РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2349044

СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Патентообладатель(ли): ***Государственное образовательное учреждение высшего профессионального образования "Саратовский государственный университет им. Н.Г. Чернышевского" (RU)***

Автор(ы): ***см. на обороте***

Заявка № **2007132422**

Приоритет изобретения **27 августа 2007 г.**

Зарегистрировано в Государственном реестре изобретений Российской Федерации ***10 марта 2009 г.***

Срок действия патента истекает **27 августа 2027 г.**

Руководитель Федеральной службы по интеллектуальной собственности, патентам и товарным знакам

Б.П. Симонов

Автор(ы): ***Короновский Алексей Александрович (RU), Москаленко Ольга Игоревна (RU), Храмов Александр Евгеньевич (RU)***

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 349 044** (13) **C1**

(51) МПК
H04L 9/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2007132422/09, 27.08.2007**

(24) Дата начала отсчета срока действия патента:
27.08.2007

(45) Опубликовано: **10.03.2009 Бюл. № 7**

(56) Список документов, цитированных в отчете о поиске: **RU 2295835 C1, 20.03.2007. RU 2000107936 A, 27.02.2002. RU 2204886 C2, 20.06.2003. US 5291555 A, 01.03.1994. US 6744893 B1, 01.06.2004. US 6363151 B1, 26.03.2002. US 5923760 A, 13.07.1999. WO 01/65755 A2, 07.09.2001.**

Адрес для переписки:
410012, г.Саратов, ул. Московская, 155, СГУ, ПЛО, О.И. Куприяновой, рег. № 330

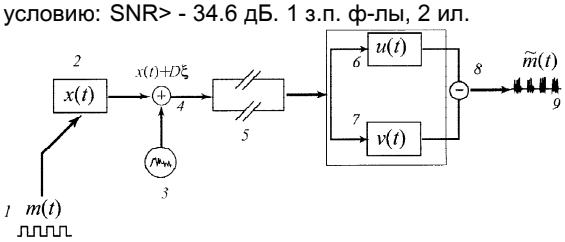
(72) Автор(ы):
Короновский Алексей Александрович (RU),
Москаленко Ольга Игоревна (RU),
Храмов Александр Евгеньевич (RU)

(73) Патентообладатель(и):
Государственное образовательное учреждение высшего профессионального образования "Саратовский государственный университет им. Н.Г. Чернышевского" (RU)

(54) СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

(57) Реферат:

Изобретение относится к радиотехнике и передаче информации и может найти применение в системах связи для помехоустойчивой передачи цифровой информации с определенной степенью конфиденциальности. Технический результат - повышение надежности и создания дополнительной секретности. Для этого в способе скрытой передачи информации полезный сигнал кодируют в двоичный код, формируют посредством первого хаотического генератора исходный детерминированный хаотический сигнал путем модуляции параметров хаотического сигнала полезным цифровым сигналом, передают сформированный таким образом сигнал по каналу связи принимающей стороне, где его делят на два идентичных сигнала, которыми воздействуют на второй и третий хаотические генераторы. Второй и третий хаотические генераторы идентичны друг другу по управляющим параметрам и выбраны с возможностью обеспечения режима обобщенной синхронизации с первым хаотическим генератором. Снятые с выходов указанных второго и третьего генераторов сигналы подают на вычитающее устройство и при наблюдении или отсутствии хаотических колебаний определяют наличие полезного цифрового сигнала, представленного в виде двоичного кода. Сформированный первым хаотическим генератором детерминированный хаотический сигнал перед передачей по каналу связи суммируют с шумовым сигналом, производимым генератором шума, при этом первый хаотический генератор и генератор шума настраивают в режим, при котором отношение сигнал/шум SNR удовлетворяет следующему условию: SNR> - 34.6 дБ. 1 з.п. ф-лы, 2 ил.



