УДК 621.391

ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ СПЕКТРАЛЬНО-ПРОСТРАНСТВЕННОГО КОДИРОВАНИЯ

А.И. МИТЮХИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 9 марта 2021

Аннотация. Рассматривается подход решения задачи защиты информации путем применения методов частотного преобразования и помехоустойчивого кодирования. Показано, что предлагаемый вычислительных алгоритм на основе линейного ортогонального дискретного преобразования и низкоскоростного кодирования над полем целых чисел обеспечивает высокую степень скрытности сигнала. Метод защиты информации основывается на практическом подходе из теории информации.

Ключевые слова: обнаружение, кодирование, спектр, дискретное преобразование, скрытность, корреляция, источник, шум, полином.

Введение

Одним из основных требований при проектировании специальных инфокоммуникационных систем является эффективная и надежной защита пространственно-временного сигнала от перехвата. Современные системы перехвата включают в себя аппаратно-программные средства для спектрального анализа передаваемого сигнала и высоко производительные средства радиоразведки параметров сигнала. К таким основным параметрам относятся период излучаемого кодированного сигнала, вид модуляции, класс кодов, конкретная структура порождающей / проверочной матрицы или полинома и др. Имея достаточно мощные специальные аппаратно-программные средства, можно с высокой достоверностью решать задачи, связанные с перехватом информации. При этом необходимо учитывать вид (класс) наблюдаемой системы, когда успешному перехвату, может предшествовать решение задачи обнаружения, различения, распознавания, декодирования сигнала. Задача перехвата существенно усложняется, когда на получение необходимых энергетических, пространственных, временных, спектральных, поляризационных признаков сигналов требуются временные затраты, превосходящие сеанс перехватываемой связи.

Известно [1], требование надежной защиты может выполняется при условии применения низкоскоростных помехоустойчивых кодов. В этом случае можно уменьшить спектральную плотность мощности сигнала до величины, обеспечивающей его энергетическую скрытность. Кроме того, вероятность обнаружения сигнала усложняется, если применять сигналы, модулированные кодом с равномерным спектром в полосе частот канала.

В статье описывается вычислительный алгоритм защиты информации, где используется спектральное описание сигнала, а затем кодирование квантованных коэффициентов преобразования низкоскоростным кодом.

Теоретические принципы

Пусть сигнал с шириной спектра W передается в течении временного интервала T. Канальный параметр $q = \frac{S}{N}$ характеризует отношение средней мощности S сигнала к средней мощности $N = N_0 W$ шума на входе канала перехватчика. Шум описывается равномерным распределением плотности мощности N_0 в полосе W. Физические параметры T, W, S и N описывают основной канал. Обобщенно свойство канала можно представить в виде его геометрической интерпретации – объема

$$V = WT\frac{S}{N} = WTq. \quad (1)$$

Канал перехвата также характеризуется физическими параметрами. Перехват усложняется, если временные затраты T_c на обнаружение сигнала, выявление способов модуляции, декодирования и пр. превышают T, т.е. $T_c > T$. Поиск сигнала по частоте потребует производить частотное сканирование по несущей и тактовой частоте в канале с шумами при отношении

$$\frac{S}{N_0} \ll 1. \quad (2)$$

Очевидно, при отсутствии априорных знаний о частотных параметрах: несущей частоты и ширины спектра W (тактовой частоты) возникают дополнительные временные затраты на прием сигнала.

По аналогии с (1) свойство канала перехвата представим в виде величины его объема

$$V_c = W_c T_c q_c.$$

Для надежной передачи информации по основному каналу необходимо, чтобы выполнялось условие $V_c < V$. Возможное выполнение этого неравенства можно рассмотреть, используя два подхода.

1. Практическая стратегия надежной защиты инфокоммуникационной системы должна строится на ограничении времени t передачи открытой информации, когда $t \ll T_c$. Решение этой задачи возможно, применяя алгоритмы эффективного кодирования. Например, такие как энтропийный, универсальный, арифметический, спектральный. Недостатком первых трех является сравнительно низкая эффективность.

