

МЕТОД ПОСТРОЕНИЯ НЕЛИНЕЙНОГО ВЕЙВЛЕТНОГО КОДА ДЛЯ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В КАНАЛАХ СВЯЗИ

DOI: 10.36724/2072-8735-2021-15-2-26-32

Manuscript received 14 October 2020;
Accepted 02 December 2020

Кузнецов Николай Алексеевич,
 Краснодарское высшее военное училище
 имени генерала армии С.М. Штеменко,
 г. Краснодар, Россия,
cuznetsow.colia2014@yandex.ru

Ключевые слова: целостность, нелинейный код, вейвлетное преобразование, масштабирующая функция, маскирование ошибки, корректирующая способность

Предложен способ построения нелинейного вейвлетного кода (НВК) для обеспечения целостности данных в каналах связи с учетом актуальных угроз безопасности информации в современной динамической стохастической обстановке. Особое место среди методов борьбы с угрозами нарушения целостности информации занимает помехоустойчивое кодирование [1]. В статье построен эффективный в вычислительном смысле метод обеспечения целостности данных в каналах связи за счет использования нелинейных преобразований и вейвлетов. Под аппроксимацией вейвлетного преобразования понимается разделение сигнала на аппроксимирующую и детализирующую составляющие. Непрерывные и дискретные вейвлетные преобразования широко используются для анализа сигналов в современных каналах связи [2]. Множество функций, определяющих вейвлетное преобразование, принадлежит пространству квадратично-интегрируемых функций на прямой и обеспечивает необходимое условие построения конструкций нелинейных кодов на основе теории вейвлетного разложения. В процессе вейвлет-анализа происходит разложение сигнала по ортогональному базису, образованному сдвигами вейвлетной функции [2]. Отличительной чертой такого подхода является то, что свертка сигнала с вейвлетами позволяет выделить характерные особенности сигнала в области локализации этих вейвлетов. Для проведения вычислительных расчетов необходим набор коэффициентов масштабирующей функции и вейвлет. Матрица вейвлетного преобразования зависит от коэффициентов масштабирующей функции. Результаты, приведенные в статье, описывают новый подход к обеспечению целостности данных в каналах связи при помощи НВК. Представлен вычислительный пример.

Информация об авторах:

Кузнецов Николай Алексеевич, Начальник учебной лаборатории кафедры, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия;
 Аспирант заочной формы обучения в Ульяновском государственном университете (кафедра телекоммуникационных технологий и сетей)

Для цитирования:

Кузнецов Н.А. Метод построения нелинейного вейвлетного кода для обеспечения целостности данных в каналах связи // T-Comm: Телекоммуникации и транспорт. 2021. Том 15. №2. С. 26-32.

For citation:

Kuznetsov N.A. (2021) Method for constructing nonlinear wavelet code to ensure data integrity in communication channels. T-Comm, vol. 15, no.2, pp. 26-32. (in Russian)

Введение

В связи с постоянно возрастающими требованиями к надежности хранения и передачи информации по каналам связи в условиях роста активности нарушения ее целостности, перехвата, взлома и ослабления существующих средств защиты вследствие разрабатываемых новых приемов со стороны злоумышленников, появилась необходимость разработки эффективных подходов к совершенствованию процессов выявления угроз нарушения целостности.

С развитием технологий хранения и обработки данных появляются новые угрозы целостности, вследствие чего возникает необходимость в совершенствовании существующих методов защиты данных. Существует несколько факторов, в результате которых возникает несанкционированная модификация хранимой информации. Нарушение целостности данных может быть вызвано аппаратными и программными ошибками, а также действиями злоумышленников. Например, ошибка, при чтении битов в индексном дескрипторе файла может привести к тому, что файловая система перезапишет этот файл и полностью уничтожит важную информацию. Вероятность ошибок может определяться интенсивностью помех, действующих в канале связи. Различают флюктуационные, гармонические и импульсные помехи [2]. Флюктуационная помеха представляет явление, проявляющееся во времени случайным образом. Гармоническая помеха приближенно описывается синусоидальным колебанием. Эти помехи возникают в самой аппаратуре из-за проникновения в канал связи различных несущих колебаний. Импульсной помехой называется помеха, максимальное значение которой соизмеримо с амплитудой сигнала. Импульсные помехи, как правило, появляются пачками. Характер процесса появления пачек помех во времени и отдельных помех внутри одной пачки существенно изменяется в канале в различные периоды времени. Отметим, что в реальных условиях ошибки, появляющиеся в передаваемых данных в большинстве случаев коррелированы и сгруппированы в пачки. В интервалах между пачками возникают редкие независимые ошибки. Законы распределения ошибок в каналах связи исследуют преимущественно экспериментальным путем и на основании этого создают математические модели реальных каналов связи [2].