Фиг. 1

RU 2349044 C1

RU 2349044 C1

RUSSIAN FEDERATION

(19) **RU** (11) **2 349 044** (13) **C1**

(51) Int. Cl.
H04L 9/00 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2007132422/09, 27.08.2007**

(24) Effective date for property rights: **27.08.2007**

(45) Date of publication: **10.03.2009 Bull. 7**

Mail address:
410012, g.Saratov, ul. Moskovskaja, 155, SGU, PLO, O.I. Kuprijanovoj, reg. № 330

(72) Inventor(s):
Koronovskij Aleksej Aleksandrovich (RU),
Moskalenko Ol'ga Igorevna (RU),
Khramov Aleksandr Evgen'evich (RU)

(73) Proprietor(s):
Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Saratovskij gosudarstvennyj universitet im. N.G. Chernyshevskogo" (RU)

(54) METHOD OF HIDDEN INFORMATION TRANSFER

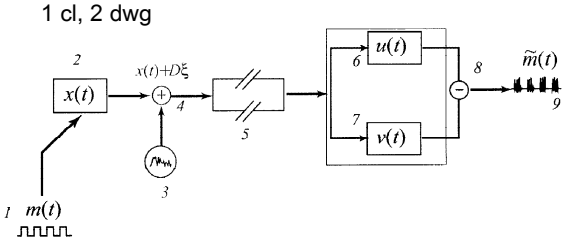
(57) Abstract:

FIELD: physics, radio.

SUBSTANCE: invention concerns a radio engineering and an information transfer and application in communication systems for unjammable transmission of the numeral information with a certain degree of confidentiality can find. In an expedient of the latent information transfer the useful signal code in a dyadic code, shape by means of the first chaotic generator the initial determined chaotic signal by modulation of parameters of a chaotic signal by the useful numeral signal, transmit the signal generated thus on a communication channel to a receiving party where it divide into two identical signals with which influence the second and third chaotic generators. The second and third chaotic generators are identical each other on driving parameters and are chosen with possibility of maintenance of a mode of the generalised sync with the first chaotic generator. Obtained from outputs of the specified second and third generators signals submit on subtracting device and at observation or lack of chaotic oscillations spot presence of the useful numeral signal presented in the form of a dyadic code. The determined chaotic signal generated by the first chaotic generator before transmission on a communication channel with the noise signal yielded by the generator of noise, thus the first chaotic generator and the noise generator attune in a mode at which signal/noise SNR satisfies the relation to a following requirement: SNR>- 34.6 dB.

EFFECT: pinch of reliability and making of additional privacy.

1 cl, 2 dwg



Фиг. 1

RU 2349044 C1

RU 2349044 C1

Изобретение относится к радиотехнике и передаче информации и может найти применение в системах связи для помехоустойчивой передачи цифровой информации с определенной степенью конфиденциальности.

В большинстве предложенных ранее способов скрытой передачи информации используется явление полной хаотической синхронизации между идентичными хаотическими генераторами, находящимися на различных сторонах канала связи. Это, в первую очередь, хаотическая маскировка (Cuomo K., Oppenheim A. Communication using synchronized chaotic systems // US Patent No. 5291555 от 1.03.1994), переключение хаотических режимов (Dedieu H., Kennedy M.P., Hosler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using delf-synchronizing Chua's circuits // IEEE Trans. on Circ. Sys., I. 40, 1993, 634), нелинейное подмешивание информационного сигнала к хаотическому (Dmitriev A.S., Panas A.I., Starkov S.O. Experiments on speach and music signals transmission using chaos // Int. J. Bifurcations and Chaos. 5 (4), 1995, 1249), модулирование управляющих параметров хаотического сигнала информационным (Yang T., Chua L.O. Secure communication via chaotic parameter modulation // IEEE Trans. on Circ. Sys., I. 43, 1996, 817) и др. Существуют также попытки использования обобщенной синхронизации для этих целей (Terry J.R., VanWiggeren G.D. Chaotic communication using generalized synchronization // Chaos, Solitons and Fractals. 12, 2001, 145) или обоих вышеупомянутых типов синхронного поведения одновременно (Murali K., Lakshmanan M. Secure communication using a compound signal from generalized synchronizable chaotic systems // Phys. Lett. A. 241, 1998, 303; Terry J.R., VanWiggeren G.D. Chaotic communication using generalized synchronization // Chaos, Solitons and Fractals. 12, 2001, 145).