Пусть качестве исходного информационного источника (1D или 2D) рассматривается дискретный источник информации без памяти, где множество $\{x_1, x_2, ..., x_m\} \in X$ – это алфавит источника. Источник описывается распределением вероятностей $P = \{p_1, p_2, ..., p_m\}$, где p_i – вероятность появления символа x_i. Примем, что i-у символу источника X соответствует X_i-е информационное слово источника одиночных символов на множестве $\{1, -1\}$. Длина слова этого равномерного кода равна k. Если учитывать статистические характеристики источника (априорное знание распределения P) появляется возможность более эффективно использовать сигнал объемом V.

2. Уменьшая временной параметр объема V, появляется возможность применения метода широкополосного кодирования, т.е. увеличения значения составляющей W объема V. Свойство

$$\frac{k}{n} \ll 1 \quad (3)$$

широкополосного кода на втором этапе кодирования источника может обеспечить высокую степень информационной безопасности за счет необходимости при перехвате решать задачу обнаружения сигнала. Очевидно, увеличение объема V_c приведет к усложнению выполнения условия $V_c < V$ и решению задачи перехвата с учетом условий (2) и (3).

Спектральное кодирование. С целью обеспечения экономии вычислительных и временных ресурсов кодер источника строится с использованием ортогонального действительного дискретного преобразования Хартли (ДПХ). Ортогональный базис дискретных функций Хартли на интервале из N точек выражается числами вида [2]

$$h_v = \mathrm{cas}\left(\frac{2\pi}{N} nv\right),\ n, v \in \{0, 1, ..., N-1\},$$

где N – период дискретного сигнала $g_n = (g_0, g_1, ..., g_{N-1})$ источника. Аргументы n и v определяют соответственно временной (пространственный) и частотный (частотно-

пространственный) параметры сигнала. 1-D спектральное преобразование по всей пространственной области выполняется как [2]

$$\hat{g}_v = \frac{1}{N}\sum_{n=0}^{N-1} g_n \mathrm{cas}\left(\frac{2\pi}{N} nv\right), v \in \{0,1,...,N-1\}. \quad (4)$$

Вычисление (4) выполняется с помощью быстрого алгоритма типа БПФ. Сокращение времени передачи информации сводится к отбору коэффициентов преобразования (4) с наибольшей дисперсией. Для того, чтобы не передавать служебную информацию о номере v отобранных коэффициентов $\hat{g}_v$ предлагается использовать зональный метод отбора (фильтрации) [3]. Учитывая знание распределения вероятностей P источника X, вид ковариационной матрицы реального сигнала (например, речи, контура изображения объекта и пр.), зона фильтрации определяется через вычисление 1D- или 2D-функции распределения дисперсий компонент спектра [4]. В спектре случайного сигнала источника, как правило, имеется составляющая, соответствующая значению его математического ожидания. Компонента $\hat{g}_v$ на частоте $v = 0$ проявляется в большей степени, чем остальные составляющие спектрального образа сигнала. Поэтому преобразование (4) выполняется для процесса с нулевым математическим ожиданием.

Пространственное кодирование. Второй этап кодирования связан с выбором $[n,k,d]$- кода, обеспечивающего получение псевдослучайного потока двоичных символов и тем самым структурную скрытность. В спектральной области выбор класса кода связан с необходимостью иметь сравнительно равномерный спектр для всех форм кодовых слов кода. Возможность обнаружения кодированного сигнала сводится к минимуму, если в наблюдаемой полосе частот отсутствуют периодически повторяющие спектральные точки. Известно [5], чем меньше боковые остатки функция автокорреляции сигнала (АКФ), тем более равномерным амплитудным спектром описывается сигнал. В наибольшей степени этому условию удовлетворяет сигнал, модулированный симплексным кодом Рида-Маллера первого порядка $RM(1,k)$ [6]. Для двузначного алфавита $(1,-1)$ АКФ $r(\tau)$ имеет только два значения: $r(\tau) = 1, \quad \tau = 0$ и $r(\tau) = -\frac{1}{n}, 0 \le \tau \le n-1$. Возможность эффективного обнаружения и декодирования сигнала с малой вероятностью ошибки при энергетическом условии (2) в полосе приема практически сложно осуществить. Выбор этого кода обусловлен и тем, что при условии (3) практически восстановить порождающий полином кода не представляется возможным. Структуру полинома можно раскрыть путем решения системы линейных уравнений. Однако, это возможно при условии последовательного правильного приема всех символов сегмента кода длиной $2k$. Например, в основном канале выбран для применения $RM(1,7)$- код, вероятность ошибки в канале перехвата равна $p = 0{,}1$. Для этого условия вектор ошибок $\mathbf{E}$ имеет вес $\mathrm{wt}(\mathbf{E}) \cong 13$. Вероятность последовательного правильного приема 14-и символов близка к нулевому значению. Заметим, требование надежной передачи информации в реальных энергетически скрытных каналах предполагает работу с уровнем шума, при котором на входе приемного устройства перехвата вероятность ошибки $p \ge 0{,}1$.

