09

Скрытая передача информации при использовании запаздывания для выделения полезного сигнала из маскирующих колебаний

© Э.В. Кальянов

Институт радиотехники и электроники им. В.А. Котельникова РАН (фрязинский филиал), Фрязино (Моск. обл.)
E-mail: erast@ms.ire.rssi.ru

Поступило в Редакцию 13 октября 2008 г.

Рассмотрен новый способ скрытой передачи информации, основанный на использовании запаздывания для выделения полезного сигнала из шумоподобных колебаний, которые могут быть как хаотическими, так и стохастическими. Численными методами исследованы математические модели при использовании источника хаотических колебаний. Рассмотрена маскировка при передаче незакодированного сигнала, а также при импульсной передаче информации с помощью бит 0/1.

PACS: 05.45.-a

Хаос относится к одной из наиболее интересных проблем физики начала XXI в. [1], и его практически полезному применению уделяется большое внимание [2,3]. Важным является использование хаотических колебаний для маскировки передаваемых сигналов. Многие из предлагаемых для этих целей способов основаны на использовании различных видов синхронизации хаотических осцилляций [4,5]. Все виды синхронизации хаоса, однако, очень критичны к параметрам синхронизируемых систем, и практическая реализация скрытой связи при использовании реальных хаотических генераторов затруднительна. К тому же практические генераторы, обладающие развитым хаосом, не являются чисто хаотическими, так как сильное влияние на возбуждение колебаний оказывают внутренние шумы. Известные экспериментально реализованные способы маскировки развитым хаосом созданы без использования явления синхронизации [6,7].

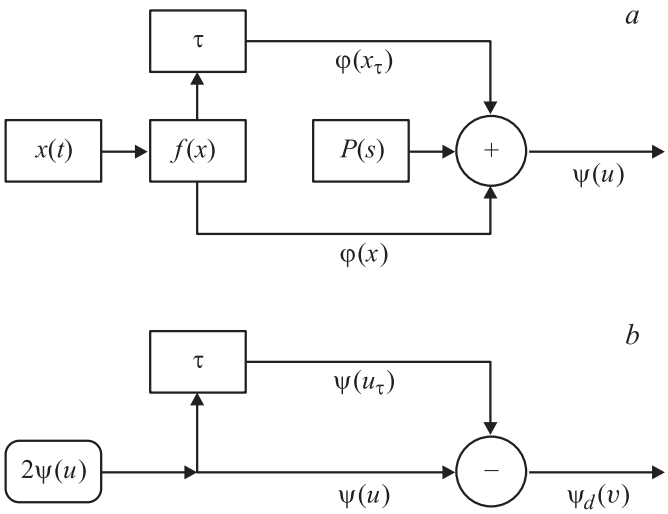

Рис. 1. Схема скрытой передачи информации при использовании с целью выделения информации запаздывания маскирующих колебаний и их сравнения со смесью полезного и маскирующих сигналов.

В настоящей работе моделируется новый способ скрытой передачи информации при маскировке шумоподобными колебаниями, основанный на использовании задержек сигналов с целью выделения полезной информации. При этом маскирующий сигнал может быть как хаотическим, так и стохастическим.

Схема, поясняющая описываемый способ скрытой передачи информации, представлена на рис. 1. Источник шумоподобных колебаний генерирует колебания $x = x(t)$ (хаотические или стохастические). Из этих колебаний выделяется радиоимпульс $f(x)$ длительностью τ, который разветвляется на два одинаковых сигнала $\varphi(x)$ (при $f(x) = 2\varphi(x)$), поступающих в разные каналы. В одном из каналов сигнал $\varphi(x)$ задерживается на время, равное длительности импульса, преобразуясь в сигнал $\varphi(x_\tau)$ (при $x_\tau = x(t-\tau)$), и поступает на сумматор. На этот же сумматор подаются незадержанный радиоимпульс $\varphi(x)$ и передаваемое сообщение $P(s)$ (при $s = s(t)$). Результирующий сигнал $\psi(u) = \varphi(x) + P(s) + \varphi(x_\tau)$ усиливается и передается по каналу связи.

