала на основе семейства ортогональных функций. Свойства предложенного подхода исследованы с помощью компьютерного эксперимента. Проведено сравнительное исследование различных семейств ортогональных функций для кодирования передаваемого сообщения.

1. СХЕМА КОДИРОВАНИЯ СООБЩЕНИЯ

Будем кодировать сообщения, состоящие из нулей и единиц. Пусть сообщение разбито на кадры длиной n бит. Рассмотрим кодирование одного кадра. Все кадры кодируются одинаково. Запишем представление кадра в виде битовой последовательности:

$$M = b_0 b_1 ... b_n .$$

Сопоставим кадру функцию:

$$F(t) = \sum_{i=0}^{n} c_i f_i(t).$$

В этой функции коэффициенты c_i вычисляются на основе битов сообщения b_i:

$$c_i = 2b_i - 1, \quad i = 1, \ldots, n.$$

Для нулевого бита $b_i = 0$ получаем $c_i = -1$, для единичного бита $b_i = 1$ получаем $c_i = 1$; $f_i(t)$, $i = 1, \ldots, n$ – семейство ортогональных функций на отрезке $[a, b]$, t – ось времени. Условие ортогональности имеет вид

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

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

где $w(t)$ – весовая функция.

Декодирование сообщения основано на свойстве ортогональности функций. Вычисляя последовательно проекции функции $F(t)$ на функции множества $f_i(t)$, определяем биты исходного сообщения. Сначала определим вспомогательные коэффициенты d_i:

$$d_i = \int_a^b w(t) F(t) f_i(t) dt.$$

Подставляя в это соотношение выражение для функции $F(t)$, получим равенство между d_i и c_i:

$$d_i = \sum_{j=0}^{n} c_j \int_a^b w(t) f_j(t) f_i(t) dt = \sum_{j=0}^{n} c_j \delta_{ij} = c_i.$$

Используем эти равенства для случая хаотической маскировки сигнала. Добавим к полезному сообщению $F(t)$ хаотический сигнал $G(t)$:

$$G(t) = F(t) + H(t).$$

Разложим составной сигнал $G(t)$ по ортогональным функциям $f_i(t)$:

$$e_i = \int_a^b w(t)G(t)f_i(t)dt.$$

Подставляя выражение для $G(t)$, получим соотношения для коэффициентов e_i и d_i:

$$e_i = d_i + h_i,$$

$$h_i = \int_a^b w(t)H(t)f_i(t)dt.$$

Для истинно случайного сигнала $H(t)$ коэффициенты h_i должны быть нулевыми:

$$h_i = 0, \quad i = 0,..., n.$$

В результате коэффициенты e_i будут равны как d_i, так и c_i:

$$e_i = d_i = c_i.$$

При реализации данной схемы необходимо выполнить автоматическое интегрирование. Простейший подход состоит в численном интегрировании на принимающей стороне. Для этого надо реализовать одну из схем численного интегрирования. Передающая сторона формирует аналоговый сигнал. Принимающая сторона определяет значение сигнала в дискретные моменты времени с шагом k:

$$Gj = G(a + jk), \quad j = 0,..., s, \quad s = [(b - a)/k].$$

После этого коэффициенты e_i вычисляются с помощью метода прямоугольников численного интегрирования:

$$e_i = \sum_{j=0}^{s} w(a + jk)G_j f_i(a + jk).$$

Для коэффициентов d_i и h_i будут выполняться аналогичные равенства:

$$d_i = \sum_{j=0}^{s} w(a+jk)F_j f_i(a+jk),$$

$$h_i = \sum_{j=0}^{s} w(a+jk)H_j f_i(a+jk),$$

$$F_j = F(a+jh),\ \ j = 0,...,s,$$

$$H_j = H(a+jh),\ \ j = 0,...,s,$$

$$s = [(b-a)/h].$$

В каналах передачи информации возможны случайные шумы. Численное интегрирование обладает погрешностями вычисления. Поэтому большое количество коэффициентов h_i будет отлично от нуля. Для вычисления коэффициентов исходного сообщения необходимо использовать пороговую схему:

$$c_i = \begin{cases} 1, & e_i \geq 0, \\ 0, & e_i < 0. \end{cases}$$

Точность вычисления интегралов зависит от выбранного шага k. При уменьшении шага k возрастает объем вычислений. Скорость передачи сообщения уменьшается.

2. КОМПЬЮТЕРНЫЙ ЭКСПЕРИМЕНТ

В компьютерном эксперименте проводилось сравнение ошибок передачи сообщения. Тестировались три семейства ортогональных функций. Первое семейство ортогональных функций строилось на основе простых тригонометрических функций:

$$f_j(t) = \sqrt{2}\cos(\pi j t).$$

Для этого семейства весовая функция $w(t)=1,$ интервал ортогональности [0, 1]. Второе семейство ортогональных функций строилось на основе полиномов Лагранжа:

$$f_0(t)=1, \quad (j+1)f_{j+1}(t)=(2j+1)xf_j(t)-jf_{j-1}(t).$$

Для этого семейства весовая функция $w(t)=1,$ интервал ортогональности [–1, 1].

