РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 295 835** (13) **C1**

(51) МПК
H04L 9/12 (2006.01)
H04K 1/02 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005133906/09, 03.11.2005**

(24) Дата начала отсчета срока действия патента:
03.11.2005

(45) Опубликовано: **20.03.2007 Бюл. № 8**

(56) Список документов, цитированных в отчете о поиске: **US 5291555 A1, 01.03.1994. RU 2185032 C1, 10.07.2002. US 6049614 A1, 11.04.2000. US 5930364 A1, 27.07.1999. US 6744893 A1, 01.06.2004. WO 0113518 A1, 22.02.2001. WO 0165755 A1, 07.09.2001. EP 0872975 A1, 21.10.1998. US 5857165 A1, 05.01.1999. US 5379346 A1, 03.01.1995.**

Адрес для переписки:
410012, г.Саратов, ул. Московская, 155, СГУ, ПЛО, О.И. Куприяновой

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

(73) Патентообладатель(и):
ГОУ ВПО "Саратовский государственный университет им. Н.Г. Чернышевского" (RU)

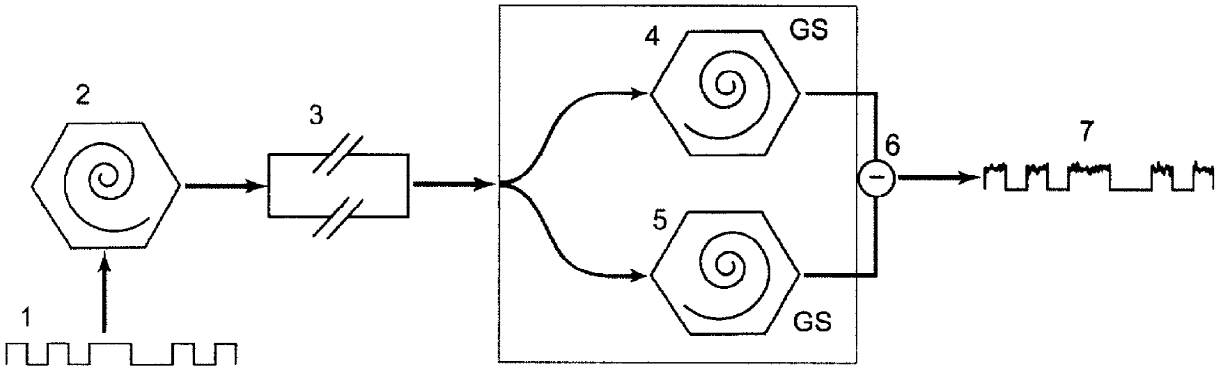
(54) СПОСОБ СЕКРЕТНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

(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. Техническим результатом является повышение надежности способа секретной передачи информации при упрощении его реализации с использованием детерминированных хаотических сигналов, достигаемый тем, что осуществляют формирование исходного хаотического детерминированного сигнала первым генератором хаоса, передачу по каналам связи, прием и разделение на два идентичных сигнала, при этом первым сигналом воздействуют на второй генератор с возможностью получения сигнала, синхронизованного с исходным, из которого вычитают второй сигнал, получая полезный цифровой сигнал, а формирование сигнала осуществляют путем модуляции параметров хаотического сигнала полезным, а вторым идентичным сигналом воздействуют на третий генератор, идентичный второму по управляющим параметрам, при этом первый и второй генераторы выбирают с возможностью обеспечения режима обобщенной хаотической синхронизации. 6 ил.

RU 2295835 C1

RU 2295835 C1



Фиг. 1

RU 2295835 C1

RU 2295835 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 295 835** (13) **C1**

(51) Int. Cl.
H04L 9/12 (2006.01)
H04K 1/02 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005133906/09, 03.11.2005**

(24) Effective date for property rights: **03.11.2005**

(45) Date of publication: **20.03.2007 Bull. 8**

Mail address:
410012, g.Saratov, ul. Moskovskaja, 155, SGU, PLO, O.I. Kuprijanovoj

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

(73) Proprietor(s):
GOU VPO "Saratovskij gosudarstvennyj universitet im. N.G. Chernyshevskogo" (RU)

(54) METHOD FOR SECRET TRANSFER OF INFORMATION

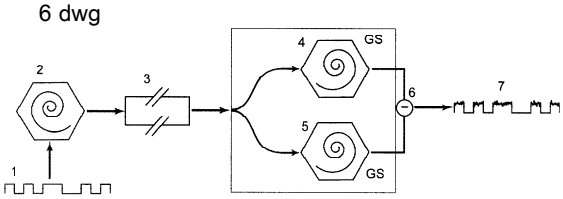
(57) Abstract:

FIELD: radio engineering, information transfer technologies, possible use in communication systems for interference-resistant transmission of digital information with certain degree of confidentiality.

