

СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА ГЕНЕРАЦИИ ХАОТИЧЕСКИХ АВТОКОЛЕБАНИЙ

© 2006 В.В. Зайцев, О.В. Зайцев¹

Предложен алгоритм преобразования и восстановления сигналов, обеспечивающий защиту передаваемой информации. Алгоритм основан на использовании в качестве маскирующего сигнала хаотических автоколебаний дискретного осциллятора. Приведен пример применения алгоритма.

Введение

Использование широкополосных сигналов — одно из распространенных направлений защиты информации от несанкционированного доступа. В последнее время появился ряд публикаций [1–3], авторы которых при кодировании информации в качестве источников широкополосных сигналов применяют динамические системы, функционирующие в режиме хаотических колебаний, а для выделения информационного сигнала предлагают использовать явление полной хаотической синхронизации копированных систем [4]. Авторы коллективной монографии [5] для декодирования модулированных хаотических колебаний рекомендуют опираться на методы реконструкции динамических систем.

В настоящем сообщении описан метод скрытой передачи информации с низкочастотным спектром, основанный на алгоритме генерации автоколебаний в дискретном осцилляторе Ван дер Поля (ВдП). Эта дискретная автоколебательная система предложена ранее в работе [6]. Широкие возможности системы для демодуляции ЧМ-сигналов и АМ-сигналов с подавленной несущей продемонстрированы в сообщениях [7, 8]. В работе [9] показано, что дискретный осциллятор ВдП имеет режимы хаотических автоколебаний.

1. Хаотические автоколебания в дискретном осцилляторе ВдП

Дискретный осциллятор ВдП — автоколебательная система второго порядка, синтезированная по аналоговому осциллятору нелинейным методом импульсной

¹Зайцев Валерий Васильевич (zaitsev@ssu.samara.ru), Зайцев Олег Валерьевич, кафедра радиофизики и компьютерного моделирования радиосистем Самарского государственного университета, 443011, Россия, г. Самара, ул. Акад. Павлова, 1.

инвариантности [6]. Алгоритм генерации определяется нелинейным разностным уравнением

$$y[n] = \alpha_1 y[n-1] + \alpha_2 y[n-2] + \gamma (1 - y^2[n-1]) (y[n-1] - y[n-2]), \quad (1)$$

где параметр нелинейности характеризует глубину положительной обратной связи в системе, приводящей к генерации незатухающих колебаний. Коэффициенты α_1 и α_2 линейной части уравнения (1) связаны с собственной частотой Ω_0 и добротностью Q контура-прототипа соотношениями

$$\alpha_1 = 2 \exp\left(-\pi \frac{\Omega_0}{Q}\right) \cos(2\pi \Omega_0), \quad \alpha_2 = -\exp\left(-2\pi \frac{\Omega_0}{Q}\right). \quad (2)$$

Здесь и в дальнейшем все частоты измеряются в единицах частоты дискретизации (тактовой частоты). Формулы (2) можно использовать для настройки входящего в состав системы дискретного колебательного контура на заданную частоту Ω_0 и изменения его добротности.

В работе [9] показано, что существуют области значений параметров γ , Ω_0 и Q , в которых дискретный осциллятор ВдП генерирует хаотические автоколебания с широким спектром в высокочастотной области. Для примера на рис. 1 приведен амплитудный спектр хаотических автоколебаний в осцилляторе с параметрами $\gamma = 0,195$, $\Omega_0 = 0,2$, $Q = 30$. Оценка спектра получена методом усреднения периодограмм (методом Бартлетта) с 512-точечным преобразованием Фурье по реализации автоколебаний длиной $N = 2^{16}$. Эффективное значение хаотических автоколебаний $A_y = 1,93$.

