УДК 537.86

СИСТЕМА ЦИФРОВОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ, МАСКИРУЕМОЙ ХАОТИЧЕСКИМ СИГНАЛОМ СИСТЕМЫ С ЗАПАЗДЫВАНИЕМ

А. С. Караваев,
канд. физ.-мат. наук, доцент
Д. Д. Кульминский,
инженер
Саратовский государственный университет им. Н. Г. Чернышевского
В. И. Пономаренко,
доктор физ.-мат. наук, ведущий научный сотрудник
М. Д. Прохоров,
доктор физ.-мат. наук, ведущий научный сотрудник
Саратовский филиал Института радиотехники и электроники им. В. А. Котельникова РАН

Система передачи информации с нелинейным подмешиванием информационного сигнала к хаотическому сигналу генератора с запаздывающей обратной связью экспериментально реализована на программируемых микроконтроллерах с цифровой линией передачи. Предложенная схема позволяет передавать и принимать речевые и музыкальные сигналы в реальном времени без заметных искажений.

Ключевые слова *— система передачи информации, хаотическая синхронизация, системы с запаздыванием.*

Введение

Разработка систем передачи информации, использующих явление синхронизации хаотических автоколебаний, привлекает к себе большое внимание [1–7]. Интерес к хаотическим коммуникационным системам обусловлен тем, что хаотические системы обладают широкополосным спектром мощности, позволяют обеспечить высокую скорость передачи информации и остаются работоспособны при малых отношениях сигнала к шуму. Кроме того, они допускают возможность простой аппаратурной реализации с большим выбором различных колебательных режимов.

Для повышения конфиденциальности хаотических систем связи было предложено осуществлять скрытую передачу данных на основе систем с запаздыванием, демонстрирующих хаотическую динамику очень высокой размерности [8–12]. В настоящее время известно много разных способов передачи информационного сигнала с хаотической несущей, из которых одним из наиболее распространенных является нелинейное подмешивание информационного сигнала к хаотическому [5]. Однако одним из главных недостатков таких систем связи является сравнительно низкая помехоустойчивость [6]. Дело в том, что для обеспечения скрытности передачи информации уровень сигнала сообщения должен быть существенно меньше уровня хаотической несущей. В таких условиях наличие помех в канале связи приводит к значительному искажению информационного сигнала, выделяемого на выходе схемы.

В данной работе мы предлагаем систему передачи информации, основанную на принципе нелинейного подмешивания, в которой информационный сигнал подмешивается к хаотическому сигналу генератора с запаздывающей обратной связью, 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 использует маскировку информационного сигнала хаотическим сигналом высокой размерности и позволяет передавать и принимать речевые и музыкальные сигналы в реальном времени без заметных искажений.

Система передачи информации

Блок-схема системы связи с нелинейным подмешиванием 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:

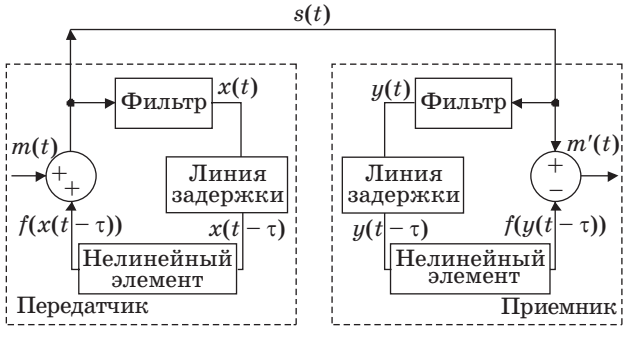
$$\varepsilon\dot{x}(t) = -x(t) + f\big(x(t-\tau)\big) + m(t), \qquad (1)$$

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 $\dot{\Delta}(t) = -\Delta(t)/\varepsilon$. 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 передавать без искажений сложные информационные сигналы.



■ ***Рис. 1.*** Блок-схема системы передачи информации с нелинейным подмешиванием

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. Параметры передатчика выбираются таким образом, чтобы система находилась в режиме развитых хаотических колебаний.

