



ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

**(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ**

(21)(22) Заявка: **2011152150/08**, **20.12.2011**

(24) Дата начала отсчета срока действия патента:  
**20.12.2011**

Приоритет(ы):

(22) Дата подачи заявки: **20.12.2011**

(45) Опубликовано: **20.09.2013** Бюл. № 26

(56) Список документов, цитированных в отчете о  
поиске: **US 2002/0154677 A1**, **24.10.2002**. **RU**  
**2429566 C1**, **20.09.2011**. **US 6751602 B2**,  
**15.06.2004**. **US 2002/0116196 A1**, **22.08.2002**. **RU**  
**2428795 C1**, **10.09.2011**.

Адрес для переписки:

**410012, г.Саратов, ул. Московская, 155, СГУ,  
ЦПУ, Н.В. Романовой**

(72) Автор(ы):

**Назимов Алексей Игоревич (RU),  
Павлов Алексей Николаевич (RU)**

(73) Патентообладатель(и):

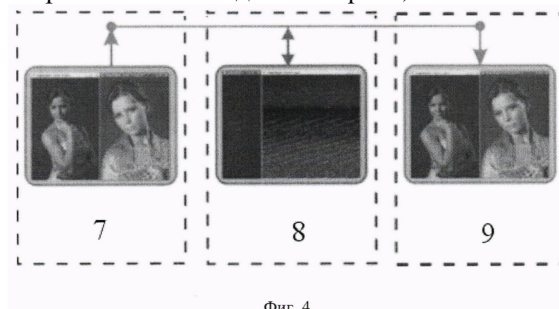
**Федеральное государственное бюджетное  
образовательное учреждение высшего  
профессионального образования  
"Саратовский государственный университет  
им. Н.Г. Чернышевского" (RU)**

**(54) СПОСОБ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ  
ИМПУЛЬСНОГО КОДИРОВАНИЯ**

(57) Реферат:

Изобретение относится к радиотехнике и теории связи и может найти применение в системах связи, использующих хаотические маскирующие сигналы для повышения степени защиты передаваемой информации от несанкционированного доступа. Технический результат заключается в повышении степени защиты информации. Способ защищенной передачи информации включает формирование информационного сигнала с закодированной информацией, аддитивное суммирование этого сигнала с хаотическим маскирующим сигналом, передачу суммарного сигнала по

каналу связи к приемному устройству, детектирование информации, в процессе детектирования проводят распознавание информационного сигнала на основе нейросетевого метода. 1 з.п. ф-лы, 4 ил.



Фиг. 4



FEDERAL SERVICE  
FOR INTELLECTUAL PROPERTY

**(12) ABSTRACT OF INVENTION**(21)(22) Application: **2011152150/08, 20.12.2011**(24) Effective date for property rights:  
**20.12.2011**

Priority:

(22) Date of filing: **20.12.2011**(45) Date of publication: **20.09.2013 Bull. 26**

Mail address:

**410012, g.Saratov, ul. Moskovskaja, 155, SGU,  
TsPU, N.V. Romanovoj**

(72) Inventor(s):

**Nazimov Aleksej Igorevich (RU),  
Pavlov Aleksej Nikolaevich (RU)**

(73) Proprietor(s):

**Federal'noe gosudarstvennoe bjudzhetnoe  
obrazovatel'noe uchrezhdenie vysshego  
professional'nogo obrazovanija "Saratovskij  
gosudarstvennyj universitet im. N.G.  
Chernyshevskogo" (RU)****(54) METHOD FOR SECURE TRANSMISSION OF INFORMATION USING PULSE CODING**

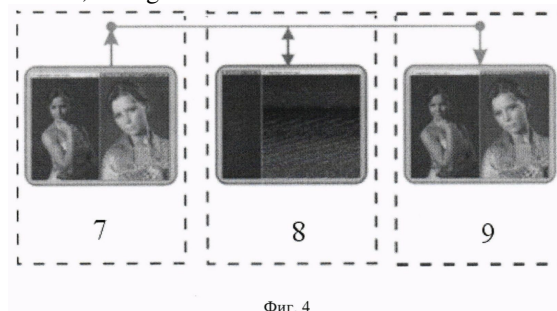
(57) Abstract:

FIELD: radio engineering, communication.