SUBSTANCE: in accordance to method, original chaotic determined signal is generated by first chaos generator, transferred via communication channels, received and divided onto two identical signals, while first signal affects second generator with possible production of signal, synchronized to original signal, subtracted from which is second signal, producing useful digital signal, and generation of signal is realized by modulating parameters of chaotic signal by useful one, and second identical signal affects third generator, identical to second one in terms of control parameters, while first and second generators are picked with possible setup of generalized chaotic synchronization mode.

EFFECT: increased reliability of method for secret transfer of information while simplifying its realization with usage of determined chaotic signals.

6 dwg



Фиг. 1

RU 2295835 C1

RU 2295835 C1

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

Известны способы секретной передачи информации, основанные на использовании явления хаотической синхронизации и синхронного отклика генераторов хаоса (Cuomo K., Oppenheim A. Communication using synchronized chaotic systems // US Patent No. 5291555 от 1.03.1994; Abarbanel H., Rulkov N., Tsimring L., Rabinovich M. Chaotic communication apparatus and method for use with a wired or wireless transmission link // US Patent No. 5923760 от 13.07.1999; Kim C. Synchronized chaotic system and communication system using synchronized chaotic system // US Patent No. 6,049,614 от 11.04.2000; Carroll T.L., Johnson G. Synchronizing autonomous chaotic systems using filters // US Patent No. 6370248 от 9.04.2002). Также различные способы передачи данных с использованием хаотической синхронизации можно найти в работах Parlitz U., Chua L.O., Kocarev Lj., Halle K.S., Shang A. Transmission of digital signal by chaotic synchronization // Int. J. Bifurcation and Chaos. 1992. Vol.2. №4. P.973-977; Hayes S., Grebogy C., Ott E. Communication with chaos // Phys. Rev. Lett. 1993. Vol.70, №20. P.3031-3034; Kocarev L., Halle K.S., Eckert K., Chua L., Parlitz U. Experimental demonstration of secure communications via chaotic synchronization // Int. J. Bifurcation and Chaos. 1992. Vol.2, №3. P.709-713; Cuomo M.K., Oppenheim A.V., Strogatz S.H. Synchronization of Lorenz-based chaotic circuits with application to communications // IEEE Trans. Circuits and Syst., 1993. Vol.40. №10. P.626; Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. М.: Физматлит, 2002.

В предложенных ранее способах секретной передачи информации с помощью хаотической синхронизации используется явление полной хаотической синхронизации между генераторами хаоса на передающей и принимающей сторонах канала связи, соответственно. В этом случае на передающем конце полезный сигнал примешивается в сумматоре к несущему хаотическому сигналу и далее передается по каналу связи. В приемнике осуществляется полная хаотическая синхронизация находящегося в нем генератора хаоса с помощью принимаемого сигнала, в результате чего динамика принимающего генератора становится идентичной передающему генератору. Детектированный сигнал получается после прохождения вычитающего устройства как разность между принимаемым сигналом и синхронным откликом генератора хаоса в приемнике.

За счет сильной ляпуновской неустойчивости фазовых траекторий в передающем генераторе хаоса имеет место зависимость колебаний генератора от начальных условий и несущий сигнал никогда заранее не определен, что делает невозможным перехват и дешифровку сообщения при отсутствии копии принимающего генератора. Последнее обеспечивает конфиденциальность передачи данных с использованием вышеназванного способа, основанного на полной хаотической синхронизации. Также устройство, реализующее хаотический синхронный отклик, обладает свойством нелинейного фильтра, позволяющего распознавать сигналы данного источника хаоса среди сигналов, порождаемых другими источниками. Последнее дает возможность увеличить пропускную способность канала связи за счет одновременной передачи целого ряда сообщений (мультиплексирование).