Кодировались сообщения от 0 до 255. Для каждого сообщения использовалась длина 8 бит. Случайный шум генерировался на основе линейного конгруэнтного генератора. Амплитуда полезного сигнала была равна единице. Амплитуда шума была равна 100. Шаг дискретизации k изменялся от 0.01 до 0.1. Мера Хэмминга вычислялась между исходным и декодированным сообщением. Пример соотношения между полезным сигналом и маскирующим шумом представлена на рис. 1.

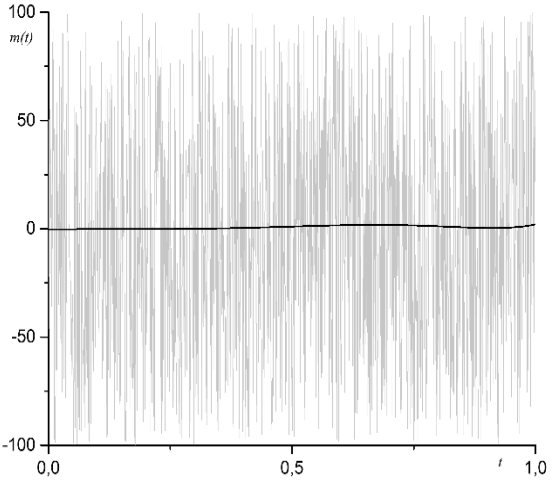

Рис.1. Маскирующий (светлый) и полезный (темный) сигналы. Амплитуда шума 100

На рис. 2 представлена зависимость расстояния Хэмминга от шага дискретизации для трех тестируемых семейств ортогональных функций при амплитуде шума 100.

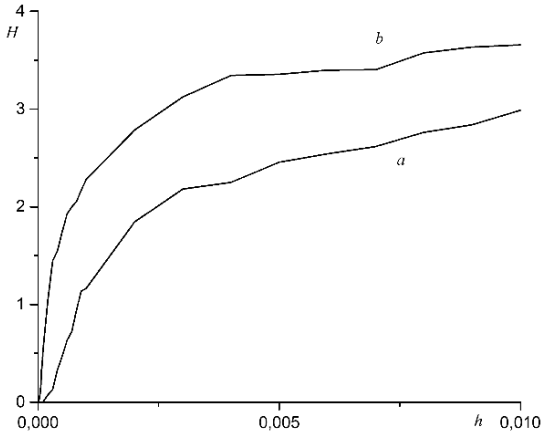

Рис. 2. Зависимость среднего расстояния Хэмминга от шага дискретизации для двух тестируемых семейств ортогональных функций и при амплитуде шума 100:

a – тригонометрические функции; *b* – полиномы Лагранжа

ЗАКЛЮЧЕНИЕ

В статье предложена схема хаотической маскировки на основе семейств ортогональных функций. Компьютерный эксперимент показал, что использование тригонометрических функций является предпочтительным. Ортогональные полиномы менее устойчивы к шуму.

СПИСОК ЛИТЕРАТУРЫ

1. *Downes P.T.* Secure communication using chaotic synchronization // Proceedings of SPIE. – 1993. – Vol. 2038. – P. 227–234.

2. *Perez G., Cerderia H.A.* Extracting messages masked by chaos // Physical Review Letters. – 1995. – Vol. 74. – P. 1970–1973.

3. *Short K.M.* Unmasking a modulated chaotic communication scheme // International Journal of Bifurcation and Chaos. – 1996. – Vol. 6, N 2. – P. 367–375.

4. *Ponomarenko V.I., Prokhorov M.D.* Extracting information masked by the chaotic signal of a time-delay system // Physical review. E, Statistical, Nonlinear, and Soft Matter Physics. – 2002. – Vol. 66. – P. 026215.

5. Differential chaos shift keying: a robust coding for chaos communication / G. Kolumban, G.K. Vizvari, W. Schwarz, A. Abel // Proceedings International

Workshop on Non-linear Dynamics of Electronic Systems (NDES'96). – Sevilla, Spain, 1996. – P. 92–97.

6. *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, N 12. – P. 1510–1519.

7. *Kaddoum G.* Design and performance analysis of a multiuser OFDM based differential chaos shift keying communication system // IEEE Transactions on Communications. – 2016. – Vol. 64, N 1. – P. 249–260.

8. *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, N 1. – P. 146–156.

9. *Wren T.J., Yang T.C.* Orthogonal chaotic vector shift keying in digital communications // IET Communications. – 2010. – Vol. 4, N 6. – P. 739–753.

10. *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, N 9. – P. 5197–5208.

11. I-DCSK: an improved noncoherent communication system architecture / G. Kaddoum, E. Soujeri, C. Arcila, K. Eshteiwi // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2015. – Vol. 62, N 9. – P. 901–905.

12. *Xu W.K., Wang L., Kolumban G.* A novel differential chaos shift keying modulation scheme // International Journal of Bifurcation and Chaos. – 2011. – Vol. 21, N 3. – P. 799–814.