SUBSTANCE: method for secure transmission of information includes generating an information signal with encoded information, adaptive summation of said signal with a chaotic masking signal, transmitting the resultant signal over a communication channel to a receiving device, detecting information; during detection, the information signal is identified based on a neural network technique.

EFFECT: high information security.

2 cl, 4 dwg



Фиг. 4

Изобретение относится к радиотехнике и теории связи и может найти применение в системах связи, использующих хаотические маскирующие сигналы для повышения степени защиты передаваемой информации от несанкционированного доступа.

Применение хаотических сигналов в качестве маскирующих или несущих колебаний представляет собой один из новых способов защиты информации в системах связи, активно разрабатываемый с начала 1990-х годов. Первые работы, посвященные использованию явления динамического хаоса для обеспечения конфиденциальности передаваемой информации, заложили теоретические основы новых принципов кодирования и детектирования информационных сигналов (Cuomo K.M., Oppenheim A.V. Circuit implementation of synchronized chaos with applications to communications // Phys. Rev. Lett. 71, 1993, 65; Cuomo K.M., Oppenheim A.V. Communication using synchronized chaotic systems // US Patent №5291555 от 01.03.1994; Kocarev L., Halle K.S., Eckert K., Chua L.O., Parlitz U. Experimental demonstration of secure communications via chaotic synchronization // Int. J. Bifurcation Chaos. 2, 1992, 709; Dedieu H., Kennedy M.P., Hasler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit // IEEE Trans. Circuits Syst. 40, 1993, 634; Parlitz U. Estimating model parameters from time series by autosynchronization // Phys. Rev. Lett. 76, 1996, 1232). В предложенных структурных схемах практической реализации процедуры детектирования информационных сигналов, передаваемых путем модуляции параметров генератора хаотических колебаний, расположенного в передающем устройстве, или путем аддитивного суммирования информационного сигнала и хаотических маскирующих колебаний, был сделан акцент на явлении полной синхронизации колебаний. Однако эффективность таких структурных схем ограничивается требованием высокой идентичности генераторов приемника и передатчика, которую сложно обеспечить на практике. Несмотря на достигнутые успехи по передаче речевых и музыкальных сигналов в низкочастотном и в радиодиапазонах (Dmitriev A.S., Panas A.I., Starkov S.O. Experiments on speech and music signals transmission using chaos // Int. J. Bifurcation and Chaos. 5(4), 1995, 1249), стало ясно, что применение явления полной хаотической синхронизации не позволяет улучшать характеристики систем связи, использующие хаотические сигналы, так как приводит к серьезным ограничениям на качество канала связи.

Возможными решениями существующей проблемы являются модификации систем связи путем использования явления обобщенной хаотической синхронизации (Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е. Способ секретной передачи информации // Патент РФ №2295835 от 20.03.2007) или отказ от принципов хаотической синхронизации и применение альтернативных способов детектирования. В качестве таких способов может быть использована, например, техника реконструкции динамических систем, позволяющая устранить ряд принципиальных проблем, присущих системам связи, использующим принцип синхронизации хаоса (Anishchenko V.S., Pavlov A.N. Global reconstruction in application to multichannel communication // Phys. Rev. E. 57, 1998, 2455; Павлов А.Н., Анищенко В.С. Способ многоканальной конфиденциальной передачи информации // Патент РФ №2382502 от 20.02.2010). Значительный прогресс в развитии систем связи, применяющих явление динамического хаоса, был достигнут в работах группы А.С. Дмитриева (ИРЭ РАН), предложивших схему прямохаотической радиосвязи и использование для передачи сообщений хаотических радиоимпульсов (Дмитриев А.С., Панас А.И., Старков С.О. и др. Способ передачи информации с помощью хаотических сигналов // Патент РФ №2185032 от 27.07.2000; Дмитриев А.С., Панас А.И. Динамический хаос. Новые

носители информации для систем связи. М: Физматлит, 2002).

