Министерство образования Республики Беларусь

Учреждение образования

Гомельский государственный технический университет имени П.О. Сухого

Факультет автоматизированных и информационных систем

Кафедра «Информатика»

Отчет по лабораторной работе №5

по дисциплине: «Основы защиты информации»

по теме: «Патентный поиск»

Выполнил: студент гр. ИП-32

Кирпиченко Д.Д.

Принял: профессор

Кудин В.П.

Гомель 2022

**Цель работы:** изучить принципы работы с патентными данными.

**Задание:**

1. Выбрать объект промышленной собственности, имеющий непосредственное отношение к вычислительной технике и программированию, а также к защите информации (системы обработки данных в различных отраслях, компьютерные системы, обработка или генерация данных, секретная связь, устройства для секретной или скрытой связи и т.д.)

2. Для выбранного объекта по вышеописанной методике найти 4 – 5 релевантных патентных документов и предоставить их исчерпывающие описания в отчёте о проведенном поиске.

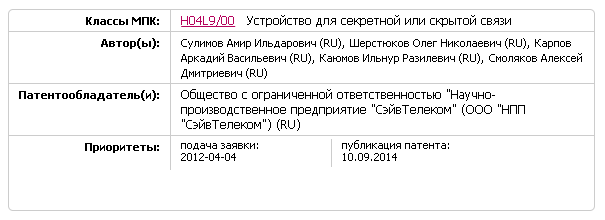
**Ход работы:**

**Раздел патентного поиска:**

H04L 9/00 Устройства для секретной или скрытой связи

**Патент 1**





**Формула:**

Способ защиты информации, основанный на двусторонней передаче и последующем обнаружении зондирующих радиосигналов, несущих отметки времени момента своего излучения, привязанные к предварительно сведенным шкалам времени, и исходящих от расположенных на обоих концах радиолинии устройств связи, проведении необратимых математических преобразований над числовыми последовательностями, шифровании и дешифровании сообщений с использованием ключа, отличающийся тем, что выполняют операцию взаимного опознавания участников информационного обмена и синхронизуют шкалы времени устройств связи участников, задают интервал времени работы средств защиты информации, в течение которого на обоих концах радиолинии накапливают два совпадающих друг с другом набора двоичных эквивалентов оцифрованных результатов измерений случайных относительных задержек моментов прихода в точку приема различных дошедших до приемника по независимым путям со случайными протяженностями копий зондирующего многолучевую среду сигнала, над накопленными наборами двоичных эквивалентов каждым из устройств связи выполняют совпадающие на обоих концах радиолинии необратимые математические преобразования, формируют на приемном и передающем концах пару идентичных экземпляров ключа симметричного шифрования, накопленные наборы двоичных эквивалентов пополняют двоичными эквивалентами оцифрованных результатов очередных измерений случайных относительных задержек моментов прихода в точку приема различных дошедших до приемника по независимым путям со случайными протяженностями копий зондирующего многолучевую среду сигнала, при этом в качестве механизма распределения экземпляров ключа симметричного шифрования используют свойства взаимности условий многолучевого распространения радиоволн.

**Прототип**

Наиболее близким по сути предлагаемого изобретения - прототипом - является способ защиты информации, основанный на использовании свойств случайного природного процесса - случайной траектории многолучевого распространения радиоволн . В прототипе в качестве элементов ключа симметричного шифрования применяют двоичные эквиваленты измерений случайной фазы результирующего радиосигнала, претерпевшего распространение через многолучевый радиоканал.

Прототип обладает следующими недостатками:

способ защиты информации, патент № 2527734 трудно осуществимые на практике требования к точности синхронизации шкал времени устройств связи, расположенных на обеих сторонах взаимного многолучевого радиоканала;

способ защиты информации, патент № 2527734 необходимость обеспечения высокого отношения (сигнал/шум) для выполнения точных когерентных измерений фазы несущей и/или промежуточной частоты;

способ защиты информации, патент № 2527734 сосредоточенность большой мощности зондирующих сигналов в узкой полосе частот, что создает интенсивную помеху для других информационно-телекоммуникационных систем (ИТС) и не обеспечивает удовлетворяющую стандартам [4, 5] электромагнитную совместимость (ЭМС) с ними.