Принципиальными недостатками всех предложенных в настоящее время схем являются следующие:

1) Требование высокой степени идентичности хаотических генераторов на различных сторонах канала связи, что является очень серьезной и труднореализуемой задачей, особенно в течение длительного времени эксплуатации устройств. Малая расстройка значений управляющих параметров этих генераторов приводит к потере значительной части передаваемой информации.

2) Достаточно низкая устойчивость к шумам и флуктуациям в канале связи. При превышении интенсивностью шума и флуктуаций некоторого порогового значения, сравнимого с естественными шумами и искажениями, известные системы передачи информации становятся неработоспособными.

3) Возможность реконструкции параметров передающего генератора по сигналу, передаваемому по каналу связи (особенно в случае использования полной хаотической синхронизации для скрытой передачи информации). Из-за наличия точной копии передающего генератора на другой стороне канала связи третья сторона в некоторых случаях может легко дешифровать информационное сообщение.

Всех вышеперечисленных недостатков лишен способ скрытой передачи информации (Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е. Способ секретной передачи информации // Патент на изобретение №2295835 от 20.03.2007). Он основан на явлении обобщенной хаотической синхронизации и является наиболее близким к заявляемому способу скрытой передачи информации. Согласно этому способу полезный информационный сигнал кодируется в виде бинарного кода. Один или несколько управляющих параметров передающего хаотического генератора модулируется полезным цифровым сигналом. Полученный таким образом сигнал передается по каналу связи принимающей стороне, содержащей два идентичных хаотических генератора, способных находиться с передающим генератором в режиме обобщенной хаотической синхронизации. Сигналы, снимаемые с выходов генераторов принимающей стороны, подаются на вычитающее устройство и по наличию/отсутствию хаотических колебаний детектируется полезный цифровой сигнал, представленный в виде двоичного кода.

Принципиальным недостатком такого способа скрытой передачи информации является

тот факт, что сигнал, передаваемый по каналу связи, несет на себе следы модуляции управляющего параметра, что может позволить третьей стороне в некоторых случаях декодировать информационное сообщение. Таким образом, известный способ не обеспечивает высокую надежность передачи конфиденциальной информации.

В то же самое время, именно данный способ с перечисленной совокупностью признаков обладает значительной устойчивостью к шумам и флуктуациям в канале связи, что было обнаружено авторами настоящего изобретения при проведении исследований по влиянию шума на эффективность работоспособности различных способов и устройств аналогичного назначения.

Задачей настоящего изобретения является усовершенствование способа скрытой передачи информации с целью повышения его надежности и создания дополнительной секретности.

Поставленная задача решается тем, что в способе скрытой передачи информации, содержащей полезный цифровой сигнал, заключающемся в кодировании полезного сигнала в двоичный код, формировании посредством первого хаотического генератора исходного детерминированного хаотического сигнала путем модуляции параметров хаотического сигнала полезным цифровым сигналом, передаче сформированного таким образом сигнала по каналу связи принимающей стороне, его делении на два идентичных сигнала, воздействии ими на второй и третий хаотические генераторы, идентичные друг другу по управляющим параметрам, выбранные с возможностью обеспечения режима обобщенной синхронизации с первым хаотическим генератором, подаче снятых с выходов указанных второго и третьего генераторов сигналов на вычитающее устройство и определении при наблюдении или отсутствии хаотических колебаний наличия полезного цифрового сигнала, представленного в виде двоичного кода, согласно изобретению сформированный первым генератором детерминированный хаотический сигнал перед передачей по каналу связи суммируют с шумовым сигналом, производимым генератором шума.