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 микроконтроллере 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 в 16-битной ячейке памяти, т. е. 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:

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

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

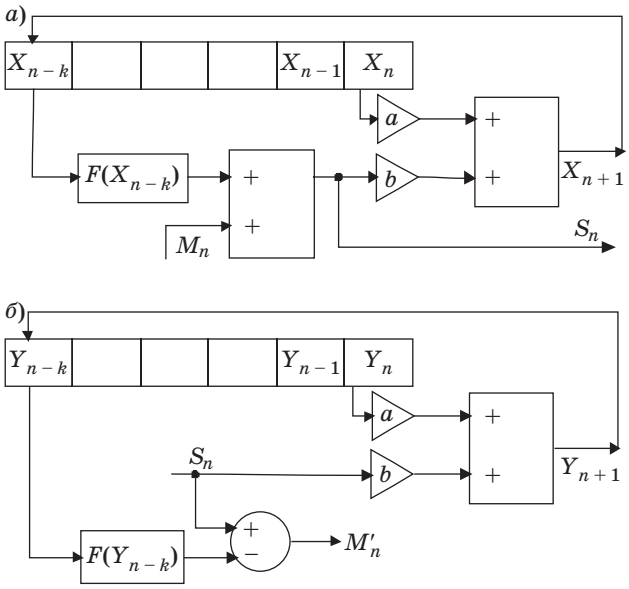
$$\varepsilon\dot{X}(t) = -X(t) + \Lambda - \frac{(X(t-\tau))^2}{2^{14}} + M(t). \qquad (5)$$

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

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

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

Блок-схема передатчика, программно реализованного на базе микроконтроллера, представлена на рис. 2, *а*. На первом шаге работы программы массив кольцевого буфера, содержащего зна-



■ ***Рис. 2.*** Блок-схемы передатчика (*а*) и приемника (*б*), программно реализованных на базе микроконтроллера: *a* и *b* — постоянные множители, $a = 1 - \Delta t/\varepsilon$, $b = \Delta t/\varepsilon$

чения от X_{n-k} до X_n, инициализируется некоторой постоянной величиной в качестве начального 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. Блок-схема приемника, программно реализованного на базе микроконтроллера, представлена на рис. 2, *б*.

Линейное преобразование сигнала осуществлялось нами с помощью низкочастотного цифрового фильтра Баттерворта первого порядка. Следует отметить, что использование фильтров высокого порядка, как правило, позволяет повысить конфиденциальность системы связи. Чем больше коэффициентов в уравнении, описывающем фильтр, тем больше предыдущих значений переменной используется для вычисления следующего значения. При этом для выделения скрытого сообщения необходимо знать больше параметров. Нелинейное преобразование также может быть выбрано разного вида. Например, можно использовать отображение «тент» или другие отображения с хаотической динамикой. Использованная в данной работе квадратичная нелинейная функция, имеющая единственный управляющий параметр, была выбрана в качестве простейшего примера нелинейного преобразования для реализации хаотического автогенератора с запаздыванием на базе микроконтроллера.