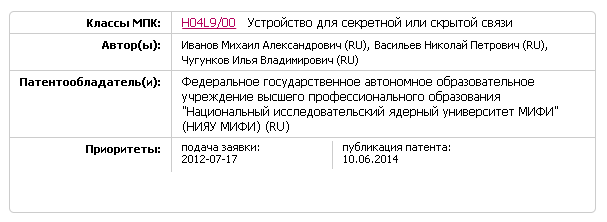
**Что отличается:**

Целью предлагаемого изобретения является повышение надежности защиты информации в процессе обмена информацией.

Цели достигают тем, что в процессе обмена информацией производят двустороннюю передачу и последующее обнаружение зондирующих радиосигналов, исходящих от расположенных на обоих концах радиолинии устройств связи. Зондирующие радиосигналы несут отметки момента времени своего излучения, привязанные к предварительно сведенным шкалам времени. Задают, исходя из требуемой степени надежности защиты информации, интервал времени работы устройств связи на обоих концах радиолинии. В течение заданного времени на обоих концах радиолинии накапливают два совпадающих друг с другом набора двоичных эквивалентов оцифрованных результатов измерений случайного природного процесса. В качестве упомянутого природного процесса используют случайные относительные задержки моментов прихода в точку приема различных копий зондирующего многолучевую среду сигнала. Каждая копия сигнала (парциальный луч) преодолевает непредсказуемый путь при распространении от передатчика к приемнику, в результате чего время ее (копии) прихода в точку приема оказывается случайной величиной. В каждом из упомянутых устройств связи накопленные наборы измерений подвергают одинаковым необратимым математическим преобразованиям и образуют в упомянутых устройствах связи шифрующую на передающем конце и дешифрующую на приемном конце последовательности. Шифрующая и дешифрующая последовательности представляют собой два идентичных экземпляра ключа симметричного шифрования, единого для приемного и передающего устройств связи. Далее применяют шифрование и дешифрование сообщений с использованием ключа. При этом пополняют упомянутые накопленные наборы двоичных эквивалентов результатов измерений двоичными эквивалентами результатов очередных измерений относительных задержек прихода различных парциальных лучей в точку приема. В качестве механизма распределения двух экземпляров сгенерированного ключа симметричного шифрования между участниками информационного обмена (устройствами связи, расположенными на противоположных концах радиолинии) используют свойства взаимности условий многолучевого распространения радиоволн как в прямом, так и в обратном направлениях передачи.

**Патент 2**





**Формула:**

Способ трехмерного нелинейного преобразования замены, включающий представление входного блока М и всех промежуточных результатов преобразования разрядностью N3 (N > 1) бит в виде кубического массива битов NхNх N; введение понятие слоя (Layer) - квадратного массива битов NхN; выполнение трех раундов преобразования соответственно вдоль осей х, у, z; деление блока данных М перед выполнением преобразований первого раунда на N слоев L x0, Lx1, ..., Lx(N-1) вдоль оси х; деление результата работы первого раунда перед выполнением преобразований второго раунда на N слоев Ly0, Ly1, ..., L y(N-1) вдоль оси у; деление результата работы второго раунда перед выполнением преобразований третьего раунда на N слоев Lz0, Lz1 , ..., Lz(N-1) вдоль оси z; отличающийся тем, что формируют k таблиц замен Si размерностью Nх2N каждая, i = 0, 1, ..., (k - 1), 1способ трехмерного нелинейного преобразования замены, патент № 2519004 k; в первом раунде выполняют N двухмерных преобразований замены слоев Lx0, Lx1, ..., Lx(N-1); во втором раунде выполняют N двухмерных преобразований замены слоев Ly0 , Ly1, ..., Ly(N-1) ; в третьем раунде выполняют N двухмерных преобразований замены слоев Lz0, Lz1, ..., Lz(N-1), при этом двумерное преобразование замены слоя L выполняется за два шага, на первом шаге слой L делят на NN -разрядных векторов-строк R0, R1 ..., R(N-1) , каждый j-й N-разрядный вектор Rj , j= 0, 1, ..., (N - 1), заменяют N-разрядным вектором из соответствующей таблицы замен Si согласно выражению Rj = Sj (Rj), выбранные из таблицы замен NN- разрядных векторов Rj объединяют в преобразованный слой L; на втором шаге слой L делят на NN -разрядных векторов-столбцов С0 , С1 ..., С (N-1), каждый j-й N-разрядный вектор Cj, j = 0, 1, (N - 1), заменяют N-разрядным вектором из соответствующей таблицы замен Sj согласно выражению Cj = Sj (Cj), выбранные из таблицы замен N N -разрядных векторов Cj объединяют в преобразованный слой L, который выдают в качестве результата двумерного преобразования замены слоя L.

