РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2421923

СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ С ИЗМЕНЯЮЩИМИСЯ ХАРАКТЕРИСТИКАМИ ГЕНЕРАТОРА ШУМА

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

Автор(ы): ***см. на обороте***

Заявка № **2010104117**

Приоритет изобретения **10 февраля 2010 г.**

Зарегистрировано в Государственном реестре изобретений Российской Федерации ***20 июня 2011 г.***

Срок действия патента истекает **10 февраля 2030 г.**

Руководитель Федеральной службы по интеллектуальной собственности, патентам и товарным знакам

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 421 923** (13) **C1**

(51) МПК
H04L 9/22 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2010104117/09, 10.02.2010**

(24) Дата начала отсчета срока действия патента:
10.02.2010

Приоритет(ы):
(22) Дата подачи заявки: **10.02.2010**

(45) Опубликовано: **20.06.2011** Бюл. № **17**

(56) Список документов, цитированных в отчете о поиске: **RU 2349044 C1, 10.03.2009. RU 2295835 C1, 20.03.2007. RU 2232475 C1, 10.07.2004. US 5432814 A, 11.07.1995. US 4475208, 02.10.1984.**

Адрес для переписки:
410012, г.Саратов, ул. Московская, 155, СГУ, ЦПУ, Н.В. Романовой

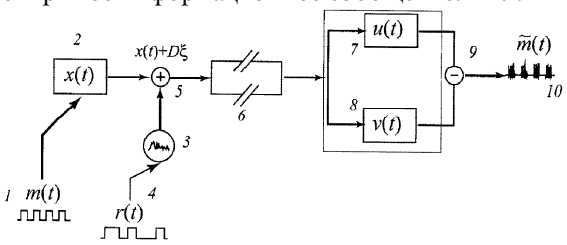
(72) Автор(ы):
Москаленко Ольга Игоревна (RU),
Короновский Алексей Александрович (RU),
Храмов Александр Евгеньевич (RU)

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

(54) СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ С ИЗМЕНЯЮЩИМИСЯ ХАРАКТЕРИСТИКАМИ ГЕНЕРАТОРА ШУМА

(57) Реферат:

Изобретение относится к радиотехнике и может найти применение в системах связи для помехоустойчивой передачи цифровой информации с высокой степенью конфиденциальности. Достигаемый технический результат - повышение надежности и расширение пропускной способности канала связи. Способ характеризуется тем, что кодируют полезный сигнал в двоичный код, формируют исходный детерминированный хаотический сигнал путем модуляции параметров хаотического сигнала полезным цифровым сигналом, суммируют сформированный таким образом сигнал с шумовым сигналом, производимым генератором шума, передают полученный сигнал по каналу связи принимающей стороне, где его делят на два идентичных сигнала, воздействуют ими на второй и третий хаотические генераторы, сигналы с которых подают на вычитающее устройство, при этом характеристики генератора шума модулируют цифровым или аналоговым сигналом, содержащим ложное, несущественное или открытое информационное сообщение. 2 ил.



Фиг. 1

RU 2421923 C1

RU 2421923 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 421 923** (13) **C1**

(51) Int. Cl.
H04L 9/22 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2010104117/09, 10.02.2010**

(24) Effective date for property rights:
10.02.2010

Priority:
(22) Date of filing: **10.02.2010**

(45) Date of publication: **20.06.2011 Bull. 17**

Mail address:
410012, g.Saratov, ul. Moskovskaja, 155, SGU, TsPU, N.V. Romanovoj

(72) Inventor(s):
Moskalenko Ol'ga Igorevna (RU),
Koronovskij Aleksej Aleksandrovich (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 TRANSFER OF INFORMATION WITH VARIABLE CHARACTERISTICS OF NOISE GENERATOR

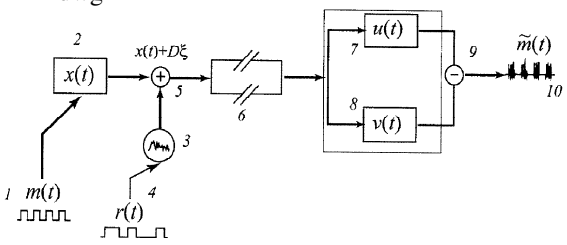
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: useful signal is coded into a binary code, an initial determinate chaotic signal is formed by modulation of the chaotic signal parameters with the useful digital signal, the signal generated in this manner is summed with a noise signal produced by the noise generator, the received signal is sent along the communication channel to a receiving side, where it is divided into two identical signals, they are used to act at the second and third chaotic generators, signals from which are sent to a subtracting device. At the same time the noise generator characteristics are modulated with a digital or analogue signal, containing a false, irrelevant or open information message.