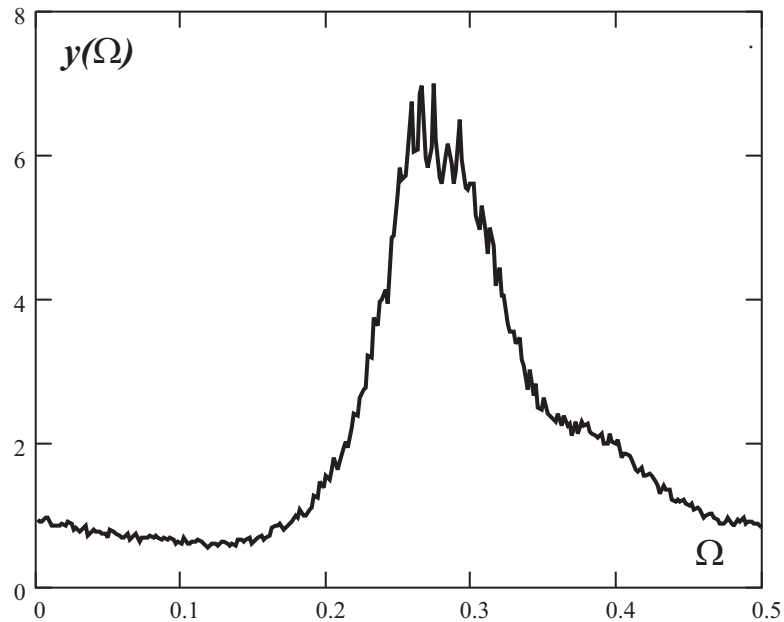


Рис. 1. Амплитудный спектр хаотических автоколебаний

2. Алгоритм скрытой передачи информации

Форма спектра хаотических автоколебаний указывает на целесообразность их использования для маскировки информационного сигнала со спектром, сосредоточенным в области частот $0,25 < \Omega < 0,35$ [10]. Для маскировки сигнала $x[n]$ со спектром в низкочастотной области можно путем гетеродинирования перенести его в окрестность частоты $\Omega = 0,3$ либо сместить в область низких частот спектр хаотических автоколебаний $y[n]$. Выберем второй вариант. Для этого сигнал автогенератора (1) подвергнем нелинейному преобразованию дискретной системой первого порядка:

$$z[n] = \sigma y[n-1] + 2\pi\Omega_c (y^2[n] + x[n]). \quad (3)$$

Здесь $\sigma = \exp(-2\pi\Omega_c)$, Ω_c — частота среза низкочастотного фильтра.

Сигнал $z[n]$ является передаваемым сообщением. В дальнейшем будем называть его сигналом передатчика.

Для декодирования сигнала $z[n]$ в приемнике следует воспользоваться сконструированным на основе (3) алгоритмом фильтрации

$$w[n] = \frac{z[n] - \sigma z[n-1]}{2\pi\Omega_c} - y^2[n]. \quad (4)$$

При этом в приемнике генерируются хаотические автоколебания $y[n]$, идентичные автоколебаниям передатчика. Такая генерация возможна, если параметры γ , Ω_0 и Q передатчика и приемника совпадают. Кроме того, в передатчике и приемнике необходимо реализовать одинаковые начальные генерации условия $y[0]$ и $y[1]$.

В целом условием отсутствия ошибки декодирования является идентичность параметров γ , Ω_0 , Q , $y[0]$, $y[1]$ и Ω_c передатчика (1), (3) и приемника (1), (4). Наличие шести независимых параметров открывает широкие возможности защиты информации от несанкционированного доступа.

3. Пример применения алгоритма

Для иллюстрации возможностей предложенного алгоритма приведем пример скрытой передачи изображения. Рассмотрим еще один весьма наглядный пример применения алгоритма (3), (4) — скрытую передачу изображения. В качестве входного сигнала $x[n]$ в (3) используем последовательность значений, полученных построчной выборкой из матрицы 267×1389 , хранящей бинарное изображение текста. Эффективное значение сигнала масштабированием доведено до уровня $A_x = 0.085$. Амплитудные спектры информационного сигнала $x[n]$ и сигнала передатчика $z[n]$ показаны на рис. 2. Из сопоставления спектров очевидно, что хаотические автоколебания полностью маскируют информационный сигнал.

Для количественной характеристики качества восстановленного сигнала $w[n]$ будем использовать отношение "сигнал/шум":

$$\frac{S}{N} = \frac{A_x}{\sqrt{\langle (w[n] - x[n])^2 \rangle}},$$

где угловыми скобками обозначено усреднение по времени.