В приемном устройстве сигнал усиливается до величины, достаточной для его обработки. Пренебрегая для простоты временем распространения сигнала в канале связи, которое легко учитывается, допустим, что принятый сигнал усиливается до уровня $2\psi(u)$, после чего разветвляется на два канала. В этом случае в каждый канал поступает сигнал $\psi(u) = \varphi(x) + P(s) + \varphi(x_\tau)$. В одном из каналов, например в первом, сигнал $\psi(u)$ проходит без изменения, а в другом задерживается на время τ, так что на выходе этого канала будем иметь сигнал в виде $\psi(u_\tau) = \varphi(x_\tau) + P[s(t-\tau)] + \varphi[x(t-2\tau)]$. Вычитая из этого сложного сигнала колебания $\psi(u)$, проходящие без задержки, будем иметь разностный сигнал $\psi_d(v) = -[\varphi(x) + P(s)] + P[s(t-\tau)] + \varphi[x(t-2\tau)]$. Этот сигнал отображает наличие трех последовательно следующих друг за другом радиоимпульсов. Первый радиоимпульс отображает обращенную сумму незадержанных маскирующего и полезного сигналов. Второй радиоимпульс определяет только полезный задержанный сигнал, а третий радиоимпульс — лишь маскирующие колебания, задержанные на 2τ. Поскольку полезным является лишь второй радиоимпульс, то первый и третий целесообразно устранить, что можно сделать путем открытия вычитающего устройства импульсом соответствующей длительности, вырабатываемым, например, в модуляторе при поступлении входного сигнала.

Численная реализация рассматриваемого способа скрытой передачи информации проводилась при использовании многомодового источника хаотических колебаний с запаздыванием. Его динамика описывается следующей системой дифференциальных уравнений [8]:

$$dx/dt = y - (\omega_0/Q)s, \quad dy/dt = F(z) - \omega_0^2 x, \quad dz/dt = [x_{\tau 0} - z]/\delta, \quad (1)$$

где $x = x(t)$, $y = y(t)$, $z = z(t)$, $x_{\tau 0} = x(t-\tau_0)$, τ_0 — время запаздывания колебаний в цепи обратной связи, ω_0, Q — резонансная частота и добротность фильтра в цепи обратной связи, δ — параметр релаксации инерционного элемента, $F(z)$ — нелинейная функция, определяющая характеристику усилителя. Расчеты проводились при асимметричной характеристике нелинейного элемента, имеющей вид

$$F(z) = Bz/[1 + (z - \xi)^n], \quad (2)$$

где B, ξ, n — парамтеры усиления, асимметрии и нелинейности.

Полезный сигнал формировался с помощью соотношения

$$s(t) = D[1 + m\sin(\omega_m t)]\sin(\omega_s t), \quad (3)$$

где D, m, ω_m, ω_s — постоянные величины.

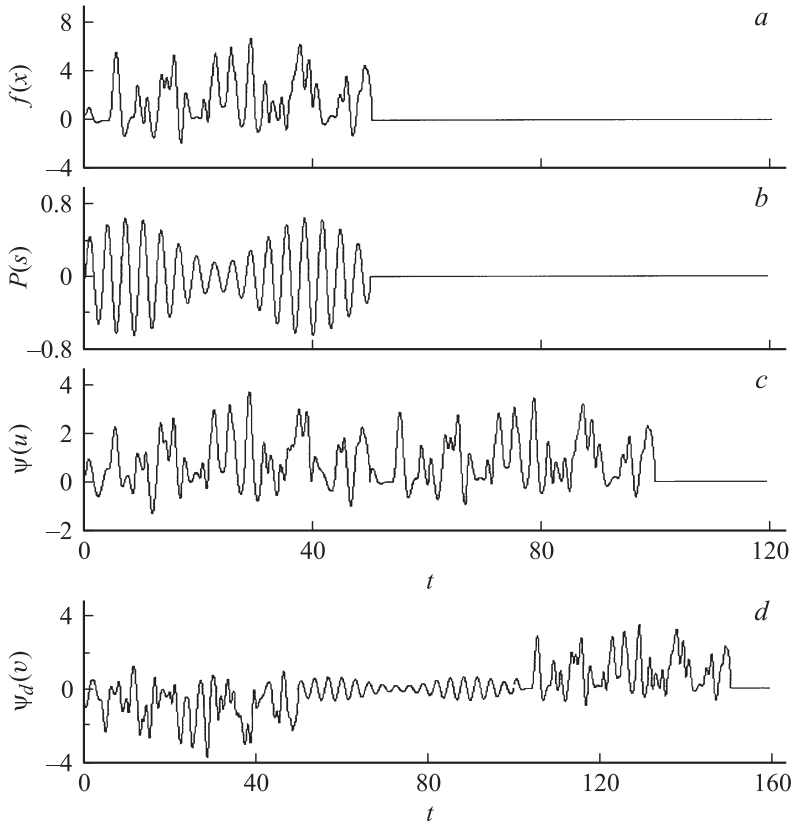

Рис. 2. Радиоимпульсы в передающем (a–c) и приемном (d) устройствах при передаче информации одним радиоимпульсом: a — маскирующие колебания; b — информационный сигнал; c — сумма полезного и маскирующих (задержанного и незадержанного) сигналов; d — разностные колебания.