Кроме того, первый хаотический генератор и генератор шума настраивают в режим, при котором отношение сигнал/шум SNR удовлетворяет следующему условию: SNR> - 34.6 дБ.

В заявляемом техническом решении шум играет конструктивную роль, в то время как во всех аналогах роль шума является деструктивной. Поэтому положительное влияние шумов было использовано с целью совершенствования способа скрытой передачи информации (Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е. Способ секретной передачи информации // Патент на изобретение №2295835 от 20.03.2007) и улучшения его конфиденциальности.

Технический результат, достигаемый в предлагаемом способе скрытой передачи информации, состоит в том, что шумовой сигнал, производимый генератором шума, обеспечивает отсутствие следов модуляции управляющих параметров, а следовательно, и дополнительную маскировку передаваемого по каналу связи сигнала, тем самым препятствуя третьей стороне декодировать информационное сообщение, что гарантирует конфиденциальность заявляемого способа скрытой передачи информации.

Изобретение поясняется чертежами, где на фиг.1 представлена схема для реализации заявляемого способа скрытой передачи информации; на фиг.2 - представлены графики, характеризующие процесс передачи сигнала: исходный полезный цифровой сигнал (а); сигнал, передаваемый по каналу связи (б); переданный полезный цифровой сигнал, восстановленный в приемнике хаотических автоколебаний (в).

Позициями на фиг.1 обозначены: 1 - полезный бинарный сигнал, 2 - первый (передающий) хаотический генератор, 3 - генератор шума, 4 - сумматор, 5 - канал связи, 6 - второй (принимающий) хаотический генератор, 7 - третий генератор, идентичный второму генератору 6 по управляющим параметрам, 8 - вычитающее устройство, 9 - восстановленный полезный сигнал.

Заявляемый способ скрытой передачи информации основан на явлениях обобщенной хаотической синхронизации (Rulkov N.F., Sushchik M.M., Tsimring L.S., Abarbanel

H.D.I. Generalized synchronization of chaos in directionally coupled chaotic systems // Phys. Rev. E 51, 1995, 980) и синхронизации, индуцированной шумом (Fahy S., Hamman D.R. Transition from chaotic to nonchaotic behavior in randomly driven systems // Phys. Rev. Lett., 69, 1992, 761). Обобщенная синхронизация может наблюдаться в системе двух однонаправлено связанных хаотических генераторов, ведущего и ведомого (что и реализуется в заявляемом способе), и означает, что между их состояниями x(t) (ведущего) и u(t) (ведомого) устанавливается некоторое функциональное соотношение F[.] такое, что u(t)=F[x(t)]. Наиболее простым и легко осуществимым на практике (но при наличии копии ведомого генератора) способом диагностики этого режима является метод вспомогательной системы {Abarbanel H.D.I., Rulkov N.F. and Sushchik M. Generalized synchronization of chaos: The auxiliary system approach // Phys. Rev. E 53, 1996, 4528). В случае индуцированной шумом синхронизации случайный сигнал, действующий на два независимых, но идентичных хаотических генератора, приводит к тому, что их колебания «полностью синхронизуются». По сути дела, эти два типа синхронного поведения обусловлены одной и той же причиной и могут быть рассмотрены как единый тип синхронного поведения связанных хаотических систем (Hramov A.E., Koronovskii A.A., Moskalenko O.I. Are generalized synchronization and noise-induced synchronization identical types of synchronous behavior of chaotic oscillators? // Phys. Lett. A. 354, 2006, 423). Отличие между ними состоит лишь в характере внешнего сигнала, случайный он или детерминированный. Поэтому возможно их совместное использование для скрытой передачи информации.