**Прототип**

Наиболее близким по своей технической сущности к заявленному способу является принятый за прототип способ трехмерного преобразования [Иванов М.А., Ковалев А.В., Чугунков И.В. и др. Стохастические методы защиты информации в компьютерных системах и сетях. М.: Кудиц-Пресс, 2009, с.243-246], включающий представление входного блока M и всех промежуточных результатов преобразования разрядностью 512 бит в виде кубического массива; введение понятие слоя (Layer) - квадратного массива разрядностью 128 бит; выполнение трех раундов преобразования соответственно вдоль осей x, y, z; деление блока данных M перед выполнением преобразований первого раунда на 4 слоя Lx0, Lx1, Lx2, Lx3 вдоль оси x; деление результата работы первого раунда перед выполнением преобразований второго раунда на 4 слоя Ly , Ly1, Ly2, Ly3 вдоль оси y; деление результата работы второго раунда перед выполнением преобразований третьего раунда на 4 слоя Lz0, Lz1, L z2, Lz3 вдоль оси z. **Чем отличается:**

К причинам, препятствующим достижению указанного ниже технического результата, относится недостаточная эффективность при реализации на основе гибридных суперкомпьютерных технологий из-за малой степени параллелизма на уровне инструкций и зависимость разрядности используемых блоков замены от разрядности обрабатываемых блоков данных.

Указанный технический результат при осуществлении изобретения достигается тем, что в многораундовом трехмерном преобразовании замены, включающем

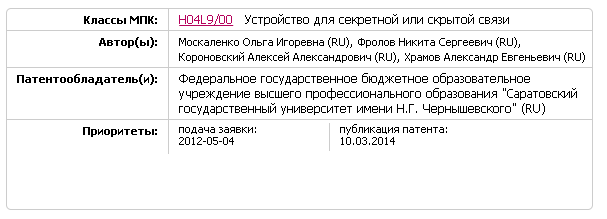
представление входного блока M и всех промежуточных результатов преобразования разрядностью N3 (N>1) бит в виде кубического массива битов N×N×N;

введение понятие слоя (Layer) - квадратного массива битов N×N;

выполнение трех раундов преобразования соответственно вдоль осей x, y, z;

**Патент 3**





**Формула:**

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

2. Способ по п.1, отличающийся тем, что сформированный первым генератором детерминированный хаотический сигнал перед передачей по каналу связи суммируют с шумовым сигналом, производимым генератором шума.

3. Способ по п.2, отличающийся тем, что характеристики генератора шума модулируются цифровым или аналоговым сигналом, содержащим ложное, несущественное или открытое информационное сообщение.