Расчеты проводились при следующих значениях управляющих параметров: $\tau_0 = 4$, $\omega_0 = 2.8$, $Q = 1$, $\delta = 0.25$, $B = 6$, $\xi = 0.6$, $n = 4$, $D = 0.4$, $m = 0.6$, $\omega_s = 2$, $\omega_m = 0.6$. При этом длительность импульса, в пределах которой передается полезный сигнал и реализуется маскировка хаосом, равна $\tau = 50$.

На рис. 2, a показан радиоимпульс маскирующих колебаний $f(x)$, генерируемый в интервале времени $t \in [0; 50]$. Радиоимпульс разветв-

ляется в передающем устройстве на два канала, и в одном из них осуществляется задержка маскирующего радиоимпульса $\varphi(x)$ на время $\tau = 50$. Оба маскирующих импульса поступают на сумматор, на который подается также маскируемый сигнал, иллюстрируемый рис. 2, *b*. Результирующий сигнал на выходе сумматора $\psi(u)$ представлен на рис. 2, *c*. Этот сигнал в интервале времени $t \in [0; 50]$ отображает сумму маскирующего и полезного сигналов, а в интервале времени $t \in [50; 100]$ — маскирующие колебания.

Будем полагать, что в канале связи сигнал, показанный на рис. 2, *c*, не задерживается, а на входе приемного устройства усиливается до уровня $2\psi(u)$. В этом случае, после разветвления сигнала, в одном из каналов, не содержащем задержки, он будет занимать интервал времени $t \in [0; 100]$, а в другом (после задержки на время τ) — интервал $t \in [50; 150]$, имея при этом вид, подобный реализации, показанной на рис. 2, *c*. Разностные колебания на выходе вычитающего устройства $\psi_d(\nu)$ отображаются в этом случае фрагментом реализации, который представлен на рис. 2, *d*. Этот сигнал отображает в интервале времени $t \in [0; 150]$ колебания трех последовательно следующих друг за другом радиоимпульсов. В интервале времени $t \in [0; 50]$ реализуется обращенная сумма маскирующего и маскируемого сигналов, а в интервале $t \in [50; 100]$ выделяется полезный сигнал; в интервале времени $t \in [100; 150]$ отображаются только задержанные маскирующие колебания. Если вычитающее устройство открыто лишь на время $t \in [50; 100]$, то сигнал на выходе воспроизводится в этом интервале времени в виде, подобном показанному на рис. 2, *b*.

Рассмотренный способ маскировки и выделения информации представляет большой интерес при использовании ее передачи с помощью бинарного бита 0/1. Возможность такой скрытой передачи информации иллюстрируется рис. 3, который рассчитан применительно к серии радиоимпульсов при тех же параметрах в соотношениях (1) и (2), что и рис. 2, за исключением длительности импульсов и структуры подмешиваемого сигнала. В данном случае подмешиваемый сигнал может быть любым, в том числе и хаотическим. Для простоты и наглядности численное моделирование проводится при использовании гармонических колебаний.

На рис. 3, *a* показан фрагмент из серии радиоимпульсов $f(x)$, имеющих длительность $\tau = 15$ при скважности 1, формируемых из непрерывных хаотических колебаний $x(t)$. После разветвления колебаний и их задержки в одном из каналов на время длительности импульса