Способ скрытой передачи информации (фиг.1) заключается в следующем. Полезный информационный сигнал m(t) 1 кодируется в виде бинарного кода. Один или несколько управляющих параметров передающего (первого) хаотического генератора 2 модулируется информационным сигналом таким образом, что характеристики передаваемого сигнала меняются незначительно. Для обеспечения дополнительной маскировки информационного сигнала и изменения характеристик передаваемого сигнала используется генератор шума 3. Сигнал, генерируемый передающей системой, примешивается в сумматоре 4 к шумовому сигналу и далее передается по каналу связи 5. Здесь он также подвергается влиянию шумов и флуктуации, неизбежно присутствующих в реальных устройствах. Принимающее устройство находится на другой стороне канала связи. Оно представляет собой два идентичных хаотических генератора, второй 6 и третий 7, способных находиться в режиме обобщенной синхронизации с передающим 2. Принцип работы принимающего устройства основан на диагностике режима обобщенной синхронизации при помощи метода вспомогательной системы (Abarbanel H.D.I., Rulkov N.F. and Sushchik M. Generalized synchronization of chaos: The auxiliary system approach // Phys. Rev. E 53, 1996, 4528). Сигнал с канала связи поступает на генераторы принимающего устройства. Полученные на выходе сигналы проходят через вычитающее устройство 8, и затем детектируется восстановленный полезный сигнал $\tilde{m}(t)$ 9.

Параметры модуляции управляющих параметров передающего (первого) генератора должны быть выбраны таким образом, чтобы в зависимости от передаваемого бинарного бита 0/1 между передающим и принимающими генераторами в отсутствие шумов и флуктуации существовал/отсутствовал режим обобщенной хаотической синхронизации. Тогда после прохождения через вычитающее устройство будет детектироваться восстановленный полезный сигнал, представляющий собой чередующуюся последовательность участков с несинхронным (бинарный бит 1) и синхронным поведением (бинарный бит 0).

В качестве примера конкретной реализации заявляемого способа скрытой передачи информации можно привести численное моделирование однонаправлено связанных систем Ресслера, выбранных в качестве передающего и принимающего генераторов. Принципиальная схема генератора Ресслера приведена в работе (Rico-Martinez R., Kreischer K.E., Flatgen G., Anderson J.S., Kevrekidis I.G. Adaptive Detection of Instabilities: An Experimental Feasibility Study // Physica D. 176, 2003, 1).

Передающий генератор описывается следующей системой дифференциальных уравнений:

$$\dot{x}_1 = -\omega_x x_2 - x_3, \qquad (1)$$

$$\dot{x}_2 = \omega_x x_1 + a x_2,$$

$$\dot{x}_3 = p + x_3(x_1 - c),$$

где $x(t)=(x_1,x_2,x_3)$ - вектор состояния передающего генератора, характеризующий колебания напряжений, снимаемых в различных участках цепи, a=0.15, p=0.2 и c=10- управляющие параметры (представляющие собой композицию параметров самой системы), ω_x - управляющий параметр, характеризующий собственную частоту колебаний системы.

Величина параметра ω_x модулируется полезным цифровым сигналом следующим образом. Если в заданный интервал времени передается бинарный бит 1, тогда ω_x=0.95 на протяжении всего этого интервала. При передаче бинарного бита 0 ω_x=1 (Hramov A.E., Koronovskii A.A., Moskalenko O.I. Generalized synchronization onset // Europhysics Letters. 72 (6), 2005, 901).