Рис. 3, а демонстрирует изображение, восстановленное по (1), (4) при условии полного совпадения параметров передатчика и приемника. В этом случае отношение "сигнал/шум" достигает значения $S/N = 278 \text{ db}$ и определяется арифметическими ошибками при выполнении операций кодирования и декодирования. На

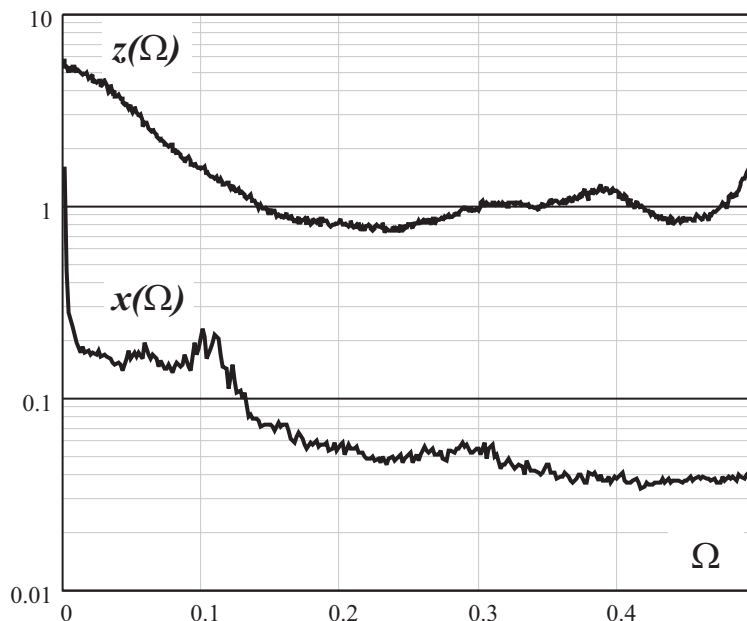


Рис. 2. Спектры информационного и передаваемого сигналов

*Предвозлежатель Бессмертных Совета, Хроноса сын, Громовержец Зевес
В бурно кипящий предвечный хаос ясный порядок внести возжелавши,
В светлом эфире разжег череду колебаний, давши пространству размеры
И времени чувство навек заложивши в Космосе,
В Боге, в душе человека.*

а

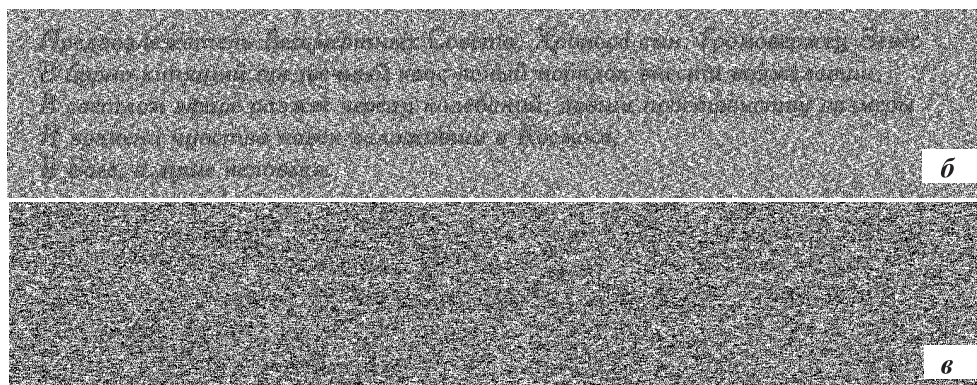


Рис. 3. Восстановленные изображения

рис. 3, б показано ухудшение качества восстановленного изображения при несовпадении одного параметра — частоты $\Omega_c = 0,055$ в приемнике с аналогичной частотой $\Omega_c = 0,05$ в передатчике. Отношение "сигнал/шум" в этом случае равно $S/N = -10,8 \text{ db}$.