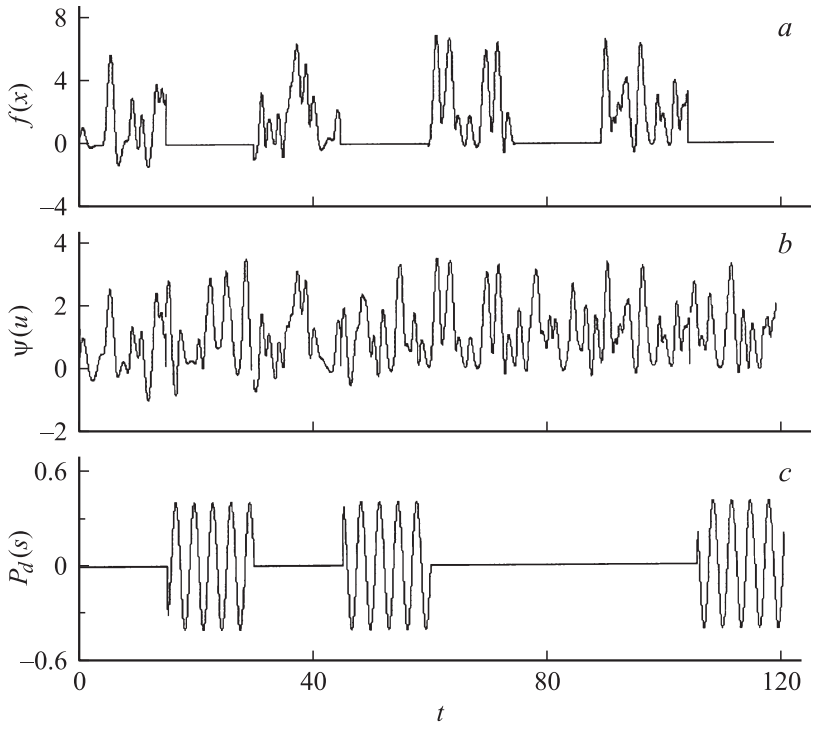

Рис. 3. Радиоимпульсы в передающем (a, b) и приемном (c) устройствах при передаче бинарной информации серией радиоимпульсов: a — маскирующие радиоимпульсы; b — сумма задержанных маскирующих радиоимпульсов и радиоимпульсов, несущих бинарный информационный сигнал; c — серия выделенных бинарных битов 0/1.

$\tau = 15$ в первый, второй и четвертый незадержанные радиоимпульсы в сумматоре подмешиваются регулярные колебания, получающиеся с помощью соотношения (3) при $m = 0$; по-прежнему $D = 0.4$, $\omega_s = 2$. Колебания на выходе передающего устройства иллюстрируются рис. 3, *b*. Полагая, что в канале связи сигнал не задерживается, для его выделения в приемном устройстве проводятся те же действия, что и в случае одиночного импульса, но при меньшей задержке сигнала (при $\tau = 15$). В результате на выходе вычитающего устройства реа-

лизуется сложный колебательный процесс с чередованием интервалов времени, в которых наблюдаются хаотические и регулярные колебания. Если открывать это устройство такими же импульсами, что и импульсы, определяющие колебательный процесс в передатчике, то выходной сигнал при соответствующей задержке открывающих импульсов преобразуется к серии радиоимпульсов $P_d(s)$, представленной на рис. 3, *c*. Импульсы, реализующиеся в интервалах времени $t \in [15; 30]$, $t \in [45; 60]$ и $t \in [105; 120]$, отображают единичные биты. Пропущенный импульс в интервале времени $t \in [75; 90]$ соответствует бите 0.

Приведенные результаты свидетельствуют о возможности практической реализации предложенного способа скрытой передачи информации при использовании как хаотических, так и стохастических маскирующих сигналов. Результаты численного моделирования показывают, что этот способ пригоден как применительно к незакодированной передаче информации, так и к передаче в режиме бита 0/1.

Работа выполнена при поддержке РФФИ (проект № 07-02-00351).

Список литературы

[1] *Гинзбург В.Л.* // УФН. 2007. Т. 177. В. 4. С. 346.
[2] *Дмитриев А.С., Панас А.И.* Динамический хаос: новые носители информации для систем связи. М.: Изд-во физ.-мат. литературы, 2002.
[3] *Залогин Н.Н., Кислов В.В.* Широкополосные хаотические сигналы в радиотехнических и информационных системах. М.: Радиотехника, 2006.
[4] *Пономаренко В.И., Прохоров М.Д.* // Письма в ЖТФ. 2005. Т. 31. В. 6. С. 73–78.
[5] *Короновский А.А., Москаленко О.И., Попов В.А.* и др. // Изв. РАН. Сер. Физ. 2008. Т. 72. № 1. С. 143–147.
[6] *Дмитриев А.С., Кяргинский Б.Е., Панас А.И.* и др. // Радиотехника и электроника. 2001. Т. 46. № 2. С. 224–233.
[7] *Кальянов Э.В., Кислов В.Я., Кяргинский Б.Е.* // Радиотехника и электроника. 2006. Т. 51. № 8. С. 976–983.
[8] *Кальянов Э.В.* // ЖТФ. 2007. Т. 77. В. 8. С. 1–5.