Иллюстрация работы схемы

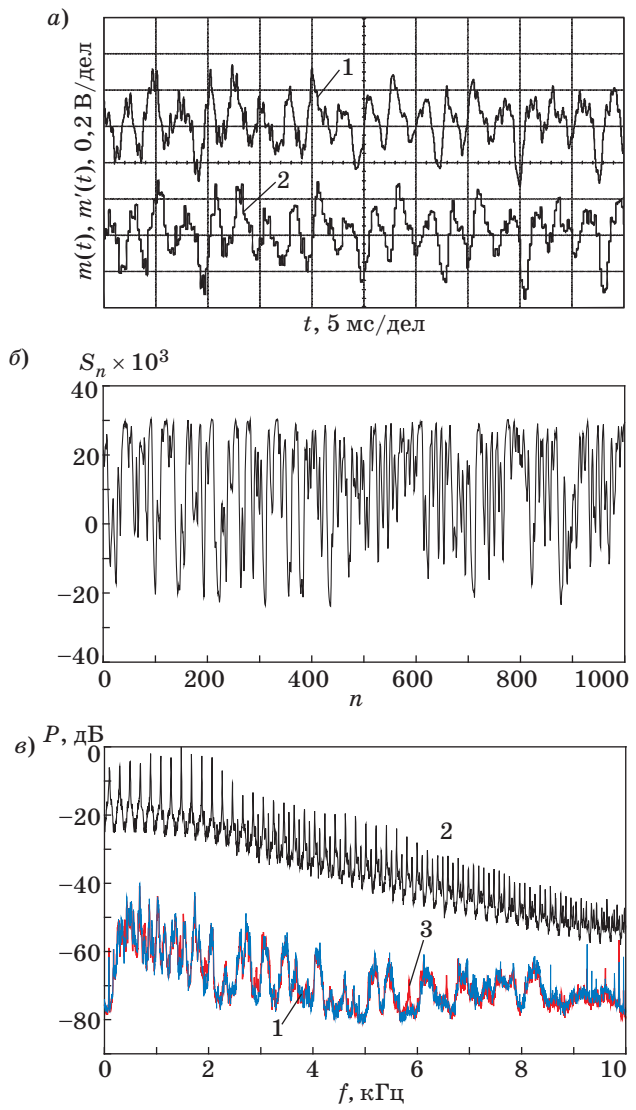
Передатчик реализован в нашей схеме на основе программируемого микроконтроллера семейства Atmel xmegaAVR. Аналоговый информационный сигнал $m(t)$ подается на вход аналого-цифрового преобразователя (АЦП), а сигнал M_n с его выхода подмешивается в динамику передающей системы. Вычисления проводятся с использованием целочисленной арифметики.

Проиллюстрируем работоспособность предложенной схемы при выборе в качестве информационного сигнала музыкальной композиции с достаточно широким спектром в диапазоне звуковых частот (песни). Фрагмент временной реализации такого сигнала представлен на рис. 3, *а*. Для оцифровки сигнала мы использовали 12 разрядов АЦП с частотой дискретизации 20 кГц ($\Delta t = 50$ мкс).

Фрагмент временной реализации хаотического сигнала $S_n = F(X_{n-k}) + M_n$, генерируемого автогенератором с задержкой на микроконтроллере при $\lambda = 1{,}9$, $\Delta t/\varepsilon = 0{,}5$ и $k = 100$, показан на рис. 3, *б*. Этот 16-битный сигнал тоже имел частоту дискретизации 20 кГц и передавался по цифровому каналу связи стандарта RS-485. Если пропустить этот сигнал через цифроаналоговый преобразователь (ЦАП) и воспроизвести, то будет слышен только шум без каких-либо признаков речи и музыки.

Приемник в схеме реализован на основе такого же программируемого микроконтроллера, что и передатчик. На выходе вычитателя приемника имеем выделенный информационный сигнал $M'_n = F(X_{n-k}) + M_n - F(Y_{n-k})$. При отсутствии шумов и выборе параметров приемника, равных параметрам передатчика, имеем $F(Y_{n-k}) = F(X_{n-k})$ и $M'_n = M_n$. Подав цифровой сигнал M'_n на вход ЦАП, получим на выходе восстановленный аналоговый информационный сигнал $m'(t)$. Фрагмент его временной реализации тоже представлен на рис. 3, *а* для случая, когда параметры приемника имеют такие же значения, как и параметры передатчика. Из рис. 3, *а* видно, что временные реализации передаваемого и выделенного информационных сигналов очень похожи. На слух исходный музыкальный сигнал $m(t)$ и сигнал $m'(t)$ на выходе приемника не различимы.

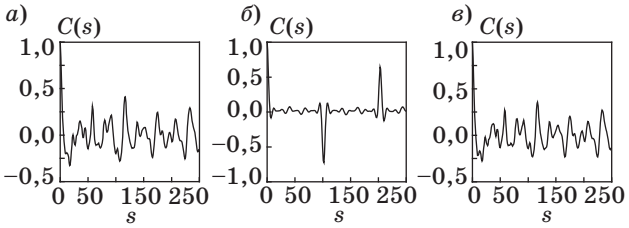
Спектры мощности хаотического сигнала S_n, информационного сигнала M_n и выделенного в приемнике информационного сигнала M'_n приведены на рис. 3, *в*. Амплитуда музыкального ин-



■ ***Рис. 3.*** Осциллограммы реализаций музыкального информационного сигнала $m(t)$ на входе схемы *1* и восстановленного информационного сигнала $m'(t)$ на выходе схемы *2* (*а*); фрагмент временной реализации хаотического сигнала S_n (*б*); спектры мощности сигналов: *1* — M_n; *2* — S_n, *3* — M'_n (*в*)

формационного сигнала составляет около 5 % от амплитуды хаотической несущей, и его присутствие незаметно в спектре мощности передаваемого сигнала S_n. Из рис. 3, *в* видно, что спектры сигналов M_n и M'_n практически совпадают.

