09

Цифровая система скрытой передачи информации на основе системы с запаздыванием

© А.С. Караваев, В.И. Пономаренко, Е.П. Селезнев, Е.Е. Глуховская, М.Д. Прохоров

Саратовский филиал Института радиотехники и электроники им. В.А. Котельникова РАН
E-mail: mdprokhorov@yandex.ru

Поступило в Редакцию 4 марта 2011 г.

Система скрытой передачи информации с нелинейным подмешиванием информационного сигнала к хаотическому сигналу генератора с запаздывающей обратной связью впервые экспериментально реализована на программируемом микроконтроллере с аналоговым входом и цифровой линией передачи.

Разработка информационно-коммуникационных систем, использующих явление синхронизации хаотических автоколебаний, привлекает к себе в последнее время большое внимание [1–11]. Распространенным способом передачи информации с хаотической несущей является нелинейное подмешивание информационного сигнала к хаотическому [12,13]. Одним из главным недостатков таких систем связи является сравнительно низкая помехоустойчивость [3,9]. Дело в том, что для обеспечения скрытности передачи информации уровень подмешиваемого сигнала должен быть существенно меньше уровня несущей. В таких условиях наличие помех в канале связи приводит к значительному искажению информационного сигнала, выделяемого на входе схемы.

Нами предлагается схема передачи информации, основанная на принципе нелинейного подмешивания, в которой информационный сигнал подмешивается к хаотическому сигналу, формируемому в результате цифровых вычислений на микроконтроллере. При этом в приемник, параметры которого совпадают с параметрами передатчика, поступает цифровой сигнал, и для извлечения его информационной компоненты также используются цифровые вычисления. Такая система передачи информации позволяет использовать маскировку информационного сигнала хаотическим сигналом высокой размерности и обладает

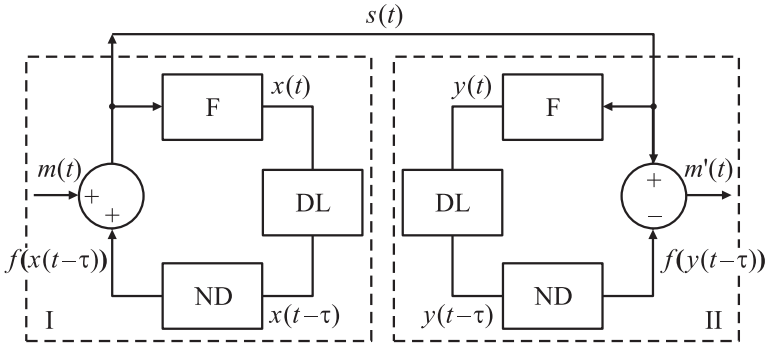

Рис. 1. Блок-схемы системы передачи информации с нелинейным подмешиванием: I — передатчик, II — приемник, DL — линия задержки, ND — нелинейный элемент, F — фильтр.

достаточно хорошей помехоустойчивостью, типичной для цифровых систем передачи информации.

Для повышения уровня конфиденциальности коммуникационных систем, использующих хаотические сигналы, было предложено осуществлять скрытую передачу данных на основе систем с запаздыванием, демонстрирующих хаотическую динамику очень высокой размерности [14–17]. Поэтому нами была выбрана схема передачи информации с нелинейным подмешиванием на базе генератора с запаздывающей обратной связью, блок-схема которой представлена на рис. 1. Передатчик представляет собой кольцевую систему из линии задержки, нелинейного элемента и линейного фильтра низких частот. Информационный сигнал $m(t)$ с помощью сумматора добавляется к хаотическому сигналу $f(x(t-\tau))$ на выходе нелинейного элемента, и сигнал $s(t) = f(x(t-\tau)) + m(t)$ передается в канал связи и одновременно вводится в кольцо обратной связи передающей системы, колебания которой описываются дифференциальным уравнением первого порядка с запаздыванием:

$$\varepsilon \dot{x}(t) = -x(t) + f\left(x(t-\tau)\right) + m(t), \qquad (1)$$

где $x(t)$ — состояние системы в момент времени t, f — нелинейная функция, τ — время запаздывания, ε — параметр, характеризующий

инерционность системы. При таком нелинейном подмешивании информационный сигнал непосредственно участвует в формировании сложной динамики генератора хаоса.