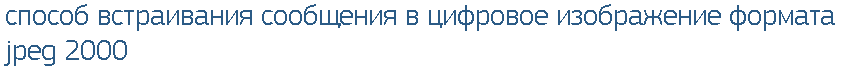
**Прототип**

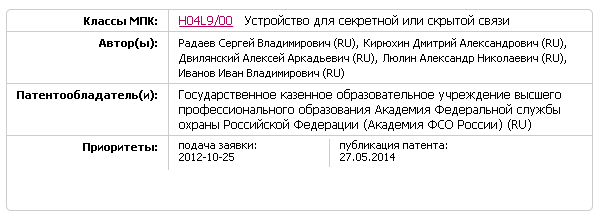
Принципиальными недостатками большинства известных схем и устройств являются, в первую очередь, нестабильность их работы при неидентичности параметров передающего и принимающего генераторов, находящихся, в том числе, на различных сторонах канала связи, деструктивное влияние шумов на качество передачи информации, низкая конфиденциальность, трудности технической реализации. В то же самое время, известен ряд способов 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; Короновский А.А., Москаленко О.И., Храмов А.Е. Способ скрытой передачи информации // Патент на изобретение № 2349044 от 10.03.2009; Москаленко О.И., Короновский А.А., Храмов А.Е. Способ скрытой передачи информации с изменяющимися характеристиками генератора шума // Патент на изобретение № 2421923 от 20.06.2011), в которых часть вышеуказанных недостатков исправлена или снижено их влияние. При этом способ (Короновский А.А., Москаленко О.Испособ скрытой передачи информации, патент № 2509423 Попов П.В., Храмов А.Е. Способ секретной передачи информации // Патент на изобретение № 2295835 от 20.03.2007) является прототипом для способа (Короновский А.А., Москаленко О. И., Храмов А.Е. Способ скрытой передачи информации // Патент на изобретение № 2349044 от 10.03.2009), который, в свою очередь, может быть рассмотрен как прототип для способа (Москаленко О.И., Короновский А.А., Храмов А.Е. Способ скрытой передачи информации с изменяющимися характеристиками генератора шума // Патент на изобретение № 2421923 от 20.06.2011). Они основаны на режиме обобщенной синхронизации и являются наиболее близкими к заявляемому способу.

**Чем отличается:**

Таким образом, положительным эффектом заявляемого способа скрытой передачи информации является ликвидация нестабильности работы способа при неидентичности параметров принимающих генераторов и повышение качества передачи информации.

**Патент 4**





**Формула:**

Способ встраивания сообщения в цифровое изображение формата JPEG 2000, заключающийся в замене кодирующих коэффициентов среднечастотных и высокочастотных поддиапазонов вейвлет-преобразования, отличающийся тем, что встраивание производят после процедуры квантования в блоки вейвлет-коэффициентов размером NxN, причем значения битов встраиваемого сообщения кодируют четностью суммы значений вейвлет-коэффициентов в блоке, при этом, если значение встраиваемого бита не совпадает с четностью суммы значений вейвлет-коэффициентов в блоке, значение одного из них увеличивают на единицу, причем для модификации выбирают вейвлет-коэффициент, значение которого имеет наибольшую дробную часть.

**Прототип**

Наиболее близким по технической сущности к заявляемому изобретению (прототипом) является способ (См. Патент США № 6556689 В1, опубл. 29.03.2003 г.), заключающийся в том, что к исходному цифровому изображению применяют дискретное вейвлет-преобразование, для встраивания цифрового водяного знака выбирают вейвлет-коэффициенты с большими значениями в среднечастотных и в высокочастотных поддиапазонах, перед встраиванием цифровой водяной знак преобразуют в псевдослучайную последовательность, при этом встраивание производят добавлением псевдослучайной последовательности к выбранным вейвлет-коэффициентам, затем к цифровому изображению применяют обратное дискретное вейвлет-преобразование.

**Чем отличается:**

Задачей изобретения является разработка способа встраивания сообщения в цифровое изображение формата JPEG 2000, обеспечивающего возможность сохранения целостности внедренной информации при передаче последней по открытым каналам связи, основанного на кодировании битов встраиваемого сообщения суммой значений вейвлет-коэффициентов в блоке размером NxN из области среднечастотных и высокочастотных поддиапазонов вейвлет-преобразования. При этом выбор размера блока зависит от требований, предъявляемых к стеганосистеме. А именно, чем больше размер блока, тем выше стойкость стеганосистемы.

**Вывод:** в ходе выполнения лабораторно работы были изучены принципы работы с патентными данными