Для обеспечения целостности данных в современных высокоскоростных каналах связи используют дублирование данных, технологию виртуализации данных RAID, а также различные методы помехоустойчивого кодирования [3, 4]. Дублирование обладает малой вычислительной сложностью, но при этом большой избыточностью и, как следствие, высокой стоимостью реализации. Технология виртуализации данных RAID обладает относительно небольшой вычислительной сложностью, но является довольно затратной с точки зрения реализации в системах хранения и обработки данных. Помехоустойчивое кодирование обладает небольшой вычислительной сложностью, но при этом малой избыточностью.

Основными недостатками существующих методов обеспечения целостности данных в каналах связи является отсутствие возможности обнаружения ошибок при равномерном распределении входных значений.

Высокая избыточность также является недостатком существующих решений по обеспечению целостности данных [2-3]. Таким образом, существующие методы обеспечения целостности данных в каналах связи не в полной мере отвечают требованиям к современным устройствам передачи и хранения данных.

В результате возникает актуальная задача, связанная с разработкой новых методов обеспечения целостности данных в каналах связи, основанных на применении нелинейных кодов с большей корректирующей способностью.

Построение НВК

В настоящее время существует достаточно обширный перечень угроз целостности данных в каналах связи [1-2]. Необходимость подробной классификации угроз нарушения целостности данных обусловлена разнообразием архитектур современных средств обработки и хранения информации.

На рисунке 1 представлена классификация угроз нарушения целостности данных в каналах связи.

Целостность данных также будет нарушена в случае возникновения случайной ошибки программного или неисправности аппаратного обеспечения [3].

В виду увеличения объемов обрабатываемых данных, повышения вычислительной сложности алгоритмов функционирования программно-аппаратных средств помехоустойчивые линейные коды не в полной мере способны обеспечивать целостность данных в современных высокоскоростных каналах связи, модели которых используются в засекречивающей аппаратуре связи и аппаратуре космических радиолиний [5]. Для нейтрализации атак злоумышленников по сторонним каналам применяют нелинейные коды, обладающие максимальной вероятностью обнаружения стochастических ошибок [3]. Существенным преимуществом нелинейных кодовых конструкций является их высокая корректирующая способность.

Для разработки эффективного с точки зрения количества необходимых вычислений метода построения нелинейного кода, обеспечивающего целостность данных в современных высокоскоростных каналах связи, используем вейвлетные преобразования. Непрерывные и дискретные вейвлетные преобразования используются для анализа сигналов в каналах передачи данных. Областью применения вейвлетов являются различные высокоскоростные алгоритмы сжатия данных [2-4].

Под аппроксимацией вейвлетного преобразования будем понимать разделение сигнала $s(t)$ на аппроксимирующую $A_m(t)$ и детализирующую $D_m(t)$ составляющие. Вейвлетное преобразование примет вид [3]:

$$s_m(t) = A_m(t) + \sum_{i=1}^m D_i(t), \quad (1)$$

где m – значение уровня разделения сигнала $s(t)$, $D_i(t)$ и $A_m(t)$ – детализирующая и аппроксимирующая составляющие разделения сигнала соответственно.



Рис. 1. Классификация угроз нарушения целостности данных

Предположим, что функция $s(t)$ принадлежит пространству квадратично-интегрируемых функций на прямой $L^2(\mathbb{R})$, т.е. $\int_{-\infty}^{+\infty} |s(t)|^2 dt < \infty$. Выполнение этого условия необходимо для построения конструкций нелинейных кодов на основе теории вейвлетного разложения [4]. Подпространство функций $s(t)$, аппроксимирующих пространство $L^2(\mathbb{R})$ для определенной величины масштаба 2^m , обозначим V_m .

В результате, вейвлетное преобразование состоит из следующих отображений: $V_{m-1} \rightarrow V_m$ и $V_m \rightarrow W_m$. Такие отображения находятся в зависимости от коэффициентов масштабирующей и вейвлетной функций.