Таким образом, явление полной хаотической синхронизации и синхронного отклика часто используется при разработке систем связи с хаотическими носителями информации. Однако в известных схемах передачи хаоса, основанных на использовании полной хаотической синхронизации или синхронного отклика генераторов хаоса в передатчике и приемнике, возникает целый ряд существенных трудностей при практической реализации. Во-первых, принципиальным требованием известных способов передачи данных является необходимость обеспечения высокой степени идентичности генераторов хаоса, используемых в передающем и принимающем устройствах, реализация чего

представляется весьма серьезной технической проблемой, особенно в течение длительного времени эксплуатации устройств. Во-вторых, на качество передачи информации с помощью вышеуказанных схем сильное влияние оказывают искажения и шумы различных типов в канале связи. Если интенсивность шума и искажений передаваемого сигнала превышает некоторый порог (который сравним с естественными шумами и искажениями), то система передачи данных на основе полной хаотической синхронизации оказывается неработоспособной.

Наиболее близким к заявляемому способу является способ секретной передачи информации (Cuomo K., Oppenheim A. Communication using synchronized chaotic systems // US Patent No. 5291555 от 1.03.1994), где передача информации происходит за счет осуществления полной хаотической синхронизации между передатчиком и приемником. Полная хаотическая синхронизация означает точное совпадение сигналов, производимых связанными генераторами хаотических автоколебаний, и возможна лишь в случае их идентичности. В способе используется несущий сигнал, обладающий характеристиками сигнала с широким спектром, и, следовательно, являющийся очень сложным и непредсказуемым. Спектр мощности такого сигнала является почти однородным в полосе рабочих частот канала связи и, по сути, аналогичен шуму низкой амплитуды. Полезный цифровой сигнал моделирует один из управляющих параметров передающего генератора хаоса. Сформированный таким образом сигнал передается по каналу связи, в приемнике делится на два идентичных сигнала. Один из них действует на принимающий генератор хаоса, восстанавливающий исходный передаваемый сигнал. Второй сигнал проходит без изменения. Оба сигнала попадают на демодулятор, играющий роль вычитающего устройства. За счет осуществления полной хаотической синхронизации на принимающем генераторе на выходе демодулятора формируется полезный сигнал.

В данном способе также используется явление полной хаотической синхронизации для выделения полезного сигнала из несущего, что требует высокой степени идентичности генераторов хаоса на обеих сторонах канала связи, реализация чего является серьезной технической проблемой. Также подобная схема в большой степени подвержена влиянию искажений и шумов различных типов. При превышении интенсивностью шума и искажений передаваемого сигнала некоторого порога (который сравним с естественными шумами и искажениями) система передачи данных на основе полной хаотической синхронизации оказывается неработоспособной. Поэтому данный способ секретной передачи информации в реальных условиях оказывается плохо применимым.

Задачей изобретения является повышение надежности способа секретной передачи информации при упрощении его реализации с использованием детерминированных хаотических сигналов.

Поставленная задача решается тем, что в способе секретной передачи информации, содержащей полезный цифровой сигнал, включающем формирование исходного хаотического детерминированного сигнала первым генератором хаоса, передачу по каналам связи, прием и разделение на два идентичных сигнала, при этом первым сигналом воздействуют на второй генератор с возможностью получения сигнала, синхронизованного с исходным, из которого вычитают второй сигнал, получая полезный цифровой сигнал, согласно изобретению формирование сигнала осуществляют путем модуляции параметров хаотического сигнала полезным, а вторым идентичным сигналом воздействуют на третий генератор, идентичный второму по управляющим параметрам, при этом первый и второй генераторы выбирают с возможностью обеспечения режима обобщенной хаотической синхронизации.

Поставленная задача достигается за счет использования в способе явления обобщенной хаотической синхронизации, не требующего идентичности генераторов хаоса в передающих и принимающих устройствах, а также имеющего более низкую чувствительность к помехам и искажениям сигнала в канале связи.

Изобретение поясняется чертежами, где на фиг.1 представлена схема реализации способа скрытой передачи информации при помощи обобщенной хаотической

синхронизации; на фиг.2 - исходный полезный цифровой сигнал; фиг.3 - фазовый портрет и спектр сигнала, снимаемого с передающего генератора хаоса; фиг.4 - фазовый портрет и спектр сигнала, снимаемого с первого принимающего генератора хаоса; фиг.5 - фазовый портрет и спектр сигнала, снимаемого со второго принимающего генератора хаоса; фиг.6 - переданный полезный цифровой сигнал, восстановленный в приемнике хаотических автоколебаний.