Приемник состоит из тех же элементов, что и передатчик, за исключением сумматора, который заменен на вычитатель, разрывающий цепь обратной связи. Уравнение, описывающее динамику принимающей системы, имеет вид:

$$\varepsilon \dot{y}(t) = -y(t) + f\big(x(t-\tau)\big) + m(t). \qquad (2)$$

На выходе вычитателя имеем восстановленный информационный сигнал $m'(t) = f(x(t-\tau)) + m(t) - f(y(t-\tau))$. Если элементы принимающей и передающей систем идентичны, то после переходного процесса эти системы синхронизуются между собой. Действительно, разность между колебаниями систем (1) и (2) $\Delta(t) = x(t) - y(t)$ уменьшается со временем при любых $\varepsilon > 0$, так как $\dot{\Delta}(t) = -\frac{\Delta(t)}{\varepsilon}$. В результате синхронизации имеем $x(t) = y(t)$, а значит $f(x(t-\tau)) = f(y(t-\tau))$ и $m'(t) = m(t)$. При этом качество восстановления сигнала $m(t)$ не зависит от его амплитудных и частотных характеристик, что означает возможность передачи без искажений сложных информационных сигналов.

Выбранный нами нелинейный элемент обеспечивает квадратичное преобразование. Уравнение передатчика при этом имеет вид:

$$\varepsilon \dot{x}(t) = -x(t) + \lambda - \big(x(t-\tau)\big)^2 + m(t), \qquad (3)$$

где λ — параметр нелинейности. Его величина была выбрана равной 1.9, что соответствовало хаотическому поведению системы.

Передающая система реализована в нашей схеме на программируемом микроконтроллере. Так как он не имеет встроенных аппаратных блоков поддержки операций с плавающей запятой, для повышения быстродействия системы все вычисления в микроконтроллера целесообразно проводить с помощью целочисленной арифметики. Для этого необходимо отмасштабировать переменные и параметры уравнения (3), воспользовавшись следующей логикой. При малых ε допустимые пределы изменения параметра λ, при которых в системе (3) существует периодический или хаотический аттрактор, составляют от 0 до 2. В этих пределах изменения λ динамическая переменная $x(t)$ может принимать значения от -2 до $+2$. Перейдем к целочисленной арифметике, преобразовав уравнение (3) так, чтобы динамическая переменная размещалась

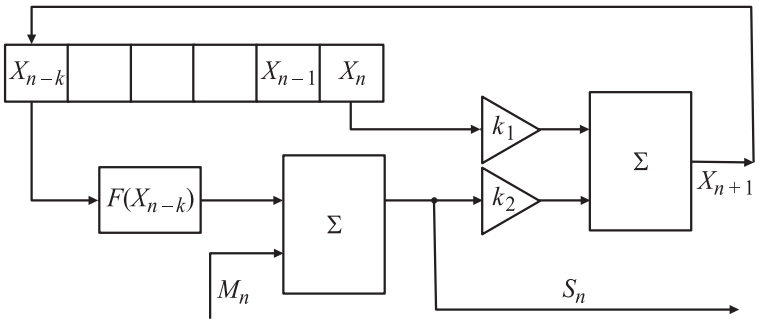

Рис. 2. Блок-схема передатчика, программно реализованного на базе микроконтроллера. Σ — сумматор, k_1 и k_2 — постоянные множители, $k_1 = 1 - \frac{\Delta t}{\varepsilon}$, $k_2 = \frac{\Delta t}{\varepsilon}$.

в 16-битной ячейке памяти, то есть, чтобы ее значение изменялось в диапазоне целых чисел от -2^{15} до 2^{15}. Это можно сделать, введя замену переменных: $X(t) = 2^{14}x(t)$, $M(t) = 2^{14}m(t)$. Тогда (3) примет следующий вид:

$$\frac{\varepsilon \dot{X}(t)}{2^{14}} = -\frac{X(t)}{2^{14}} + \lambda - \left(\frac{X(t-\tau)}{2^{14}}\right)^2 + \frac{M(t)}{2^{14}}. \tag{4}$$

Умножив обе части уравнения (4) на 2^{14} и введя $\Lambda = 2^{14}\lambda$, получим:

$$\varepsilon \dot{X}(t) = -X(t) + \Lambda - \frac{(X(t-\tau))^2}{2^{14}} + M(t). \tag{5}$$

Дифференциальное уравнение (5) можно свести к разностному уравнению, более удобному для программной реализации в микроконтроллере:

$$X_{n+1} = \left(1 - \frac{\Delta t}{\varepsilon}\right) X_n + \frac{\Delta t}{\varepsilon}\left(F(X_{n-k}) + M_n\right), \tag{6}$$

где n — дискретное время, Δt — шаг по времени, k — время задержки в единицах шагов дискретизации, $F(X_{n-k}) = \Lambda - \frac{X_{n-k}^2}{2^{14}}$.