EFFECT: increased reliability and expansion of communication channel throughput capacity.

2 dwg



Фиг. 1

RU 2421923 C1

RU 2421923 C1

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

В настоящее время известны способы скрытой передачи информации на основе полной хаотической синхронизации (см. патент US №5291555, МПК H04K 1/02; H04L 9/28; патент РФ №2295835, МПК H04L 9/12, H04K 1/02; статьи 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; 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; Yang T., Chua L.O. Secure communication via chaotic parameter modulation // IEEE Trans. on Circ. Sys., I.43, 1996, 817), фазовой синхронизации (Chen J.Y., Wong K.W., Cheng L.M., Shuai J.W. A secure communication scheme based on the phase synchronization of chaotic systems // Chaos. 13, 2003, 508), обобщенной синхронизации (Terry J.R., VanWiggeren G.D. Chaotic communication using generalized synchronization // Chaos, Solitons and Fractals. 12, 2001, 145), а также использующие несколько типов синхронного поведения совместно (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 указанных выше способов, схем и устройств являются, в первую очередь, их низкая конфиденциальность, нестабильность работы при неидентичности параметров передающего и принимающего генераторов, деструктивное влияние шумов на качество передачи информации, трудности технической реализации.

Известен способ скрытой передачи информации (см. патент РФ №2349044, МПК H04L 9/00). Способ основан на режиме обобщенной синхронизации в присутствии шума 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 информационным сигналом таким образом, что характеристики передаваемого сигнала меняются незначительно, но при этом остается возможность возникновения/разрушения режима обобщенной синхронизации в зависимости от передаваемого бинарного бита. Для обеспечения дополнительной маскировки информационного сигнала и изменения характеристик передаваемого сигнала используется генератор шума. Сигнал, генерируемый передающей системой, примешивается в сумматоре к шумовому сигналу и далее передается по каналу связи. Здесь он также подвергается влиянию шумов, неизбежно присутствующих в реальных устройствах. Принимающее устройство находится на другой стороне канала связи. Оно представляет собой два идентичных хаотических генератора, способных находиться в режиме обобщенной синхронизации с передающим генератором. Сигнал с канала связи поступает на генераторы принимающего устройства. Полученные на выходе сигналы проходят через вычитающее устройство, и затем детектируется восстановленный полезный сигнал, представленный в виде бинарного кода.

Принципиальным недостатком такого способа скрытой передачи информации является возможность одновременной передачи только одного сообщения по каналу связи. Кроме того, сигнал, передаваемый по каналу связи этим способом, не несет на

себе явных следов наличия информации, что потенциально может заставить третью сторону задуматься о том, что полезная информация скрыта в ней, и применять различные статистические тесты для ее дешифрации. Несмотря на то, что сигнал, передаваемый по каналу связи, по своим характеристикам практически не отличается от стохастического, существует вероятность того, что применение того или иного метода дешифрации все-таки позволит декодировать исходное информационное сообщение. Таким образом, этот способ является недостаточно надежным при передаче конфиденциальной информации.

В то же самое время, изменение характеристик шума, его амплитуды, среднего и дисперсии практически не влияет на эффективность именно этого способа скрытой передачи информации, что было обнаружено авторами настоящего изобретения при исследовании влияния характеристик шумового сигнала на работоспособность различных способов скрытой передачи информации. Выявленная особенность позволяет модулировать характеристики сигнала, производимого генератором шума, информационным сигналом, содержащим ложную, несущественную или открытую информацию, в течение всего времени передачи сигнала, тем самым, наталкивая третью сторону на дешифрацию ложного, несущественного или открытого сообщения. В этом случае сигнал, передаваемый по каналу связи, будет нести на себе следы амплитудной модуляции, что позволит третьей стороне без труда дешифровать соответствующее сообщение без последующего применения статистических методов анализа сигнала, передаваемого по каналу связи. В то же самое время, на принимающей стороне канала связи следы модуляции не будут влиять на дешифрацию скрытого сообщения, что позволяет говорить о повышении степени конфиденциальности передачи информации заявляемым способом. Кроме того, заявляемый способ позволяет расширить пропускную способность канала связи, то есть позволить передавать сразу два информационных сообщения, содержащих полезную и ложную информацию, соответственно. Передача второго сообщения может интерпретироваться как нескрытая передача информационного сообщения по каналу связи.