В дополнение к представлению исследуемых сигналов во временной и спектральной областях мы построили их автокорреляционные функции (АКФ). На рис. 4, *а*—*в* показаны АКФ $C(s)$ передаваемого информационного сигнала, хаотического сигнала в канале связи, а также информационного сигнала, выделенного на выходе приемника при идентичности параметров приемника



■ ***Рис. 4.*** Автокорреляционные функции информационного сигнала M_n (*а*), сигнала S_n в канале связи (*б*) и информационного сигнала M'_n на выходе приемника при идентичности параметров приемника и передатчика (*в*)

и передатчика. Видно, что АКФ передаваемого и выделенного информационных сигналов очень близки, а АКФ хаотического сигнала в канале связи быстро спадает, но имеет характерные пики на временах, близких времени запаздывания и удвоенному времени запаздывания.

Таким образом, качество восстановления информационного сигнала на выходе приемника оказывается достаточно высоким. Предложенная схема позволяет осуществлять передачу и прием речевых и музыкальных сигналов в реальном времени без заметных искажений.

Выделение информационного сигнала при расстройке параметров приемника и передатчика

В рассмотренном выше примере передатчик и приемник имели одинаковые значения параметров, что обеспечивало для авторизованного слушателя качественный прием информационного сигнала. Идентичность параметров приемника и передатчика является важной составляющей систем передачи информации, основанных на синхронизации хаотических систем. С увеличением расстройки параметров приемника и передатчика ухудшается качество хаотического синхронного отклика приемника и, как следствие, ухудшается качество выделяемого информационного сигнала [5]. Начиная с некоторого значения расстройки, выделение полезного сообщения становится невозможным. Достоинством предложенной цифровой системы связи является использование в ней программируемых микроконтроллеров, что позволяет добиться полной идентичности параметров передатчика и приемника, практически недостижимой при построении передающей и принимающих систем на аналоговых элементах.

Для стороннего наблюдателя сигнал, передаваемый через открытый канал связи, воспринимается как шум. Для выделения сигнала сообщения из хаотической несущей неавторизованному

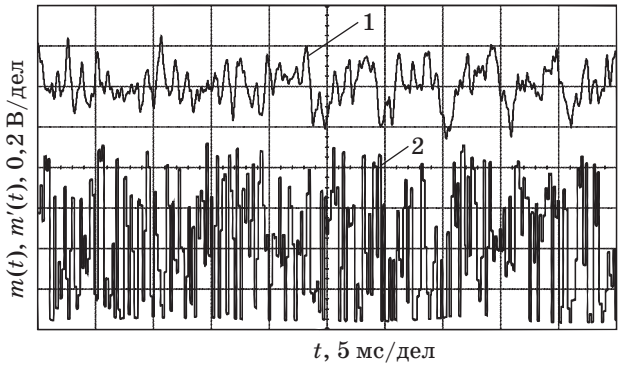
слушателю необходимо знать конфигурацию передатчика, т. е. ему должно быть известно, что передатчик описывается модельным уравнением с запаздыванием (1), а также необходимо знать вид нелинейной функции f и точные значения параметров системы. Для реконструкции модельных уравнений систем с запаздыванием и восстановления их параметров по временным рядам был предложен ряд методов [13–18]. В отсутствие шума эти методы позволяют с хорошей точностью определить неизвестные параметры систем с запаздыванием. Однако при наличии шума оценка параметров оказывается менее точной, причем с ростом уровня шума погрешность оценки параметров растет. Кроме того, присутствие шума может привести к искажению информационного сигнала на выходе схемы [19, 20].