Экспериментальные исследования

В качестве исходных данных, требующих эффективного описания и защиты от перехвата, использовалось бинарное изображение границы некоторого объекта интереса. После аналого-цифрового преобразования и бинаризации изображения получались пространственные данные в виде целочисленных пар (точек) декартового произведения. Число точек, описывающих границу, составляло $N = 16$. В пространственной области для описания границы требовалось 32 числа. Понижение размерности входа кодера $RM(1,k)$- кода за счет выполнения процедуры эффективного кодирования привело к значению $k = 7$. Проверка восстановления исходных данных путем вычисления обратного спектрального преобразования по 7-и коэффициентам

Хартли подтвердила получение всех 32 чисел с нулевым значением СКО. Далее осуществлялось кодирование 7-и информационных символов произвольно выбранной псевдослучайной последовательностью $[127, 7, 64]$-кода. Проведенные в работе экспериментальные исследования спектральных особенностей кода показали, что, начиная от значения $n \geq 63$ во всей полосе частот интенсивность коэффициентов Фурье равномерно уменьшается без явно проявляемых выбросов. В канале перехвата формировалась случайная аддитивная смесь сигнала и помехи в виде гауссовского процесса. При этом величина мощности помехи в полосе сигнала превышала на $(0 \div 10)$ дБ мощность сигнала. Экспериментальная оценка вероятности ошибки в канале перехвата давала значения $(2 \cdot 10^{-1} \div 4 \cdot 10^{-1})$.

Заключение

Предложенный вычислительный алгоритм защиты данных на основе кодирования в спектральной и пространственной областях позволяет получить определенную степень информационной безопасности. Не располагая сведениями о структурах порождающих полиномов кодов, перехватчик не может осуществить надежный прием информации, используя неоптимальные алгоритмы декодирования кодов. Исследования показали, что увеличение величины длины кода не приводит к резкому увеличению вероятности ошибки в канале перехвата, но приводит к уменьшению вероятности обнаружения сигнала в смеси сигнал/шум. Анализ формы спектра входного случайного процесса в канале перехвата показывает, что вероятность перехвата уменьшается при большем отношении сигнал/шум, но с условием увеличения длины кода. Дальнейшие исследования свойств алгоритма защиты могут быть продолжены, если для пространственного кодирования использовать сингулярные преобразования $RM(1, k)$-кода.

PROTECTION OF INFORMATION BASED ON SPECTRAL-SPATIAL CODING

A.I. MITSIUKHIN

Abstract. We are considering an approach to solving the problem of information protection through the use of frequency conversion methods and interference-resistant coding. It is shown that the proposed computational algorithm based on linear orthogonal discrete conversion and low-grown code over the field of whole numbers provides a high degree of stealth signal. The method of information protection is based on a practical approach from the theory of information.

Keywords: detection, coding, spectrum, discrete conversion, stealth, correlation, source, noise, polynom.

Список литературы

1. Ipatov V. // Spread Spektrum and CDMA. John Wiley & Sons, Ltd, 2005.
2. Митюхин А. // Докл. БГУИР, 2018, № 7 (117). С. 74–79.
3. Гонсалес Р, Вудс Р. Цифровая обработка изображений. М., 2005.
4. Mitsiukhin A., Pachynin V, Petrovskaya E. // Proc. 52. IWK. 2007. Vol. 2. P. 321–325.
5. Пестряков В. Б., Афанасьев В.П., Гурвиц В. Л. [и др.] Шумоподобные сигналя в системах передачи информации. М., 1973.
6. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. М., 1979.