Вместе с тем следует отметить, что применение хаотических колебаний для защиты передаваемых информационных сообщений в настоящее время относится к числу развивающихся направлений, и разработка новых принципов кодирования и детектирования передаваемых сигналов, способных обеспечить возможности создания систем связи, конкурентоспособных по сравнению с существующими аналогами или превосходящих их, является актуальной задачей науки и техники. С этой целью представляется целесообразным использование современных информационных технологий в области анализа сложных сигналов и систем.

Наиболее близким к предлагаемому нами способу защищенной передачи информации является метод, предложенный в работе Cuomo K.M., Oppenheim A.V. Circuit implementation of synchronized chaos with applications to communications // Phys. Rev. Lett. 71, 1993, 65. Данный метод предусматривает добавление хаотического маскирующего сигнала к передаваемому информационному сигналу и проведение процедуры детектирования на основе явления полной синхронизации колебаний. Основным недостатком данного метода является принцип детектирования, не позволяющий обеспечить приемлемое качество передачи сообщений.

Задачей настоящего изобретения является разработка нового способа защищенной передачи информации с использованием импульсного кодирования и альтернативного принципа детектирования информационных сигналов.

Технический результат, достигаемый в предлагаемом способе передачи информации, состоит в упрощении его реализации за счет перехода от систем связи с двумя идентичными генераторами хаотических колебаний в приемном и передающем устройствах к системам связи, содержащим генераторы импульсных сигналов только в передающем устройстве и не требующих их идентичности. Кроме того, предлагаемый способ является более производительным, так как предусматривает новый принцип детектирования передаваемых сообщений, основанный на нейросетевом методе распознавания сигналов.

Поставленная задача достигается тем, что способ защищенной передачи информации, включающий формирование информационного сигнала с закодированной информацией, аддитивное суммирование информационного сигнала с хаотическим маскирующим сигналом, передачу суммарного сигнала по каналу связи к приемному устройству, детектирование информации, согласно решению в качестве информационного и маскирующего сигналов используют последовательности одиночных импульсов подобной формы, при этом кодирование информации осуществляют расстоянием между соседними импульсами информационного сигнала, и в процессе детектирования проводят распознавание формы импульсов на основе нейросетевого метода и преобразуют интервалы времени между импульсами информационного сигнала в информацию. При аддитивном суммировании информационного сигнала с хаотическим маскирующим сигналом дополнительно подмешивают шум.

Распознавание формы импульсов осуществляют с использованием блока цифровой обработки сигналов, выполненного с возможностью идентифицировать похожие по форме одиночные импульсы в условиях помех с использованием принципов нейросетевого распознавания образов.

Изобретение поясняется чертежами, где на фиг.1 и фиг.2 представлены результаты распознавания последовательностей близких по форме одиночных импульсов при наличии помех на основе стандартного метода анализа главных компонент (Jolliffe

I.T. Principal Component Analysis, NY: Springer, 2002) (фиг.1) и метода искусственных нейронных сетей (Хайкин С. Нейронные сети: полный курс, М.: Вильямс, 2006) (фиг.2), схема для реализации системы передачи информации с использованием импульсного кодирования (фиг.3), а на фиг.4 представлены иллюстрации, характеризующие

эффективность системы передачи информации, где приняты следующие обозначения:

- 1 - блок преобразования информации в точечный процесс;
- 2 - генератор одиночных импульсов;
- 3 - генератор хаотической последовательности маскирующих одиночных импульсов;
- 4 - источник шума;
- 5 - блок распознавания формы одиночного импульса;
- 6 - преобразователь точечного процесса в информацию;
- 7 - передаваемые изображения,
- 8 - пример детектирования в случае несанкционированного доступа,
- 9 - детектирование с помощью настроенной нейросети.

Способ заключается в следующем. Информация с помощью блока 1 преобразуется в точечный процесс, кодирующий информацию в интервалах времени между моментами генерации одиночных импульсов, форма которых задается генератором 2.