На рис. 2 представлена блок-схема передатчика, программно реализованного на базе микроконтроллера. На первом шаге работы

программы микроконтроллера массив кольцевого буфера, содержащего значения от X_{n-k} до X_n, инициируется некоторой постоянной величиной в качестве канального условия. Затем вычисляется нелинейная функция $F(X_{n-k})$, к этому значению добавляется информационный сигнал M_n, и полученная сумма S_n передается в канал связи, организованный в виде последовательного цифрового интерфейса. Последующее значение дискретной динамической переменной X_{n+1} вычисляется в соответствии с соотношением (6) и помещается в кольцевой буфер. Через k циклов процесс инициализации завершается, и буфер заполняется реальными значениями.

Линейное преобразование сигнала осуществлялось нами с помощью низкочастотного цифрового фильтра Баттерворта первого порядка. Следует отметить, что использование фильтров высокого порядка с бесконечной или конечной импульсной характеристикой, как правило, позволяет повысить конфиденциальность системы связи. Чем больше коэффициентов в уравнении, описывающем фильтр, тем больше предыдущих значений переменной используется для вычисления следующего значения, и, следовательно, тем выше уровень конфиденциальности передаваемого сообщения. Нелинейное преобразование также может быть выбрано разного вида. Например, можно использовать отображение Бернулли, отображение „тент“ или другие отображения с хаотической динамикой.

Передатчик реализован в нашей схеме на основе программируемого микроконтроллера семейства Atmel megaAVR. В качестве информационного сигнала был выбран гармонический сигнал с частотой 10 Hz. Фрагмент его временной реализации представлен на рис. 3, *a*. Аналоговый информационный сигнал $m(t)$ подается на вход АЦП, а сигнал M_n с его выхода подмешивается в динамику передающей системы. Вычисления проводятся с использованием целочисленной арифметики. Размах колебаний хаотического сигнала составляет 16 bit, информационного сигнала — 8 bit.

На рис. 3, *b* показан фрагмент временной реализации хаотического сигнала $S_n = F(X_{n-k}) + M_n$, генерируемого автогенератором с задержкой на микроконтроллере при $\Delta t/\varepsilon = 0.5$ и $k = 10$. Этот сигнал имел частоту дискретизации 200 Hz ($\Delta t = 5$ ms) и передавался через интерфейс RS-232 по цифровому каналу связи на скорости 57.6 kbit/s. В качестве приемника использован персональный компьютер, в котором осуществляется выделение информационного сигнала. На выходе приемника имеем выделенный сигнал $M'_n = F(X_{n-k}) + M_n - F(Y_{n-k})$. При