Изображение на рис. 3, в характеризуется отношением "сигнал/шум" $S/N = -34 \text{ db}$ и получено при расстройке частот Ω_0 : в приемнике $\Omega_0 = 0,2001$, а в передатчике $\Omega_0 = 0,2$. Фактически вид восстановленного изображения озна-

чает, что расстройка частот Ω_0 в передатчике и приемнике, удовлетворяющая неравенству $|\Delta\Omega_0| \geq 0,0001$ гарантирует конфиденциальность сообщения.

Аналогичного рода численные эксперименты позволяют установить, что алгоритм декодирования (1), (4) наименее чувствителен к вариациям параметров Q и Ω_c .

Заключение

Предложенный метод кодирования может найти применение в помехозащищенных сетях передачи информации и при передаче данных на магнитных и оптических носителях. Необходимость подбора шести независимых параметров обеспечивает методу высокую степень защиты от несанкционированного доступа.

Литература

- [1] Cuomo, K.M. Circuit implementation of synchronized chaos with application to communications / K.M. Cuomo, A.V. Oppenheim // *Phys. Rev. Lett.* – 1993. – V. 71. – No. 1. – P. 65–68.
- [2] Cuomo, K.M. Synchronization of Lorenz-based chaotic circuits with application to communications / K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz // *IEEE Trans. Circ. Syst.* – 1993. – V. 40. – P. 626–633.
- [3] Gonzalez-Miranda, J.M. Communications by synchronization of spatially symmetric chaotic systems / J.M. Gonzalez-Miranda // *Phys. Lett. A.* – 1999. – V. 251. – No. 2. – P. 115–120.
- [4] Pecora, L.M. Synchronization in chaotic systems / L.M. Pecora, T.L. Carroll // *Phys. Rev. Lett.* – 1990. – V. 64. – P. 821–824.
- [5] Нелинейные эффекты в хаотических и стохастических системах / В.С. Анищенко [и др.]. – М.-Ижевск: Институт компьютерных исследований, 2003. – 544 с.
- [6] Зайцев, В.В. Динамика автоколебаний дискретного осциллятора Ван дер Поля / В.В. Зайцев, С.В. Давыденко, О.В. Зайцев // *Физика волновых процессов и радиотехнические системы.* – 2000. – Т. 3. – №2. – С. 64–67.
- [7] Зайцев, В.В. Детектор ЧМ-сигнала на основе кольца фазовой автоподстройки частоты дискретного автогенератора / В.В. Зайцев, О.В. Зайцев // *Физика волновых процессов и радиотехнические системы.* – 2005. – Т. 8. – №1. – С. 82–84.
- [8] Зайцев, О.В. Синхронный детектор дискретных АМ сигналов / О.В. Зайцев // V Международная конференция "Физика и технические приложения волновых процессов". Тезисы докладов. – Самара, 2006. – С. 411–412.
- [9] Зайцев, В.В. Статистические оценки характеристик стохастических автоколебаний дискретного осциллятора Ван дер Поля / В.В. Зайцев, О.В. Зайцев, Г.П. Яровой // *Физика волновых процессов и радиотехнические системы.* – 2001. – Т. 4. – №1. – С. 18–21.
- [10] Зайцев, В.В. Скрытая передача информации на основе хаотических автоколебаний дискретного осциллятора / В.В. Зайцев // *Физика волновых процессов и радиотехнические системы.* – 2006. – Т. 10. – №1. – С. 36–41.

Поступила в редакцию 24/XI/2006;
в окончательном варианте — 24/XI/2006.

PROTECTION OF INFORMATION BY AN ALGORITHM OF CHAOTIC SELF-OSCILLATIONS GENERATION

© 2006 V.V.Zaitsev, O.V.Zaitsev²

An algorithm of signal conversion and recovery, providing concealment of the transferred information is proposed. The algorithm is based on using signal of chaotic self-oscillations of discrete oscillator as masking signal. An example of algorithm's application is given.

Paper received 24/XI/2006.

Paper accepted 24/XI/2006.

²Zaitsev Valeriy Vasilievich (zaitsev@ssu.samara.ru), Zaitsev Oleg Valerievich, Dept. of Radiophysics and Computer Modelling of Radiotechnical Systems, Samara State University, Samara, 443011, Russia.