Принимающее устройство содержит два идентичных хаотических генератора, второй и третий, каждый из которых описывается следующей системой уравнений:

$$\dot{u}_1 = -\omega_u u_2 - u_3 + \varepsilon(s(t) - u_1), \qquad (2)$$

$$\dot{u}_2 = \omega_u u_1 + a u_2,$$

$$\dot{u}_3 = p + u_3(u_1 - c),$$

Здесь $u(t)=(u_1,u_2,u_3)$ - вектор состояния второго генератора. Пусть $v(t)=(\nu_1,\nu_2,\nu_3)$, также удовлетворяющий (2), будет вектором состояния третьего генератора (см. фиг.1). Управляющие параметры a, p и c выберем идентичными последним для принимающего генератора. Управляющий параметр ω_u, характеризующий собственную частоту принимающих генераторов, выберем равным ω_u=0.95 на протяжении всего времени передачи сигнала.

Сигнал, генерируемый передающим устройством, суммируется с сигналом, производимым генератором шума, и далее передается по каналу связи. В рассматриваемой модели это реализуется путем связи принимающих генераторов с передающим, т.е. добавлением компоненты $\varepsilon(s(t)-u_1)$ в первое уравнение системы (2). Здесь $s(t)=x_1+D\xi$ - это так называемый сигнал в канале связи. Слагаемое $D\xi$ моделирует шумы и флуктуации, производимые генератором шума. ξ - δ-кореллированный белый шум, характеризующийся следующим распределением вероятности:

$$p(\xi) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(\xi - \xi_0)^2}{2\sigma^2}\right), \qquad (3)$$

где ξ_0=0 и σ=1 - среднее и дисперсия. Важно отметить, что характер распределения случайной величины ξ не имеет особого значения, и подобные результаты могут наблюдаться для других типов распределения вероятности $p(\xi)$, например для равномерного. Параметр D определяет суммарную интенсивность добавляемого шума.

Сила связи между передающим и принимающим генераторами характеризуется параметром ε. Он был выбран равным ε=0.14. В этом случае, известно, что в отсутствие шумов и флуктуации (D=0) режим обобщенной синхронизации в системе (1)-(2) имеет место при ω_x=1, в то время как для ω_x=0.95 обобщенная синхронизация не наблюдается (более подробно см. (Hramov A.E., Koronovskii A.A., Moskalenko O.I. Generalized synchronization onset // Europhysics Letters. 72 (6), 2005, 901)).

Вычитающее устройство выполняет операцию $(u_1-\nu_1)^2$. Тогда после прохождения через него согласно методу вспомогательной системы должно наблюдаться отсутствие колебаний для ω_x=1 и наличие хаотических колебаний для ω_x=0.95. Восстановленный сигнал $\tilde{m}(t)$ будет представлять собой последовательность областей с различными типами поведения.

В демонстративных целях в качестве информационного сигнала m(t) выберем простую последовательность бинарных битов 0/1, представленную на фиг.2(а). Для интегрирования стохастического уравнения (2) будем использовать метод Эйлера с шагом дискретизации по времени h=0.0001.

Выберем интенсивность шума достаточно большой, например D=10, и покажем, как работает заявляемый способ скрытой передачи информации в этом случае. На фиг.2(б) приведен фрагмент сигнала s(t), передаваемого по каналу связи. Видно, что изменение управляющего параметра ω_x сильно не меняет характеристики передаваемого сигнала. Более того, шум большой амплитуды еще более искажает передаваемый сигнал, не оставляя никакой возможности третьей стороне декодировать информационное сообщение без полной информации о характеристиках принимающих генераторов. Фиг.2(в) иллюстрирует восстановленный сигнал $\tilde{m}(t) = (u_1 - v_1)^2$. Нетрудно видеть, что при помощи пропускания через фильтр нижних частот и выбора пороговых значений полезный цифровой сигнал может быть легко детектирован.