Позициями на фиг.1 обозначены: 1 - полезный сигнал, 2 - передающий генератор хаоса, 3 - канал связи, 4 - принимающий генератор хаоса, 5 - третий генератор, идентичный принимающему генератору 4 по управляющим параметрам, 6 - вычитающее устройство, 7 - дешифрованный передаваемый сигнал.

Заявляемый способ секретной передачи информации основан на использовании режима обобщенной синхронизации хаотических осцилляторов (см. Фиг.1). Данный тип синхронного поведения вводится для однонаправленно связанных хаотических генераторов (что и реализуется в нашем случае). Наличие режима обобщенной синхронизации означает, что между состояниями взаимодействующих ведущего $x_d(t)$ и ведомого $x_r(t)$ хаотических осцилляторов существует некоторая функциональная зависимость F[·], такая, что имеет место функциональное соотношение $x_r(t)=F[x_d(t)]$. При этом, сам вид данной зависимости F[·] может быть достаточно сложным, в том числе, и фрактальным, что представляется весьма важным при секретной передаче информации [Rulkov N.F. et al. Phys. Rev. E 51 (1995) 980; Hramov A.E., Koronovskii A.A. 71 (2005) 067201].

Удобным и легко осуществимым на практике методом диагностики обобщенной синхронизации является метод вспомогательной системы [Abarbanel H.D.I., Rulkov N.F. and Sushchik M. Phys. Rev. E 53 (1996) 4528]. Суть метода заключается в следующем: наряду с ведомой системой, генерирующей колебания $x_r(t)$, рассматривается идентичная ей вспомогательная система, генерирующая колебания $x_a(t)$. Начальные условия для вспомогательной системы $x_a(t_0)$, где t_0 - начальный момент времени, выбираются отличными от начального состояния ведомой системы $x_r(t_0)$, но лежащими в области притяжения одного аттрактора (как правило, на практике это означает небольшую расстройку начальных условий). В случае отсутствия режима обобщенной синхронизации между взаимодействующими системами вектора состояния ведомой $x_r(t_0)$ и вспомогательной $x_a(t_0)$ систем принадлежат одному и тому же хаотическому аттрактору, но являются различными за счет ляпуновской неустойчивости хаотических траекторий. В том случае, когда имеет место режим обобщенной синхронизации, в силу выполнения соотношений $x_r(t_0)=F[x_d(t_0)]$ и, соответственно, $x_a(t0)=F[x_d(t_0)]$, после завершения переходного процесса состояния ведомой и вспомогательной систем должны стать идентичными $x_a(t_0)\equiv x_r(t_0)$. Таким образом, эквивалентность состояний ведомой и вспомогательной систем после переходного процесса является критерием наличия обобщенной синхронизации между ведущим и ведомым хаотическими системами.

Способ секретной передачи информации, основанный на явлении обобщенной синхронизации, заключается в следующем: полезный сигнал кодируется в виде двоичного кода. Один или несколько управляющих параметров генератора хаотических автоколебаний 2 модулируются полезным двоичным сигналом 1. Это значит, что в зависимости от передаваемого в течение заданного интервала времени двоичного бита ("0" или "1") управляющие параметры генератора хаоса 2 изменяются каким-либо образом, например, незначительным изменением положения основной частоты в спектре хаотического сигнала передающего генератора. Сформированный таким образом сигнал поступает в канал связи 3 и с определенной мощностью передается по каналу связи принимающей стороне. На принимающем конце канала связи находится приемник.

Принцип работы приемника основан на детектировании обобщенной хаотической синхронизации с помощью метода вспомогательной системы. Для этого, на принимающей стороне сигнал, снятый с канала связи, подают на два идентичных генератора хаотических автоколебаний 4 и 5, способных находиться с передающим генератором в режиме обобщенной хаотической синхронизации. Сигналы, снимаемые с выходов

генераторов принимающей стороны, подаются на вычитающее устройство 6. Параметры модуляции управляющих параметров передающего генератора необходимо выбирать таким образом, чтобы в зависимости от передаваемого двоичного бита "0"/"1" между передающим и принимающими генераторами существовал или отсутствовал режим обобщенной хаотической синхронизации. Допустим, при передаче двоичного бита "0" управляющие параметры передатчика выбираются таким образом, что между передающим и принимающими генераторами реализуется режим обобщенной синхронизации. Тогда, в силу наличия функциональной зависимости между состояниями хаотических осцилляторов, колебания, генерируемые двумя идентичными генераторами на принимающей стороне канала связи, будут идентичными и после прохождения вычитающего устройства будет наблюдаться отсутствие каких-либо колебаний, то есть двоичный "0". Напротив, при передаче двоичного бита "1" между передающим и принимающими генераторами отсутствует режим обобщенной синхронизации, и колебания ведомых генераторов на принимающей стороне будут различными. После прохождения вычитающего устройства будут наблюдаться хаотические колебания с ненулевой амплитудой, то есть двоичный бит "1".