Задачей настоящего изобретения является усовершенствование способа скрытой передачи информации с целью повышения его надежности и расширения пропускной способности канала связи.

Технический результат, достигаемый в заявляемом способе, состоит в том, что характеристики шумового сигнала, производимого генератором шума, модулируются информационным сигналом, содержащим ложное (открытое) сообщение, что обеспечивает не только скрытие следов модуляции управляющих параметров цифровым сигналом, содержащим полезную информацию, но и наталкивает третью сторону на дешифрацию ложного сообщения, а следовательно, гарантирует конфиденциальность предлагаемого способа скрытой передачи информации. В случае передачи открытого сообщения заявляемый способ расширяет пропускную способность канала связи, позволяя одновременно передавать скрытое и открытое сообщение.

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, суммировании сформированного таким образом сигнала с шумовым сигналом, производимым

генератором шума, передаче полученного 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 решению характеристики генератора шума модулируют цифровым или аналоговым сигналом, содержащим ложное, несущественное или открытое информационное сообщение.

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 (е),

где

1 - полезный бинарный сигнал m(t);

2 - первый (передающий) хаотический генератор;

3 - генератор шума;

4 - информационный сигнал r(t), содержащий ложную информацию;

5 - сумматор;

6 - канал связи;

7 - второй (принимающий) хаотический генератор;

8 - третий генератор, идентичный второму генератору 7 по управляющим параметрам;

9 - вычитающее устройство;

10 - восстановленный полезный сигнал $\tilde{m}(t)$.

Заявляемый способ скрытой передачи информации основан на явлении 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) в присутствии шума. В способе активно используется 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), являющийся одним из наиболее эффективных методов диагностики режима обобщенной синхронизации, в том числе и при наличии внешних шумов.

Способ скрытой передачи информации (фиг.1) заключается в следующем. Полезный сигнал m(t) 1 кодируется в виде бинарного кода. Один или несколько управляющих параметров передающего (первого) хаотического генератора 2 модулируется информационным сигналом таким образом, чтобы характеристики передаваемого сигнала менялись незначительно, но при этом оставалась возможность возникновения/разрушения режима обобщенной синхронизации в зависимости от передаваемого бинарного бита. Для реализации этой особенности граница возникновения режима обобщенной синхронизации на плоскости параметров «параметр модуляции - интенсивность связи» должна обладать некоторой особенностью: при малом изменении управляющего параметра порог возникновения синхронного режима должен меняться достаточно резко. Для обеспечения дополнительной маскировки информационного сигнала и изменения характеристик

передаваемого сигнала используется генератор шума 3. Характеристики генератора шума 3 модулируются информационным аналоговым или цифровым сигналом r(t) 4, содержащим ложную информацию. Например, при передаче бинарного бита 0 генератор шума 3 производит стохастический сигнал, подчиняющийся равномерному распределению плотности вероятности, при передаче бинарного бита 1-δ-коррелированный гауссов шум с нулевым средним. Сигнал, генерируемый передающей системой, примешивается в сумматоре 5 к шумовому сигналу и далее передается по каналу связи 6, где он подвергается влиянию шумов и искажений, неизбежно присутствующих в реальных устройствах. Принимающее устройство находится на другой стороне канала связи 6. Оно представляет собой два идентичных хаотических генератора, второй 7 и третий 8, способных находиться в режиме обобщенной синхронизации с передающим 2. Принцип работы принимающего устройства основан на диагностике режима обобщенной синхронизации при помощи метода вспомогательной системы. Сигнал с канала связи 6 поступает на генераторы принимающего устройства 7, 8. Полученные на выходе сигналы проходят через вычитающее устройство 9, и затем детектируется восстановленный полезный сигнал $\tilde{m}(t)$ 10, представляющий собой чередующуюся последовательность участков с несинхронным и синхронным поведением, по которой исходный информационный сигнал может быть легко детектирован.