Введем следующие обозначения: φ_t — масштабирующая функция, ψ_t — вейвлетная функция, v_1, v_2, \dots, v_N — коэффициенты масштабирующей функции, w_1, w_2, \dots, w_N — коэффициенты вейвлетной функции. Вейвлетное преобразование в виде циклических матриц примет вид:

$$\begin{aligned} V_N &= cir(v_1, v_2, \dots, v_N), \\ W_N &= cir(w_1, w_2, \dots, w_N), \end{aligned} \quad (2)$$

где параметр d является сдвигом матрицы, который равен порядку используемого вейвлета, cir (Committed Information Rate) — гарантированная полоса пропускания виртуального канала [6].

В случае применения систематического помехоустойчивого кода, любое кодовое слово разделяется на информационную и избыточную части [6]. В их основе лежит построение кода при помощи вейвлет-преобразований.

В качестве информационной части кода выступает использование аппроксимирующей составляющей вейвлетного

разложения, а в качестве его избыточной части — детализирующей составляющей.

Допустим, что $\psi(t)$ и $\varphi(t)$ базисные функции, которые образуют множества $\psi_{m,k}(t)$ и $\varphi_{m,k}(t)$. Множество функций $\psi_{m,k}(t)$ и $\varphi_{m,k}(t)$ примет вид:

$$\psi_{m,k}(t) = 2^{-2/m} \cdot \psi(2^{-m} \cdot t - k), \quad (3)$$

$$\varphi_{m,k}(t) = 2^{-2/m} \cdot \varphi(2^{-m} \cdot t - k), \quad (4)$$

где m — коэффициент масштабирования базисной функции, k — величина сдвига ($m, k \in \mathbb{R}$).

Данное предположение основывается на описании пространства $L^2(\mathbb{R})$ через иерархические вложенные пространства, которые не пересекаются, а их объединение формирует пространство $L^2(\mathbb{R})$:

$$\dots \subset V_3 \subset V_2 \subset V_1 \subset V_0 \subset V_{-1} \subset V_{-2} \subset \dots \quad (5)$$

Вложенные пространства обладают следующими свойствами [6]:

1. Необходимое условие ортогональности подпространств: $\bigcap_{m \in \mathbb{Z}} V_m = 0$;
2. Необходимое условие полноты и плотности разбиения: $\bigcup_{m \in \mathbb{Z}} V_m = L^2(\mathbb{R})$;
3. Необходимое условие вложенности: $V_m \subset V_{m-1}$;
4. Сжатые версии представленной функции, как и сама функция, принадлежат подпространству V_{m-1} , т.е. $s(t) \in V_m \Leftrightarrow s(2t) \in V_{m-1}$;
5. Сдвиги функции $\varphi \in V_0$ могут быть представлены в виде: $\varphi_{0,k} = \varphi(t - k)$, $k \in \mathbb{Z}$.

В силу того, что пространства $V_0 \subset V_{-1}$ являются вложенными, а $\varphi_{-1,k}$ – ортонормированный базис пространства V_{-1} , имеет место следующее выражение:

$$\varphi_n(t) = \varphi_{0,0}(t) = \sqrt{2} \cdot \sum_{n=1}^{\infty} v_n \varphi_{-1,k}(t) = 2 \cdot \sum_{n=1}^{\infty} v_n \varphi(2t-n). \quad (6)$$

В таком представлении $v_n = \langle \varphi(t), \varphi(2t-n) \rangle$ является коэффициентом масштабирующей функции в пространстве $L^2(\mathbb{R})$, где n – величина сдвига, зависящая от порядка вейвлета, а $\langle \varphi(t), \varphi(2t-n) \rangle$ – скалярное произведение.

Далее определим коэффициенты вейвлетной функции через подпространство W_m .