В примере конкретной реализации заявляемого способа над исходным полезным цифровым сигналом проводили операции логического кодирования по известным методикам, направленные на избежание появления в цифровом сообщении длинной последовательности битов "0" и "1". Полученная цифровая последовательность представлена на Фиг.2. В качестве передающего генератора хаоса был выбран генератор Ресслера. Принципиальная схема генератора Ресслера приведена в работе [R.Rico-Martinez, K.Krischer, G.Flätgen, J.S.Anderson and I.G.Kevrekidis, Adaptive Detection of Instabilities: An Experimental Feasibility Study, Physica D 176, 1-18 (2003)]. Колебания напряжений x, y, z, снимаемых в различных участках цепи, могут быть описаны системой дифференциальных уравнений:

$$\dot{x} = -\omega y - z,$$

$$\dot{y} = \omega x + a y,$$

$$\dot{z} = b + z(x - c);$$

Управляющие параметры a, b, c и ω характеризуют непосредственно параметры схемы.

Для ведущего генератора Ресслера управляющие параметры были выбраны следующими: a=0.15, b=0.2, c=10, ω - частота генератора. Модуляция управляющих параметров системы определяется следующим образом: если передается бит "0", то ω=1, а если "1", то ω=0.95. Характеристики сложного хаотического сигнала (фазовый портрет в координатах (x; y) и спектр S(f), построенный по колебаниям напряжения x, где f - частота колебаний), генерируемого передающим генератором Ресслера, представлены на Фиг.3.

В принимающем устройстве расположены два идентичных по управляющим параметрам генератора Ресслера, управляющие параметры которых зафиксированы следующим образом:

a=0.15, b=0.2, c=10, ω=0.95.

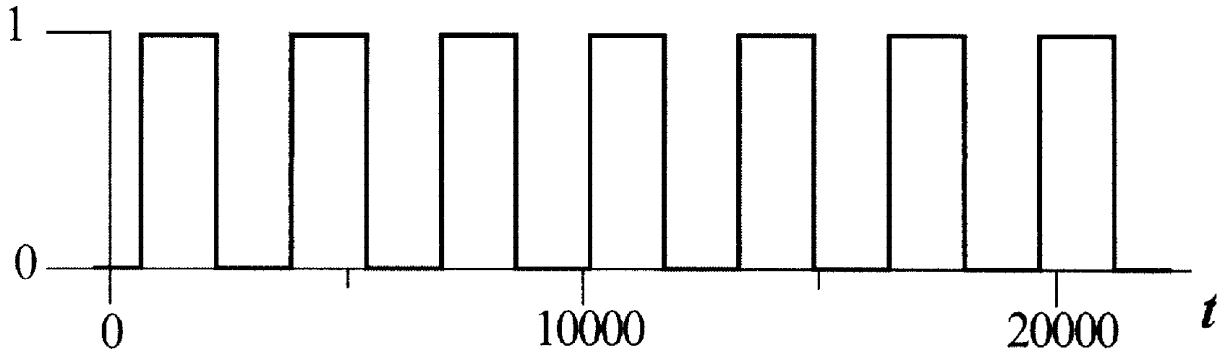
Характеристики откликов генераторов хаоса (фазовые портреты в координатах (x; y) и Фурье-спектры S(f), построенные по колебаниям напряжения x, где f - частота колебаний) на принимающем конце канала связи приведены на Фиг.4 и 5, соответственно. Спектры хаотических сигналов немного различаются между собой и сильно отличаются от спектра передаваемого сигнала, что свидетельствует о невозможности перехвата и детектирования исходного цифрового сообщения без точного знания параметров хаотических генераторов на принимающей стороне.