В качестве примера конкретной реализации заявляемого способа можно привести численное моделирование однонаправлено связанных систем Ресслера, выбранных в качестве генераторов передающего и принимающего устройств. 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:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3, \\ \dot{x}_2 &= \omega_x x_1 + a x_2, \\ \dot{x}_3 &= p + x_3(x_1 - c), \end{aligned} \qquad (1)$$

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 $\omega_x=0.91$ на протяжении всего этого интервала. При передаче бинарного бита 0 параметр ω_x принимает случайное значение из диапазона $\omega_x \in [0.9, 0.91)$ (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:

$$\begin{aligned} \dot{u}_1 &= -\omega_u u_2 - u_3 + \varepsilon(s(t) - u_1), \\ \dot{u}_2 &= \omega_u u_1 + a u_2, \\ \dot{u}_3 &= p + u_3(u_1 - c). \end{aligned} \qquad (2)$$

Здесь $u(t)=(u_1, u_2, u_3)$ - вектор состояния второго генератора. Пусть $v(t)=(v_1, v_2, v_3)$, также удовлетворяющий (2), будет вектором состояния третьего генератора (см. фиг.1). Управляющие параметры a, p и c выберем идентичными последним для передающего генератора. Управляющий параметр ω_u, характеризующий собственную частоту принимающих генераторов, выберем равным $\omega_u=0.95$ на протяжении всего времени передачи сигнала.

Сигнал, генерируемый передающим устройством 2, суммируется с сигналом, производимым генератором шума 3, и далее передается по каналу связи 6. В рассматриваемой модели это реализуется путем связи принимающих генераторов 7, 8 с передающим 2, 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, производимые генератором шума. Характеристики шумового сигнала $\xi(t)$ модулируются информационным сигналом r(t), содержащим ложную, несущественную или открытую информацию: если передается бинарный бит 0, стохастический сигнал подчиняется равномерному распределению плотности вероятности, если передается бинарный бит 1 - гауссову распределению с нулевым средним. Параметр D определяет суммарную интенсивность добавляемого шума. Следует отметить, что возможно обеспечение амплитудной модуляции не только путем изменения характера распределения случайной величины, но и путем варьирования параметра D, например, D=10, если передается бинарный бит 1, D=5, если передается бинарный бит 0, и т.п. Более того, возможна модуляция амплитуды шумового сигнала аналоговым сигналом.

Сила связи между передающим 2 и принимающим 7, 8 генераторами характеризуется параметром ε. Он был выбран равным $\varepsilon=0.14$. В этом случае, известно, что как в отсутствие, так и при наличии шумов, режим обобщенной синхронизации в системе (1)-(2) имеет место при $\omega_x\in[0.9; 0.91)$, в то время как для $\omega_x=0.91$ 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; Moskalenko O.I., Hramov A.E., Koronovskii A.A., Ovchinnikov A.A. Effect of noise on generalized synchronization: theory and experiment // Phys. Rev. E. 2009, submitted)).

Вычитающее устройство выполняет операцию $(u_1-v_1)^2$. Тогда после прохождения через него, согласно методу вспомогательной системы, должно наблюдаться отсутствие колебаний для $\omega\in[0.9; 0.91)$ и наличие хаотических колебаний для $\omega_x=0.91$. Восстановленный сигнал $\tilde{m}(t)$ 10 будет представлять собой последовательность областей с различными типами поведения.

В качестве полезного сигнала m(t) выберем последовательность бинарных битов 0/1, представленную на фиг.2 (а). Для интегрирования стохастического уравнения (2) будем использовать метод Рунге-Кутта 4 порядка, адаптированный для решения стохастических дифференциальных уравнений (Никитин Н.Н., Первачев С.В., Разевиг В.Д. О решении на ЦВМ стохастических дифференциальных уравнений следящих систем // Автоматика и телемеханика. 41975133), с шагом дискретизации по времени h=0.001.

Выберем интенсивность шума достаточно большой, например, D=10 и покажем, как работает заявляемый способ скрытой передачи информации в этом случае. Характеристики генератора шума будем модулировать простой последовательностью бинарных битов 0/1. Следует отметить, что возможно модулирование характеристик стохастического сигнала и более сложным информационным сообщением (как цифровым, так и аналоговым). На фиг.2(б) приведен фрагмент сигнала s(t),