Так как подпространство W_m является ортогональным дополнением пространства V_m и пространства V_{m-1} , то имеет место следующие аналитические выражения:

$$\begin{aligned} V_{m-1} &= V_m \oplus W_m; \\ \bigcap_{m \in \mathbb{Z}} W_m &= 0; \\ \bigcup_{m \in \mathbb{Z}} W_m &= L^2(\mathbb{R}). \end{aligned} \quad (7)$$

Предположим, что $\psi_0(t)$ – базисная функция пространства $W_0 \subset V_{-1}$. Тогда, аналогичным образом, получим следующее:

$$\psi_n(t) = \sqrt{2} \cdot \sum_n \omega_n \varphi_{-1,n(t)} = \sqrt{2} \cdot \sum_n \omega_n \varphi_{(2t-1)}. \quad (8)$$

В выражении (8) $w_n = \langle \psi_n(t), \varphi_z(2t-n) \rangle$ – коэффициент вейвлета, а n – величина сдвига, зависящая от порядка вейвлета. В случае применения декомпозиции сигнала [6], выражение (1) примет вид:

$$s_m(t) = \sum_k a_{n,k} \varphi_{n,k}(t) + \sum_{i=1}^m d_{i,k}(t) \psi_{i,k}. \quad (9)$$

В выражении (9) аппроксимирующими и детализирующими коэффициентами являются $a_{m,k}(t) = \langle s_m(t), \varphi_{z,k}(t) \rangle$ и $d_{i,k} = \langle s_m(t), \psi_{m,k}(t) \rangle$ соответственно.

Выражения, определяющие аппроксимирующие и детализирующие коэффициенты через масштабирующий коэффициент и вейвлетную функцию примут вид:

$$a_{m,k}(t) = \langle s_m(t), \varphi_{m,k}(t) \rangle = \sum_n v_{n-2k} \langle \varphi_m(t), \varphi_{m-1,n}(t) \rangle = \sum_n v_{n-2k} a_{n,m-1}, \quad (10)$$

$$d_{m,k}(t) = \langle s_m(t), \psi_{m,k}(t) \rangle = \sum_n \omega_{n-2k} \langle \varphi(t), \varphi_{m-1,n}(t) \rangle = \sum_n \omega_{n-2k} a_{n,m-1}. \quad (11)$$

Используя соотношения (10) и (11) получим следующее:

$$a_{m+1,k} = \sum_n v_{n-2k} a_{m,n}, \quad (12)$$

$$d_{m+1,k} = \sum_n \omega_{n-2k} a_{m,n}. \quad (13)$$

Матрица вейвлетного преобразования полностью зависит от коэффициентов масштабирующей функции [8].

Процесс реконструкции сигнала примет вид:

$$a_{m-1,k} = \sum_n (v_{n-2k} a_{m,n} + \omega_{n-2k} d_{m,n}). \quad (14)$$

Определим критерии к проверочным и порождающим матричным формам линейного вейвлетного кода. Допустим, что H и G являются проверочной и порождающей матрицами определенного линейного кода, а матричные формы соответствуют определенному типу вейвлетного преобразования. Для операции декодирования, а также обратного вейвлетного преобразования необходимо ввести следующие обозначения: \bar{V} и \bar{W} – проверочная и порождающая матричные формы. Представленные матричные формы должны соответствовать следующим условиям:

1. Условие восстановления: $V^T \cdot \bar{V} + W^T \cdot \bar{W} = I$, где I – единичная матрица.

2. Условия биортогональности.

$$\bar{V} \cdot V^T = I$$

$$\bar{W} \cdot V^T = 0.$$

В результате вейвлетного разложения первого порядка получается линейный вейвлетный код (ЛВК) [8]. Информационную часть этого кода обозначим $v = (v_1, v_2, \dots, v_k)$. Такая информационная часть представляет последовательность элементов поля $GF(q)$. Избыточную часть кода обозначим $r = (r_1, r_2, \dots, r_{N/2})$. Множество кодовых слов ЛВК задается с помощью проверочной и порождающей матриц [6-8]. Преобразования имеют вид: порождающая матрица ЛВК $G = V^T + a \cdot W^T \cdot J$, проверочная матрица ЛВК $G = \bar{V}^T + b \cdot J^T \cdot \bar{W}^T$ ($a, b \in GF(q)$). Помимо этого они должны удовлетворять условию: $\bar{a} \cdot \bar{b} = (p-1) \bmod p$, $p \in GF(q)$ где $J = cir(0, 1, 0, \dots, 0)$ – соответствующая матрица размером $N/2 \times N/2$.

Полученный в результате приведенных последовательных итераций код является циклическим ЛВК.