Для подобной схемы, если в течение времени, когда передается бит "0" (ω=1), передающий и принимающий генераторы находятся в режиме обобщенной синхронизации, а, следовательно, генераторы на принимающей стороне канала связи генерируют идентичные колебания, и после прохождения вычитающего устройства, производящего

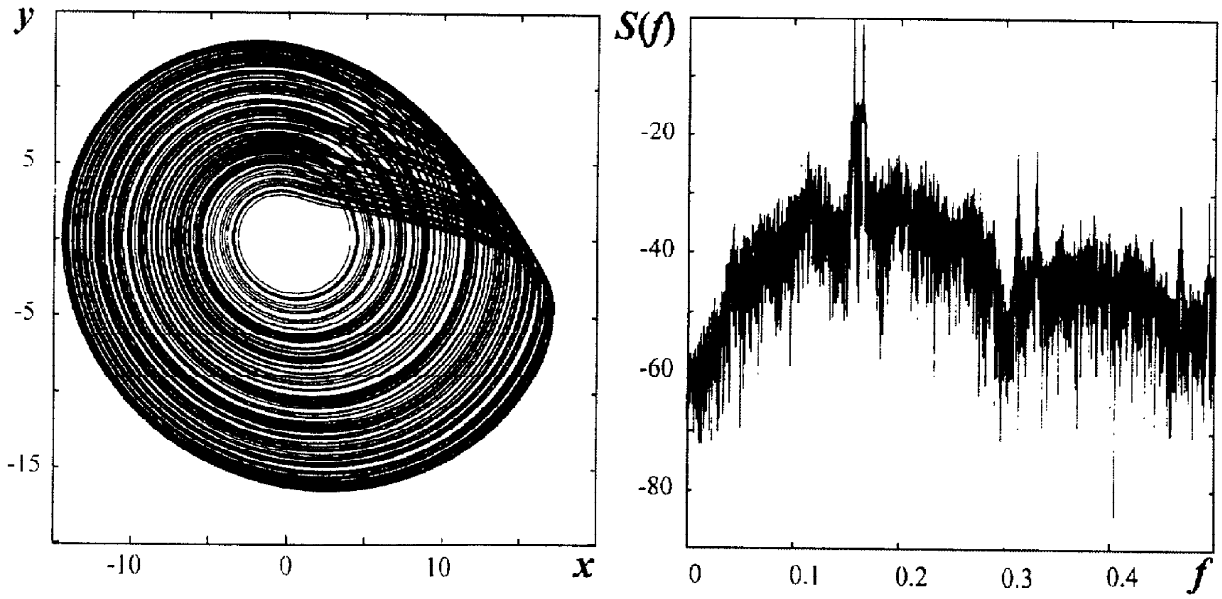
операцию $|x_3 - x_2|^2$, (где x_2 и x_3 - напряжения x генераторов 4 и 5 соответственно (см. Фиг.1)), на выходе отсутствуют колебания, то есть детектируется "0". При ω=0.95 режим обобщенной синхронизации не наблюдается, колебания ведомых генераторов будут неидентичными, и после вычитания получаются не нулевые колебания, то есть бит "1" (см. Фиг.6).