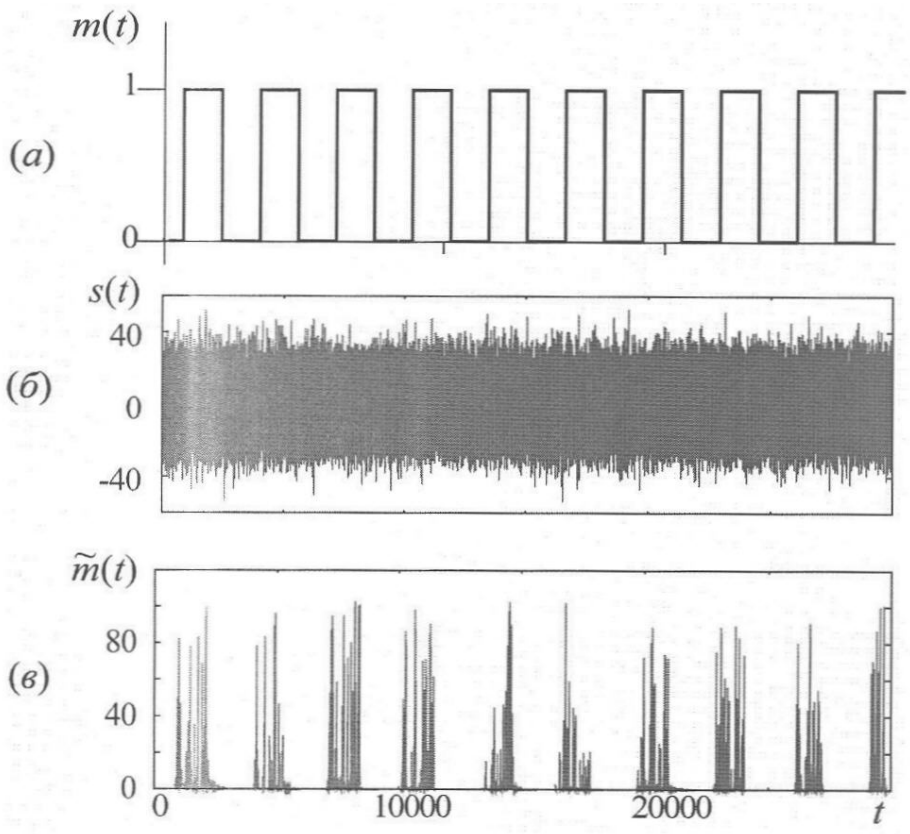
Следует отметить, что аналогичные результаты наблюдаются для различных значений интенсивности шума вплоть до D=400. В этом случае отношение сигнал/шум составляет -34.6 дБ, что свидетельствует о значительной устойчивости заявляемого способа к шумам и флуктуациям и о конструктивной роли шума для передачи информации.

Таким образом, положительным эффектом заявляемого способа скрытой передачи информации является обеспечение дополнительной маскировки передаваемого по каналу связи сигнала и, следовательно, гарантия высокой степени конфиденциальности.

Формула изобретения

1. Способ скрытой передачи информации, содержащей полезный цифровой сигнал, заключающийся в том, что полезный сигнал кодируют в двоичный код, формируют посредством первого хаотического генератора исходный детерминированный хаотический сигнал путем модуляции параметров хаотического сигнала полезным цифровым сигналом, передают сформированный таким образом сигнал по каналу связи принимающей стороне, где его делят на два идентичных сигнала, которыми воздействуют на второй и третий хаотические генераторы, идентичные друг другу по управляющим параметрам, выбранные с возможностью обеспечения режима обобщенной синхронизации с первым хаотическим генератором, снятые с выходов указанных второго и третьего генераторов сигналы подают на вычитающее устройство и при наблюдении или отсутствии хаотических колебаний определяют наличие полезного цифрового сигнала, представленного в виде двоичного кода, отличающийся тем, что сформированный первым хаотическим генератором детерминированный хаотический сигнал перед передачей по каналу связи суммируют с шумовым сигналом, производимым генератором шума.

2. Способ по п.1, отличающийся тем, что первый хаотический генератор и генератор шума настраивают в режим, при котором отношение сигнал/шум SNR удовлетворяет следующему условию: SNR>34,6 дБ.



Фиг. 2