Предположим, что над полем $GF(q)$ существует некоторый двоичный ЛВК C . Тогда проверочная матрица примет вид:

$$G = \bar{V}^T + \bar{b} \cdot J^T \cdot \bar{G}^T, \quad (15)$$

где $J = cir(0, 1, 0, \dots, 0)$ – матричная форма размерности $N/2 \times N/2$.

Введем следующие обозначения: r – избыточная часть кода, v – линейная часть. Тогда процесс кодирования схематично может быть представлен рис. 2.

Полученный код будет состоять из выражений вида (x, r^{-1}) , а вероятность маскирования ошибки может быть определена по формуле $P_M = 2^{N/2}$, $M \in [1; +\infty)$.

СВЯЗЬ

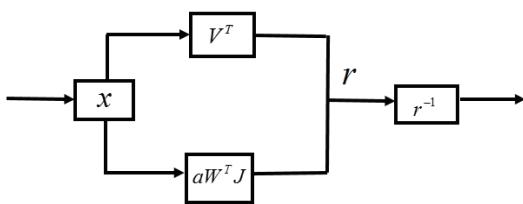


Рис. 2. Процесс кодирования на основе вычисления мультипликативного обратного в поле $GF(q)$

В случае, если осуществляется вычисление куба в поле $GF(q^k)$ для r избыточных бит, процесс формирования НВК схематично может быть представлен на рис. 3.

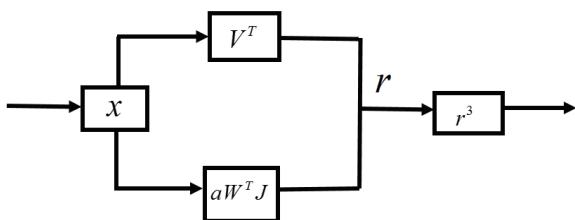


Рис. 3. Процесс кодирования, осуществляемый при помощи вычислений куба в поле $GF(q^k)$ на основе избыточной части

Вероятность маскирования в этом случае может быть определена по формуле $P_M = 2^{N/4}$.

ВЫЧИСЛИТЕЛЬНЫЙ ПРИМЕР

Допустим, что необходимо осуществить вычисление вероятности маскировки ошибки P_M в случае неравномерного распределения входных кодовых слов. Используем НВК с параметрами $n = 5$, $k = 4$. Функция кодирования НВК примет форму:

$$c_5 = c_1c_2 \oplus c_1c_3 \oplus c_1c_4 \oplus c_3c_4,$$

где c_1, c_2, c_3, c – информационные биты, c_5 – проверочный бит. Ошибки и кодовые слова представлены в табл. 1.

Пусть кодовые слова $\{0;2;4;6;9;11;13;15\}$ имеют высокую вероятность появления на входе устройства кодирования. В этом случае вероятность появления ошибки 01000 достигает своего максимального значения. Рассмотрим преобразование Грэя наиболее вероятных кодовых слов в некоторое множество $\{0,2,4,6,9,11,13,15\}$:

$$\begin{aligned} 00000(0) &\rightarrow 00000(0); \quad 00010(2) \rightarrow 00011(3); \\ 00100(4) &\rightarrow 00110(6); \quad 00110(6) \rightarrow 00101(5); \\ 01001(9) &\rightarrow 01101(13); \quad 01011(11) \rightarrow 01110(15); \\ 01101(13) &\rightarrow 01011(11); \quad 01110(15) \rightarrow 01001(9). \end{aligned}$$

Далее рассмотрим, как изменилось распределение вероятности маскировки ошибки после преобразования Грэя. В таблице 1 $Q(e)$ обозначает вероятность маскировки ошибки в случае неравномерного распределения входных кодовых слов, а $Q_G(e)$ – вероятность маскировки ошибки после преобразования Грэя.

В результате максимальное значение вероятности маскировки ошибки снизилось. Разработанная модель тестировалась для различных случаев неравномерного распределения входных кодовых слов.