Формула изобретения

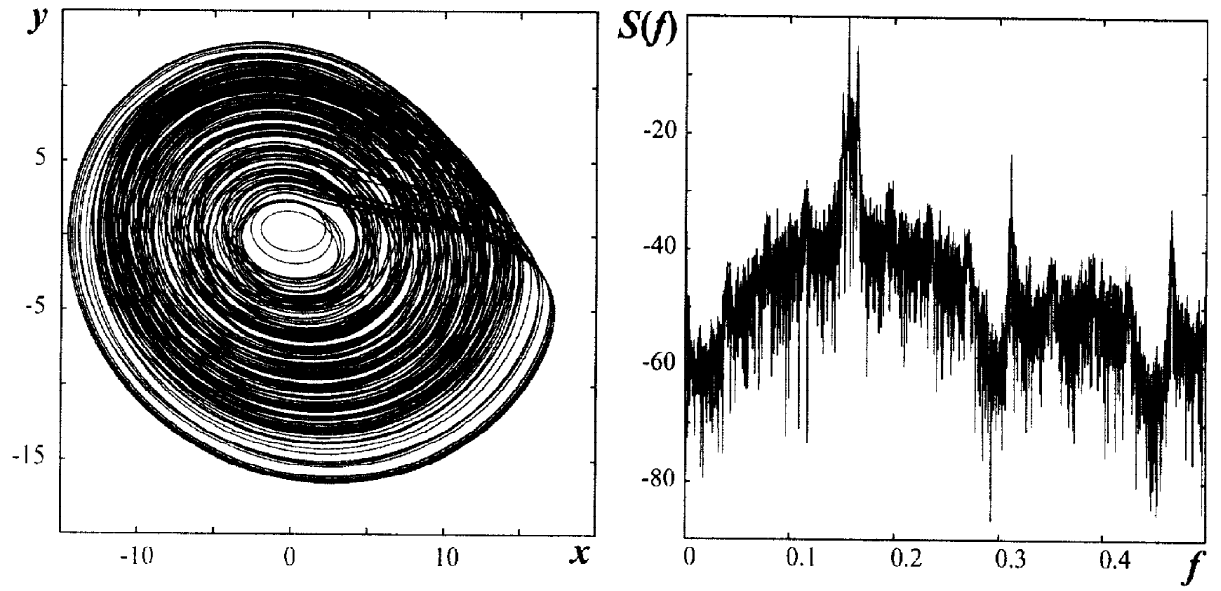
Способ секретной передачи информации, содержащей полезный цифровой сигнал, заключающийся в том, что кодируют полезный сигнал в двоичный код, формируют посредством первого генератора хаоса исходный хаотический детерминированный сигнал, причем формирование сигнала для передачи его по каналу связи осуществляют путем модуляции параметров хаотического сигнала полезным цифровым сигналом, передают сформированный таким образом сигнал по каналам связи, и принимают его на принимающей стороне, отличающийся тем, что на принимающей стороне принятый сигнал разделяют на два идентичных сигнала, при этом первым сигналом воздействуют на второй генератор хаоса, с возможностью получения сигнала, синхронизованного с исходным, причем вторым идентичным сигналом воздействуют на третий генератор хаоса, идентичный второму генератору хаоса по управляющим параметрам, при этом первый и второй генераторы хаоса выбирают с возможностью обеспечения режима обобщенной синхронизации, и снятый с выхода указанных второго и третьего генераторов хаоса сигнал, подают на вычитающее устройство и при наблюдении или отсутствии хаотических колебаний определяют наличие полезного цифрового сигнала, представленного в виде двоичного кода.