13. A multilevel code-shifted differential chaos-shift-keying system / T. Huang, L. Wang, W. Xu, F.C. Lau // IET Communications. – 2016. – Vol. 10, N 10. – P. 1189–1195.

14. Design of a new differential chaos-shift-keying system for continuous mobility / F.J. Escribano, G. Kaddoum, A. Wagemakers, P. Giard // IEEE Transactions on Communications. – 2016. – Vol. 64, N 5. – P. 2066–2078.

Белим Светлана Юрьевна, кандидат педагогических наук, доцент кафедры «Прикладная математика и фундаментальная информатика» Омского государственного технического университета. Основное направление научных исследований – модели безопасности информационных систем. Имеет более 40 публикаций. E-mail: svbelim@gmail.com

Белим Сергей Викторович, доктор физико-математических наук, профессор кафедры «Физика» Омского государственного технического университета. Основное направление научных исследований – модели безопасности информационных систем. Имеет более 200 публикаций. E-mail: sbelim@mail.ru.

DOI: 10.17212/2307-6879-2020-1-2-67-76

The chaotic masking message model using orthogonal functions*

S.Yu. Belim[1], S.V. Belim[2]

[1] *Omsk State Technical University, 11 Mira Prospekt, Omsk, 644050, Russian Federation, candidate of pedagogical sciences, docent of the applied mathematics and fundamental informatics department. E-mail: svbelim@gmail.com*
[2] *Omsk State Technical University, 11 Mira Prospekt, Omsk, 644050, Russian Federation, doctor of physical and mathematical sciences, professor of the physics department. E-mail: sbelim@mail.ru*

The model for chaotic signal masking is proposed in the article. The digital signal in the bit representation is encoded using a family of orthogonal functions. Random white noise is superimposed on the resulting analog signal. The white noise amplitude is significantly greater than the amplitude of the signal. The functions orthogonal property is used to retrieve a useful signal. The advantage proposed this model is that it is not necessary to match the noise generators in the source and in the receiver of the message. The integration operation is required to retrieve the message. The using a simple rectangle scheme is discussed. The comparative computer experiment is based on two families of orthogonal functions: simple trigonometric functions and orthogonal Lagrange polynomials. It has been shown that using the trigonometric function family results in fewer errors when retrieving a message.

Keywords: Chaotic masking, orthogonal functions, white noise

REFERENCES

1. Downes P.T. Secure communication using chaotic synchronization. *Proceedings of SPIE*, 1993, vol. 2038, pp. 227–234.

2. Perez G., Cerderia H.A. Extracting messages masked by chaos. *Physical Review Letters*, 1995, vol. 74, pp. 1970–1973.

3. Short K.M. Unmasking a modulated chaotic communication scheme. *International Journal of Bifurcation and Chaos*, 1996, vol. 6, no. 2, pp. 367–375.

4. Ponomarenko V.I., Prokhorov M.D. Extracting information masked by the chaotic signal of a time-delay system. *Physical review. E, Statistical, Nonlinear, and Soft Matter Physics*, 2002, vol. 66, p. 026215.

5. Kolumban G., Vizvari G.K., Schwarz W., Abel A. Differential chaos shift keying: a robust coding for chaos communication. *Proceedings International Workshop on Non-linear Dynamics of Electronic Systems (NDES'96)*, Sevilla, Spain, 1996, pp. 92–97.

* *Received 12 May 2020.*

6. 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.

7. Kaddoum G. Design and performance analysis of a multiuser OFDM based differential chaos shift keying communication system. *IEEE Transactions on Communications*, 2016, vol. 64, no. 1, pp. 249–260.

8. 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.

9. Wren T.J., Yang T.C. Orthogonal chaotic vector shift keying in digital communications. *IET Communications*, 2010, vol. 4, no. 6, pp. 739–753.

10. *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, N 9. - P. 5197–5208.

11. Kaddoum G., Soujeri E., Arcila C., Eshteiwi K. I-DCSK: An improved noncoherent communication system architecture. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2015, vol. 62, no. 9, pp. 901–905.

12. 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.

13. 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.

14. Escribano F.J., Kaddoum G., Wagemakers A., Giard P. Design of a new differential chaos-shift-keying system for continuous mobility. *IEEE Transactions on Communications*, 2016, vol. 64, no. 5, pp. 2066–2078.

Для цитирования:

Белим С.Ю., Белим С.В. Модель хаотической маскировки сообщений с использованием ортогональных функций // Сборник научных трудов НГТУ. – 2020. – № 1–2 (97). – С. 67–76. – DOI: 10.17212/2307-6879-2020-1-2-67-76.

For citation:

Belim S.Yu., Belim S.V. Model' khaoticheskoi maskirovki soobshchenii s ispol'zovaniem ortogonal'nykh funktsii [The chaotic masking message model using orthogonal functions]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Transaction of scientific papers of the Novosibirsk state technical university*, 2020, no. 1–2 (97), pp. 67–76. DOI: 10.17212/2307-6879-2020-1-2-67-76.