Таблица 1

Вероятность маскировки ошибки

Ошибка	Целочисленное представление входных кодовых слов	$Q(e)$	$Q_G(e)$
00000	Все векторы	1	1
00001		0	0
00010	0, 1, 6, 7, 10, 11, 12, 13	0,5(1-e)	0,5(1-e)
00011	2, 3, 4, 5, 8, 9, 14, 15	0,5(1-e)	0,5(1-e)
00100	0, 2, 4, 6, 8, 10, 12, 14	0,5(1-e)	0,25(1-e)
00101	1, 3, 5, 7, 9, 11, 13, 15	0,5(1-e)	0,75(1-e)
00110	1, 2, 4, 7, 8, 11, 13, 14	0,5(1-e)	0,25(1-e)
00111	0, 3, 5, 6, 9, 10, 12, 15	0,5(1-e)	0,75(1-e)
01000	0, 2, 4, 6, 9, 11, 13, 15	1-e	0,75(1-e)
01001	1, 3, 5, 7, 8, 10, 12, 14	e	0,25(1-e)
01010	1, 2, 4, 7, 9, 10, 12, 15	0,5(1-e)	0,25(1-e)
01011	0, 3, 5, 6, 8, 11, 13, 14	0,5(1-e)	0,75(1-e)
01100	0, 1, 2, 3, 4, 5, 6, 7	0,5(1-e)	0,5(1-e)
01101	8, 9, 10, 11, 12, 13, 14, 15	0,5(1-e)	0,5(1-e)
01110	0, 1, 6, 7, 8, 9, 14, 15	0,5(1-e)	0,5(1-e)
01111	2, 3, 4, 5, 10, 11, 12, 13	0,5(1-e)	0,5(1-e)
10000	0, 2, 5, 7, 8, 10, 13, 15	0,5(1-e)	0,5(1-e)
10001	1, 3, 4, 6, 9, 11, 12, 14	0,5(1-e)	0,5(1-e)
10010	1, 2, 5, 6, 8, 11, 12, 15	0,5(1-e)	0,5(1-e)
10011	0, 3, 4, 7, 9, 10, 13, 14	0,5(1-e)	0,5(1-e)
10100	0, 1, 2, 3, 8, 9, 10, 11	0,5(1-e)	0,5(1-e)
10101	4, 5, 6, 7, 12, 13, 14, 15	0,5(1-e)	0,5(1-e)
10110	0, 1, 4, ,5, 10, 11, 14, 15	0,5(1-e)	0,5(1-e)
10111	2, 3, 6, 7, 8, 9, 12, 13	0,5(1-e)	0,5(1-e)
11000	4, 5, 6, 7, 8, 9, 10, 11	0,5(1-e)	0,5(1-e)
11001	0, 1, 2, 3, 12, 13, 14, 15	0,5(1-e)	0,5(1-e)
11010	2, 3, 6, 7, 10, 11, 14, 15	0,5(1-e)	0,5(1-e)
11011	0, 1, 4, 5, 8, 9, 12, 13	0,5(1-e)	0,5(1-e)
11100	1, 3, 4, 6, 8, 10, 13, 15	0,5(1-e)	0,5(1-e)
11101	0, 2, 5, 7, 9, 11, 12, 13	0,5(1-e)	0,5(1-e)
11110	0, 3, 4, 7, 8, 11, 12, 15	0,5(1-e)	0,5(1-e)
11111	1, 2, 5, 6, 9, 10, 13, 14	0,5(1-e)	0,5(1-e)

В таблице 2 представлено сравнение вероятности маскировки ошибки при использовании преобразования Грэя и без него для разных параметров кодовых значений (n – длина кода, k – количество информационных символов).

Таблица 2
Сравнение вероятности маскировки ошибки

Параметры вейвлетного кода	$\max Q(e)$	$\max Q_G(e)$
$n = 5, k = 4$	0,71	0,59
$n = 10, k = 8$	0,69	0,57
$n = 20, k = 16$	0,79	0,68

В виду использования вычисления кубов избыточной части, а также вычисления мультипликативного обратного в поле $GF(q^k)$, скорость представленных кодов меньше, чем скорость у известных линейных кодов. Разработанные конструкции кодов, обладают преимуществом по сравнению с существующими конструкциями линейных кодов, а именно: максимальной вероятностью обнаружения маскировки ошибки и лучшей корректирующей способностью.

Заключение

В статье предложен метод построения НВК при помощи вейвлетных преобразований, приведены его основные преимущества и недостатки. Определены критерии к проверочным и порождающим матричным формам. Приведен вычислительный пример, демонстрирующий максимальную вероятность обнаружения маскирования стохастических ошибок при применение конструкций НВК.