В рассмотренной системе передачи информации используется нелинейное подмешивание информационного сигнала к хаотическому сигналу системы с задержкой. При этом присутствие информационного сигнала в хаотической несущей, так же как и присутствие шума, неизбежно снижает точность оценки управляющих параметров системы. Мы исследовали, насколько точно необходимо знать значения параметров передающей системы для того, чтобы выделить информационный сигнал на выходе приемника.

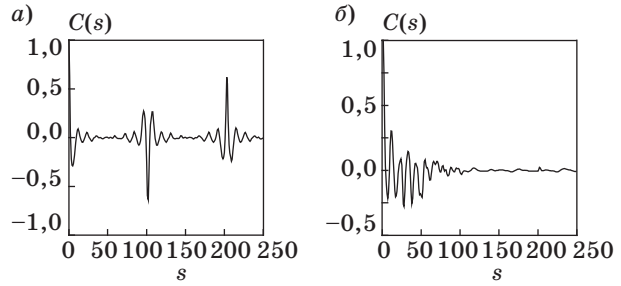
Выберем параметры передатчика так же, как в рассмотренном выше примере, и будем передавать тот же музыкальный сигнал. Параметры приемника возьмем такими же, как в передатчике, за исключением дискретного времени запаздывания k, которое будем менять вблизи истинного значения $k = 100$. Уже при минимальной расстройке k на единицу ($k = 99$ или $k = 101$) на выходе приемника слышен только шум, т. е. при расстройке времени запаздывания в приемнике и передатчике на 1 % информационный сигнал выделить не удается. Фрагменты временных реализаций исходного музыкального сигнала $m(t)$ и сигнала $m'(t)$, выделенного в приемнике при $k = 99$, показаны на рис. 5. Амплитуда сигнала $m'(t)$ значительно больше, чем у сигнала $m(t)$, а сам сигнал $m'(t)$ больше похож на хаотическую несущую.

На рис. 6, *а* приведена АКФ сигнала, выделенного на выходе приемника при расстройке дискретного времени запаздывания k на 1 %. Эта АКФ больше похожа на АКФ сигнала в канале связи (см. рис. 4, *б*), чем на АКФ информационного сигнала на входе схемы (см. рис. 4, *а*).

Исследуем теперь влияние расстройки параметра ε на качество выделения информационного сигнала. Положим параметры приемника и передатчика одинаковыми за исключением параметра ε, который будем менять вблизи истинного



■ ***Рис. 5.*** Осциллограммы реализаций исходного информационного сигнала $m(t)$ *1* и сигнала $m'(t)$ *2*, выделенного в приемнике при расстройке параметра k ($k = 99$)



■ ***Рис. 6.*** Автокорреляционные функции сигналов M'_n на выходе приемника при расстройке параметра k ($k = 99$) (*а*) и параметра ε (ε = = 99 мкс) (*б*)

значения ε = 100 мкс. Установлено, что при расстройке ε более чем на 1,5 % как в положительную, так и в отрицательную сторону, информационный сигнал на выходе приемника не прослушивается, а его временная реализация и спектр мощности существенно отличны от оригинальных. При расстройке ε на 0,1–1,0 % информационный сигнал маскируется частично. При его прослушивании на выходе приемника удается различить отдельные слова и музыкальный фон, хотя временные реализации и спектры мощности сигналов $m'(t)$ и $m(t)$ при этом существенно отличаются. При расстройке ε в приемнике и передатчике на 0,05 %, музыкальный сигнал выделяется с небольшими помехами, которые исчезают при дальнейшем уменьшении расстройки.

На рис. 6, *б* приведена АКФ сигнала, выделенного на выходе приемника при расстройке параметра ε на 1 %. Эта АКФ заметно отлична от АКФ информационного сигнала на входе схемы (см. рис. 4, *а*) и быстрее спадает.

Таким образом, для выделения информационного сигнала стороннему наблюдателю необходимо с высокой точностью восстановить параметры передатчика, что является непростой задачей для рассмотренной системы связи.

Заключение

Нами предложена и экспериментально реализована система цифровой передачи информации с нелинейным подмешиванием информационного сигнала к хаотическому сигналу генератора с запаздывающей обратной связью, в которой передатчик и приемник реализованы на простых программируемых микроконтроллерах. Такая система связи позволяет без заметных искажений передавать и принимать в реальном времени речевые и музыкальные сигналы. Высокое качество приема информационного сигнала достигается за счет использования в передатчике и приемнике цифровых элементов, обеспечивающих идентичность параметров.