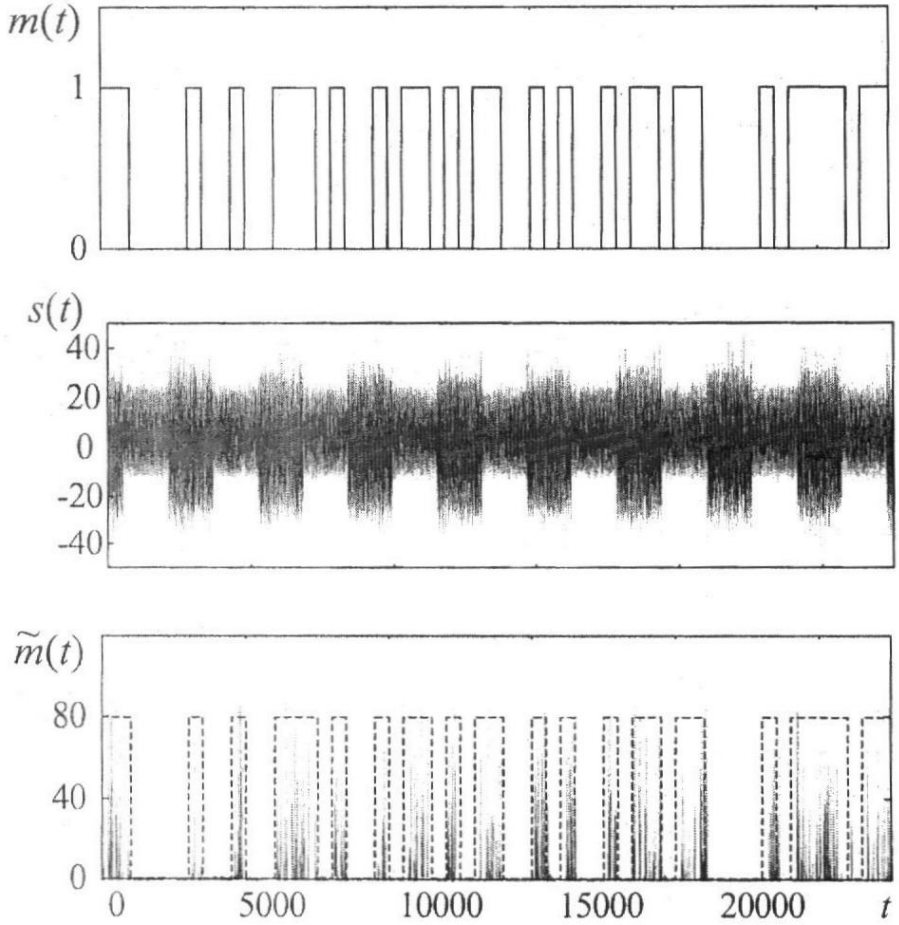
передаваемого по каналу связи 6. Нетрудно заметить наличие следов амплитудной модуляции в сигнале s(t), по наличию которых третья сторона без труда дешифрует ложное, несущественное или открытое сообщение r(t). В то же самое время, в сигнале s(t) не видно ни следов модуляции управляющего параметра ω_x полезным сигналом m(t), ни каких-либо других признаков наличия исходного скрытого информационного сообщения. Фиг.2 (в) иллюстрирует восстановленный сигнал $\tilde{m}(t) = (u_1 - v_1)^2$ 10. Нетрудно видеть, что при помощи пропускания через фильтр нижних частот и выбора пороговых значений полезный цифровой сигнал может быть легко детектирован, также как и в случае скрытия следов модуляции управляющего параметра стохастическим сигналом с постоянными характеристиками или при отсутствии такового вовсе.

Следует отметить, что аналогичные результаты наблюдаются при дальнейшем увеличении интенсивности шума D и при изменении характера распределения случайной величины. Способ становится неработоспособным, если отношение энергии на бит к спектральной плотности мощности шума E_b/N_0=-10.01 дБ, что еще раз подтверждает конструктивную роль шума при передаче информации заявляемым способом.

Таким образом, положительным эффектом заявляемого способа скрытой передачи информации является обеспечение дополнительной маскировки передаваемого по каналу связи сигнала путем модуляции характеристик генератора шума информационным сообщением, содержащим ложную, несущественную или открытую информацию, наталкивание третьей стороны на дешифрацию этого сообщения и, следовательно, гарантия высокой степени конфиденциальности передачи информации.

Формула изобретения

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, суммируют сформированный таким образом сигнал с шумовым сигналом, производимым генератором шума, и передают полученный 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 характеристики генератора шума модулируют цифровым или аналоговым сигналом, содержащим ложное, несущественное или открытое информационное сообщение.



Фиг. 2