Разработанный НВК уступает в скорости известным конструкциям линейных кодов, однако в связи с возрастающи-

ми требованиями к программно-аппаратному обеспечению, а также увеличивающейся вычислительной сложности алгоритмов их функционирования, использование НВК становится актуальным. НВК могут применяться для обеспечения целостности данных, передаваемых по высокоскоростным закрытым каналам связи космических радиолиний [4]. НВК обладает лучшей корректирующей способностью в сравнении с известными конструкциями линейных кодов.

Литература

1. Клод Шеннон. Теория информации. Математическая теория связи. М.: Издательство иностранной литературы, 1963. 211 с.
2. Cramer R. Dodis Y. Fehr S. Detection of Algebraic Manipulation with Application to robust secret sharing and fuzzy extractors // Proceeding of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology. 2008. Р. 471-488.
3. Добеши И. Десять лекций по вейвлетам. Ижевск: НИЦ Регулярная стохастическая динамика, 2001. 464 с. 68.
4. Чуи Ч. Введение в вейвлеты. М.: Мир, 2001. Р. 412.
5. Moldovyan N. Levina A. Taranov S. Symmetric Encyption for Error Correction // Proceedings of the 20th Conference of Open Innovations Association FRUCT. 2017. Р. 1-12.
6. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир. 1986. 576 с.
7. Аверилл М. Лоу, В. Дэвид Кельтон. Имитационное моделирование. Классика CS. 3-е издание. СПб: Питер. Издательская группа BHV, 2004. 847 с.
8. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. 2-изд., перераб. и доп. М.: Наука. Гл. ред. физ.-мат. лит. 1987. 336 с.

METHOD FOR CONSTRUCTING NONLINEAR WAVELET CODE TO ENSURE DATA INTEGRITY IN COMMUNICATION CHANNELS

Nikolay A. Kuznetsov, Krasnodar higher military school named after General of the army S. M. Shtemenko, Krasnodar, Russia,
cuznetsow.colia2014@yandex.ru

Abstract

A method for constructing a nonlinear wavelet code (NVC) to ensure data integrity in communication channels, taking into account current threats to information security in a modern dynamic stochastic environment, is proposed. A special place among the methods of combating threats to the integrity of information is occupied by noise-resistant encoding. The article presents a computationally effective method for ensuring data integrity in communication channels by using nonlinear transformations and wavelets. The approximation of the wavelet transform refers to the division of the signal into approximating and detailing components. Continuous and discrete wavelet transforms are widely used [2] for signal analysis in modern communication channels. The set of functions defining the wavelet transform belongs to the space of square-integrable functions on a straight line and provides a necessary condition for constructing constructions of nonlinear codes based on the theory of wavelet decomposition. As is known, in the process of wavelet analysis, the signal is decomposed along the orthogonal basis formed by shifts of the wavelet function. A distinctive feature of this approach is that convolution of the signal with wavelets allows us to identify the characteristic features of the signal in the area of localization of these wavelets. To perform computational calculations, you need a set of scaling function coefficients and a wavelet. The wavelet transform matrix depends on the coefficients of the scaling function. The results presented in the article describe a new approach to ensuring data integrity in communication channels using nvc. A computational example is presented.

Keywords: integrity, nonlinear code, wavelet transform, scaling function, error masking, correcting ability

References

1. Claude Shannon (1963). Information the y. Mathematical theory of communication. The foreign literature publishing house. 211 p.
2. R. Cramer, Y. Dodis, S. Fehr (2008). Detection of Algebraic Manipulation with Application to robust secret sharing and fuz extractors // Proceeding of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology. P. 471-488.
3. I. Daubechies (2001). en lectures on wavelets. - Izhevsk: SIC Regular ihaotic dynamics, 2001. 464 p.
4. C.H. Chui (2001). Introduction to wavelets. Moscow: Mir. 412
5. N. Moldovyan, A. Levina, S. aranov (2017). Symmetric Encryption for Error Correction. Proceedings of the 20th Conference of Open Innovations Association FRUCT. P. 1-12.
6. R. Bleichut (1986). The y and practice of error-controlling codes. Moscow: Mir. 576 p.
7. Averill M. Lowe, V. David Kelton (2004). "Simulation modeling". Classic CS. 3rd edition. SPb: Peter. BHV publishing group. 847 p.
8. B.V. Gnedenko, I.N. Kovalenko (1987). Introduction to the theory of mass service. 2nd ed. Moscow: Nauka. GL. ed. Fiz. - Mat. lit. 336 p.