Исследована возможность выделения полезной информации из хаотической несущей при расстройке параметров приемника и передатчика предложенной схемы. Установлено, что для выделения информационного сигнала расстройка параметров не должна превышать 1 %.

Работа выполнена при поддержке РФФИ, грант № 13-02-00227, и гранта президента РФ, МК-4435.2012.8.

Литература

1. **Pecora L. M., Carroll T. L.** Synchronization in chaotic systems // Phys. Rev. Lett. 1990. Vol. 64. P. 821–824.
2. **Parlitz U.** et al. Transmission of digital signals by chaotic synchronization // Int. J. of Bifurcation and Chaos. 1992. Vol. 2. P. 973–977.
3. **Cuomo K. M., Oppenheim A. V.** Circuit implementation of synchronized chaos with applications to communications // Phys. Rev. Lett. 1993. Vol. 71. P. 65–68.
4. **Pecora L. M.** et al. Fundamentals of synchronization in chaotic systems, concepts, and applications // Chaos. 1997. Vol. 7. P. 520–543.
5. **Дмитриев А. С., Панас А. И.** Динамический хаос: новые носители информации для систем связи. – М.: Физматлит, 2002. – 252 с.
6. **Короновский А. А., Москаленко О. И., Храмов А. Е.** О применении хаотической синхронизации для скрытой передачи информации // УФН. 2009. Т. 179. С. 1281–1310.
7. **Короновский А. А., Москаленко О. И., Храмов А. Е.** Скрытая передача информации на основе режима обобщенной синхронизации в присутствии шумов // ЖТФ. 2010. Т. 80. В. 4. С. 1–8.
8. **Pyragas K.** Transmission of signals via synchronization of chaotic time-delay systems // Int. J. of Bifurcation and Chaos. 1998. Vol. 8. P. 1839–1842.
9. **Ponomarenko V. I., Prokhorov M. D.** Extracting information masked by the chaotic signal of a time-delay system // Phys. Rev. E. 2002. Vol. 66. 026215.
10. **Пономаренко В. И., Прохоров М. Д.** Кодирование и извлечение информации, замаскированной хаотическим сигналом системы с запаздыванием // Радиотехника и электроника. 2004. Т. 49. № 9. С. 1098–1104.
11. **Kye W.-H., Choi M., Kim C.-M., Park Y.-J.** Encryption with synchronized time-delayed systems // Phys. Rev. E. 2005. Vol. 71. 045202.
12. **Nguimdo R. M., Colet P., Larger L., Pesquera L.** Digital key for chaos communication performing time delay concealment // Phys. Rev. Lett. 2011. Vol. 107. 034103.
13. **Voss H., Kurths J.** Reconstruction of non-linear time delay models from data by the use of optimal transformations // Phys. Lett. A. 1997. Vol. 234. P. 336–344.
14. **Bünner M. J.** et al. Reconstruction of systems with delayed feedback: (I) Theory // Eur. Phys. J. D. 2000. Vol. 10. P. 165–176.
15. **Пономаренко В. И., Прохоров М. Д., Караваев А. С., Безручко Б. П.** Определение параметров систем с запаздывающей обратной связью по хаотическим временным реализациям // ЖЭТФ. 2005. Т. 127. С. 515–527.
16. **Zunino L.** et al. Permutation-information-theory approach to unveil delay dynamics from time-series analysis // Phys. Rev. E. 2010. Vol. 82. 046212.
17. **Ma H., Xu B., Lin W., Feng J.** Adaptive identification of time delays in nonlinear dynamical models // Phys. Rev. E. 2010. Vol. 82. 066210.
18. **Dai C.** et al. Seeker optimization algorithm for parameter estimation of time-delay chaotic systems // Phys. Rev. E. 2011. Vol. 83. 036203.
19. **Никитин В. Н., Юркин Д. В.** Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6. С. 42–46.
20. **Мальцев Г. Н., Чернявский Е. В.** Кодирование сообщений в системах радиоуправления без обратного информационного канала // Информационно-управляющие системы. 2011. № 4. С. 60–65.