Преобразование в точечный процесс аналогового сигнала может проводиться в рамках модели «накопление-сброс», предусматривающей интегрирование сигнала и генерацию импульсов при достижении интегралом заданного порогового уровня, после чего значение интеграла обнуляется (Racicot D., Longtin A. Interspike interval attractors from chaotically driven neuron models // Physica D, 104, 1997, 184). Полученный информационный сигнал суммируется с хаотической последовательностью маскирующих одиночных импульсов незначительно отличающейся формы, которая генерируется в блоке 3. Для обеспечения защиты передаваемой информации дополнительно подмешивается шум 4, приводящий к искажениям формы импульсов и усложняющий их распознавание. Интенсивность шума является достаточно большой для того, чтобы затруднить процедуру идентификации формы похожих импульсов. Дополнительно данная процедура осложняется наличием шумов в канале связи. В приемном устройстве, включающем блоки 5 и 6, проводится детектирование информационного сигнала. В процессе детектирования осуществляется распознавание зашумленных одиночных импульсов с помощью блока 5, содержащего микропроцессор, запрограммированный на реализацию процедуры нейросетевого метода. Использование микропроцессора является простым и дешевым вариантом исполнения, позволяющим эффективно решать задачу распознавания формы сигнала в условиях сильных помех. Выделенная последовательность одиночных импульсов информационного сигнала в далее преобразуется в информацию в блоке 6. По аналогии, данный способ может быть реализован для цифровых сигналов.

Процедура распознавания последовательности импульсов, кодирующей передаваемое сообщение во временных интервалах между импульсами, базируется на стандартном методе распознавания сигналов на основе искусственных нейронных сетей, использующих перцептронную структуру с применением модели нейрона Маккалока-Питса (Хайкин С. Нейронные сети: полный курс, М.: Вильямс, 2006). Более эффективные методы распознавания могут основываться на вейвлетных нейронных сетях (Q. Zhang, A. Benveniste, Wavelet networks // IEEE Trans. Neural Networks, 3, 1992, 889), способных снизить погрешность идентификации формы зашумленного импульса (Тупицын А.Н., Назимов А.И., Павлов А.Н. Идентификация потенциалов действия малых ансамблей нейронов с применением вейвлет-анализа и метода

нейронных сетей // Известия Саратовского университета. Новая серия. Физика. 2, 2009, 49). Выбор того или иного типа нейросети не является принципиальным для практической реализации предлагаемого нами способа защиты передаваемой информации, и определяется техническими требованиями к характеристикам канала связи. В частности, при высоком уровне шумов использование вейвлетных нейронных сетей является более предпочтительным вариантом распознавания форм импульсных сигналов.

Распознавание сигналов с помощью нейросети требует предварительной процедуры ее адаптации (обучения) на заранее известных последовательностях одиночных импульсов, позволяющей далее проводить идентификацию формы зашумленных импульсов, поступающих на вход приемного устройства. Предварительная настройка нейросети на известной последовательности одиночных импульсов генераторов 2 и 3 является «ключом» к последующему отделению информационного сигнала от маскирующей хаотической последовательности импульсов похожей формы. Вне зависимости от выбора типа нейросети, правила обучения можно обобщить в виде следующего алгоритма вычислений:

1) Задаются начальные значения синаптических коэффициентов и пороговых уровней нейросети, а также вейвлет-коэффициентов (в случае использования вейвлетных нейросетей;

2) Проводится распознавание форм одиночных импульсов обучающей выборки. После распознавания каждой формы импульса вычисляется погрешность на основе стандартного алгоритма обратного распространения ошибки (Rumelhart D.E., Hinton G.E., Williams R.J. Learning representations of back-propagation errors // Nature (London) - 1986, 533), и корректируются коэффициенты и пороговые уровни нейросети;

3) Процедура распознавания и коррекции повторяется в течение определенного количества этапов обучения, которое определяется, исходя из специфики решаемой задачи (выбранных форм импульсных сигналов).

После предварительной настройки нейросеть позволяет разделять информационную последовательность одиночных импульсов, кодирующую передаваемое сообщение, и маскирующую хаотическую последовательность импульсов. Не располагая настроенной нейросетью, при высоком уровне шумов, подмешиваемых к передаваемому сигналу, сторонний наблюдатель не сможет достоверно различить формы импульсов генераторов 2 и 3. Это проиллюстрировано на фиг.1 и фиг.2, где приведены примеры распознавания информационной и маскирующей последовательностей близких по форме импульсов при наличии сильных помех. Метод анализа главных компонент, часто применяемый для решения задач распознавания сигналов импульсного типа, приводит к большой ошибке распознавания (более 40% при выбранном уровне фонового шума) (фиг.1), при этом нейросетевой метод обеспечивает ошибку, близкую к нулю (фиг.2).