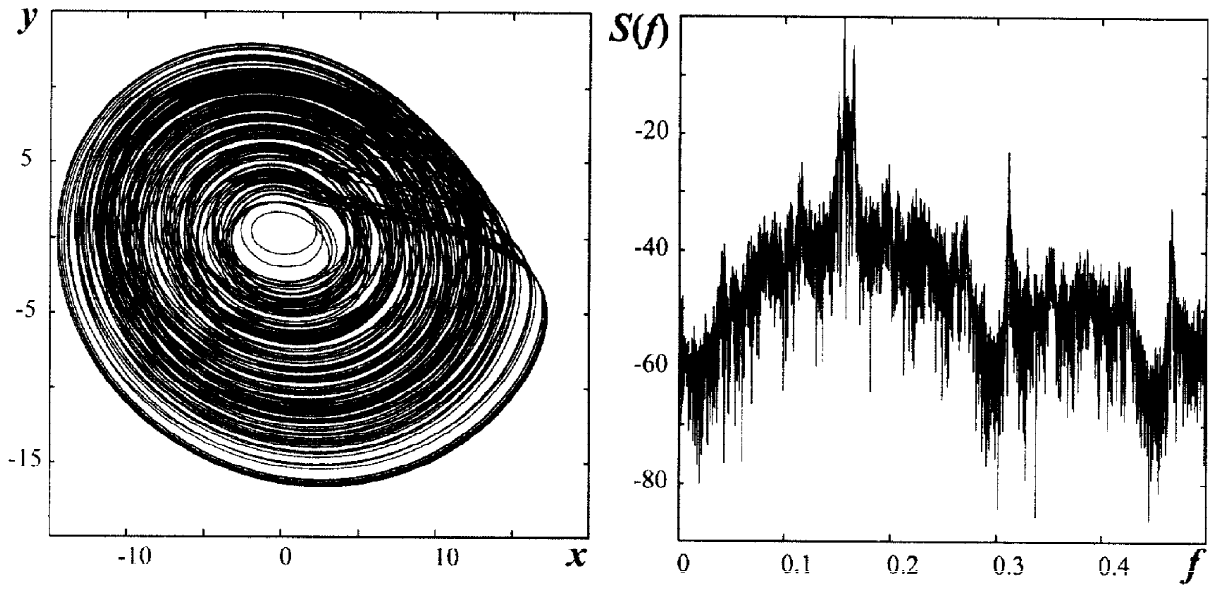
Фиг. 2



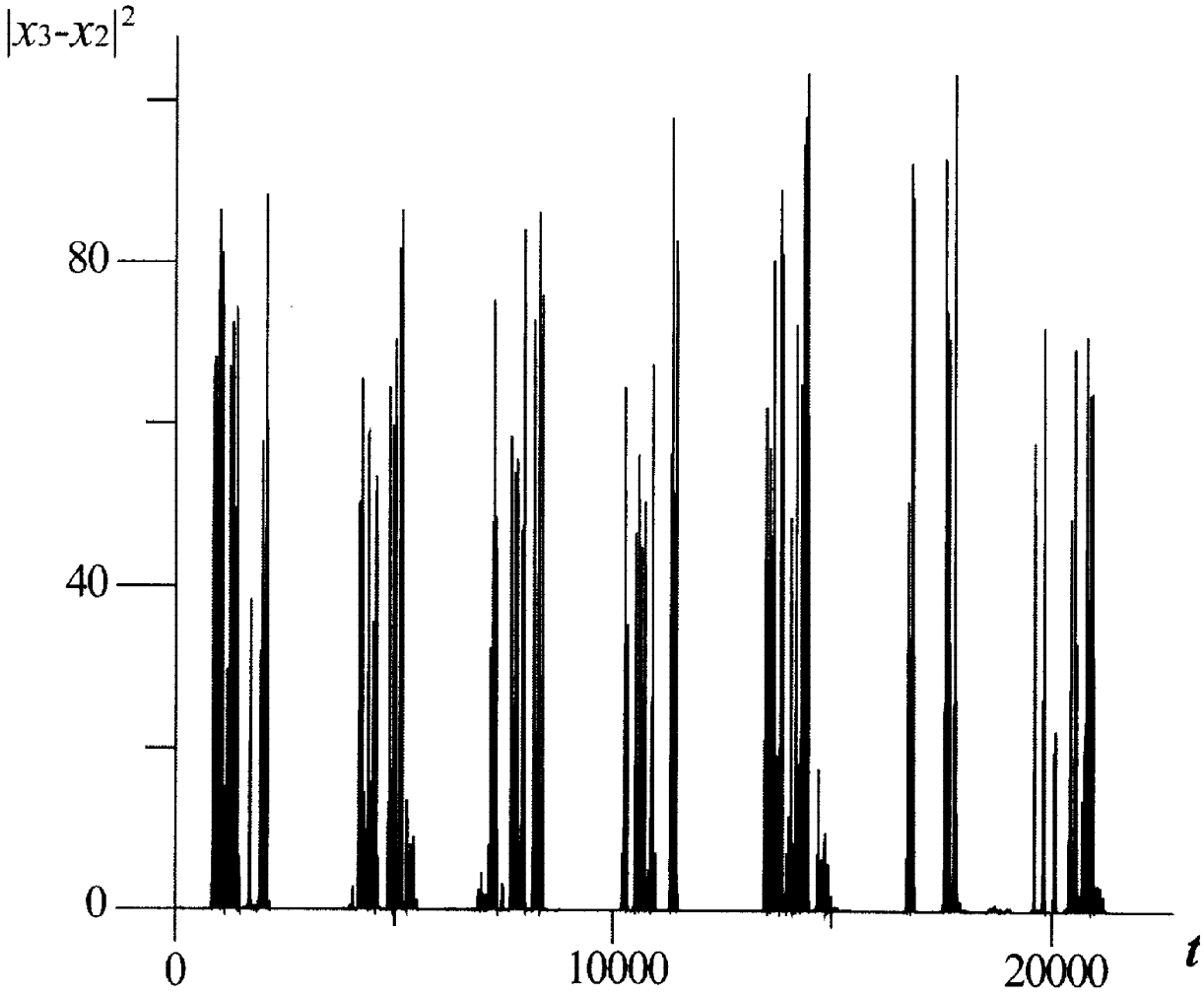
Фиг. 3



Фиг. 4


y
5
-5
-15
-10
0
10
x
S(f)
-20
-40
-60
-80
0
0.1
0.2
0.3
0.4
f

Фиг. 5


|x3-x2|2
80
40
0
0
10000
20000
t

Фиг. 6