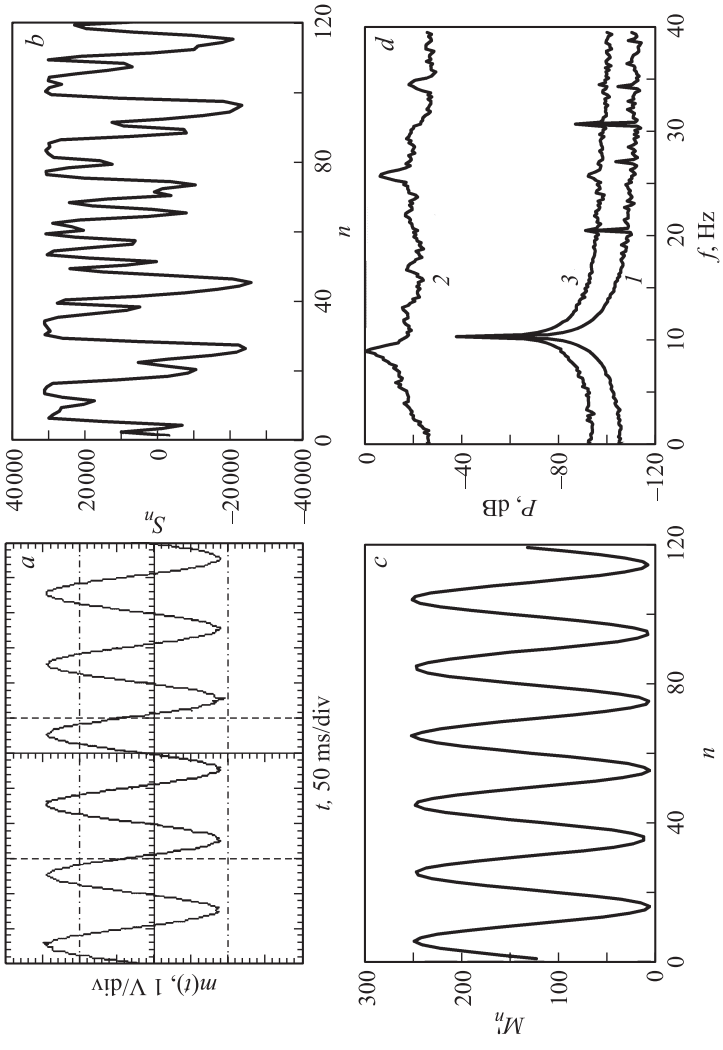

Рис. 3. *a* — осциллограмма реализации информационного сигнала $m(t)$; *b* — фрагмент временной реализации хаотического сигнала S_n; *c* — фрагмент временной реализации информационного сигнала M'_n, выделенного в приемнике; *d* — спектры мощности сигналов M_n — *1*, S_n — *2*, M'_n — *3*.

отсутствии шумов и выборе параметров приемника, равных параметрам передатчика, имеем $F(Y_{n-k}) = F(X_{n-k})$ и $M'_n = M_n$. Фрагмент временной реализации выделенного информационного сигнала M'_n представлен на рис. 3, *c*.

На рис. 3, *d* приведены спектры мощности хаотического сигнала S_n, гармонического информационного сигнала M_n и сигнала M'_n, выделенного в приемнике. Из рис. 3 видно, что качество восстановления скрытого информационного сигнала достаточно высокое.

Таким образом, нами продемонстрирована работоспособность предложенной системы цифровой передачи информации с нелинейным подмешиванием информационного сигнала к хаотическому сигналу генератора с запаздывающей обратной связью. Показано, что возможна экспериментальная реализация системы на базе единственной микросхемы.

Работа выполнена при поддержке РФФИ, грант № 10-02-00980 и целевой программы „Развитие научного потенциала высшей школы“, проект № 2.1.1/1738.

Список литературы

[1] *Cuomo K.M., Oppenheim A.V.* // Phys. Rev. Lett. 1993. V. 71. N 1. P. 65-68.
[2] *Pecora L.M., Carroll T.L., Johnson G.A.* et al. // Chaos. 1997. V. 7. N 4. P. 520—543.
[3] *Дмитриев А.С., Панас А.И.* Динамический хаос: новые носители информации для систем связи. Москва, Физматлит. 2002. 252 с.
[4] *Ponomarenko V.I., Prokhorov M.D.* // Phys. Rev. E. 2002. V. 66. N 2. P. 026215.
[5] *Chen J.Y., Wong K.W., Cheng L.M., Shuai J.W.* // Chaos. 2003. V. 13. N 2. P. 508–514.
[6] *Kye W.-H., Choi M., Kim C.-M., Park Y.-J.* // Phys. Rev. E. 2005. V. 71. N 4. 045202.
[7] *Behnia S., Akhshani A., Ahadpour S.* et al. // Phys. Lett. A. 2007. V. 366. N 4–5. P. 391–396.
[8] *Sun Y.H., Cao J., Feng G.* // Phys. Lett. A. 2008. V. 372. N 33. P. 5442–5447.
[9] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // УФН. 2009. Т. 179. В. 12. С. 1281–1310.
[10] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // ЖТФ. 2010. Т. 80. В. 4. С. 1–8.
[11] *Кальянов Э.В., Кяргинский Б.Е.* // Письма в ЖТФ. 2010. Т. 36. В. 23. С. 1–8.
[12] *Волковский А.П., Рульков Н.Ф.* // Письма в ЖТФ. 1993. Т. 19. В. 3. С. 71–75.

[13] *Dmitriev A.S., Panas A.I., Starkov S.O.* // Int. J. of Bifurcation and Chaos. 1995. V. 5. N 4. P. 1249–1254.
[14] *Mensour B., Longtin A.* // Phys. Lett. A. 1998. V. 244. N 1–3. P. 59–70.
[15] *Pyragas K.* // Int. J. of Bifurcation and Chaos. 1998. V. 8. N 9. P. 1839–1842.
[16] *Пономаренко В.И., Прохоров М.Д.* // Радиотехника и электроника. 2004. Т. 49. № 9. С. 1098–1104.
[17] *Кальянов Э.В.* // Письма в ЖТФ. 2009. Т. 35. В. 6. С. 56–62.