Сравнительный анализ нейросетевых методов распознавания формы импульсных сигналов и других методов цифровой обработки экспериментальных данных свидетельствует об эффективности аппарата искусственных нейронных сетей при решении данных задач (Тупицын А.Н., Назимов А.И., Павлов А.Н. Идентификация потенциалов действия малых ансамблей нейронов с применением вейвлет-анализа и метода нейронных сетей // Известия Саратовского университета. Новая серия. Физика. 2, 2009, 49). Проведенные тестовые исследования свидетельствуют о возможности распознавания не менее трех последовательностей близких по форме одиночных импульсов с помощью нейросетевых методов. Это позволяет осуществить

реализацию системы многоканальной связи, в рамках которой принимаемый на входе приемного устройства несущий сигнал будет содержать несколько информационных сигналов. С точки зрения практической реализации такой системы связи необходимо включить дополнительные блоки в схему, изображенную на фиг.3, а именно,  
 5 количество блоков 1, 2 и 6 должно равняться количеству одновременно передаваемых информационных сигналов.

После разделения импульсов на кластеры в пространстве характеристик нейросетевого метода, принадлежность каждого конкретного импульса  
 10 определенному кластеру идентифицируется с помощью стандартного метода k-средних (Lewicki M. A review of methods for spike sorting: the detection and classification of neural potencies // Net. Com. Neu. Sys., 9, 1998, R53). При использовании трех типов импульсов предлагаемый способ позволяет реализовать процедуру одновременной передачи двух информационных сообщений, для чего нужно предусмотреть наличие  
 15 двух генераторов импульсных сигналов, кодирующих передаваемую информацию, и генератора хаотической последовательности маскирующих одиночных импульсов.

Проведенные исследования подтвердили возможность одновременной передачи не менее двух информационных сигналов, замаскированных в хаотической  
 20 последовательности одиночных импульсов генератора 3 (фиг.4). К числу достоинств предложенного способа относятся:

1) Отсутствие проблемы идентичности генераторов приемного и передающего устройства, существенно ограничивающей возможности метода (Cuomo K.M., Oppenheim A.V. Circuit implementation of synchronized chaos with applications to  
 25 communications // Phys. Rev. Lett. 71, 1993, 65), основанного на явлении полной синхронизации хаотических колебаний;

2) Высокая помехоустойчивость способа защищенной передачи информации, существенно превосходящая возможности альтернативного подхода, основанного на  
 30 реконструкции динамических систем (Павлов А.Н., Анищенко В.С. Способ многоканальной конфиденциальной передачи информации // Патент РФ №2382502 от 20.02.2010);

3) Оригинальный метод детектирования. До настоящего времени аппарат искусственных нейронных сетей не применялся в системах связи, использующих  
 35 хаотические маскирующие сигналы.

Таким образом, положительными эффектами заявляемого способа защищенной передачи информации являются высокая помехоустойчивость, возможность  
 40 многоканальной передачи информации в режиме реального времени и новый принцип детектирования информационных сообщений в приемном устройстве.

#### Формула изобретения

1. Способ защищенной передачи информации, включающий формирование информационного сигнала с закодированной информацией, аддитивное суммирование  
 45 информационного сигнала с хаотическим маскирующим сигналом, передачу суммарного сигнала по каналу связи к приемному устройству, детектирование информации, отличающийся тем, что в качестве информационного и маскирующего сигналов используют последовательности одиночных импульсов подобной формы,  
 50 при этом кодирование информации осуществляют расстоянием между соседними импульсами информационного сигнала, и в процессе детектирования проводят распознавание формы импульсов на основе нейросетевого метода и преобразуют интервалы времени между импульсами информационного сигнала в информацию.

2. Способ по п.1, отличающийся тем, что при аддитивном суммировании информационного сигнала с хаотическим маскирующим сигналом дополнительно подмешивают шум.

5

10

15

20

25

30

35

40

45

50

