



## ДЕТЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИГНАЛОВ НА ОСНОВЕ РЕКОНСТРУКЦИИ ДИНАМИЧЕСКИХ СИСТЕМ И ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

*А.Н. Павлов*

Предлагается метод выделения передаваемых сообщений из хаотического несущего сигнала на основе сочетания техники реконструкции динамических систем и дискретного вейвлет-преобразования. Показано, что применение дискретных вейвлетов позволяет существенно повысить помехоустойчивость алгоритма детектирования, использующего принцип реконструкции.

### Введение

Защита информации при ее передаче по каналу связи является одной из проблем, особенно актуальных в период активного развития современных информационных технологий. Обеспечение защиты передаваемых сообщений является важным, в частности, при проведении банковских операций, передаче паролей и идентификационных кодов (в том числе, через интернет) и т.д. Одним из новых способов решения данной проблемы является применение для передачи сообщений широкополосных хаотических сигналов. Интенсивные исследования в этом направлении ведутся с начала 1990-х годов. В самых первых работах было предложено использовать явление хаотической синхронизации для выделения информационного сигнала из хаотического несущего. Предлагались два конкретных способа решения проблемы, основанных на использовании идентичных генераторов хаоса в передающем и приемном устройствах: аддитивное добавление информационного сообщения к несущему сигналу [1–3] и модуляция параметров генератора хаоса [4–6]. Позднее была рассмотрена задача многоканальной защищенной передачи информации на основе так называемого феномена «автосинхронизации», то есть использования систем с автоматической подстройкой параметров [7, 8]. Первые серьезные успехи были связаны с тем, что для ряда модельных схем была продемонстрирована возможность передачи цифровых и аналоговых сообщений с использованием хаотических сигналов. В схеме с нелинейным подмешиванием информационного сигнала в хаотический, передача речевых и музыкальных сигналов в низкочастотном и в радиодиапазонах была продемонстрирована экспериментально в работе [9].

Установлено, что методы, основанные на явлении синхронизации, имеют ряд недостатков, наиболее существенным из которых является требование идентично-

сти генераторов хаотических колебаний в приемнике и передатчике. Если параметры соответствующих генераторов будут отличаться более чем на 1–2%, то данные методы становятся неэффективными [10]. Разработка новых, более «практичных» способов защиты информации, передаваемой по каналу связи, на протяжении многих лет проводится отечественными учеными (можно отметить, в частности, работы по данной тематике группы А.С. Дмитриева [9–11], а также работы, проводившиеся в СГУ [12, 13]). Главные принципы, лежащие в основе существующих разработок, базирующихся на использовании хаотических колебаний в качестве несущих сигналов, заключаются в следующем.

1. Использование генератора хаотических сигналов в передающем устройстве позволяет обеспечить одновременную передачу нескольких независимых сообщений по одному каналу связи, например, путем модуляции параметров данного генератора. В отличие от классических методов (амплитудная, частотная модуляция), информационные сообщения могут передаваться путем модуляции параметров, характеризующих различные детали сложной формы хаотического несущего сигнала. В частности, в работах [14, 15] была продемонстрирована возможность одновременной передачи 3-х независимых сообщений в одном несущем и их достоверного выделения при проведении демодуляции.

2. Процедура выделения информационных сообщений из хаотического несущего сигнала невозможна без точного знания характеристик генератора хаотических колебаний в передающем устройстве, что обеспечивает высокую степень защищенности передаваемой информации. В настоящее время существует несколько базовых моделей генераторов хаоса, однако для проведения демодуляции необходимо знать не только, какая именно базовая модель используется, но и точный вид характеристики нелинейного элемента, которая может быть задана индивидуально для каждого генератора, и определить ее путем простого перебора разных вариантов в общем случае невозможно.

В рамках данной работы предлагается метод выделения передаваемых сообщений из хаотического несущего сигнала, основанный на сочетании техники глобальной реконструкции динамических систем (ДС) и дискретного вейвлет-преобразования. Первоначальная идея метода была предложена несколько лет назад в работах [16, 17]. Проведенные исследования продемонстрировали, что этот подход является достаточно универсальным и в то же время весьма простым. По аналогии с известными работами в данной области рассматривается возможность передачи информационных сообщений в хаотическом несущем сигнале путем модуляции параметров генератора хаоса. Принципиальное отличие состоит в способе детектирования. Использование техники реконструкции в сочетании с дискретными вейвлетами вместо феномена «автосинхронизации» и ряда других известных методов позволяет полностью устранить проблемы, связанные с неидентичностью генераторов в приемном и передающем устройствах, что является одним из очевидных преимуществ предлагаемого подхода.

### **1. Выделение информационных сообщений из хаотического несущего сигнала на основе реконструкции динамических систем**

Использование реконструкции для детектирования сообщений впервые обсуждалось в работах [18, 19], авторы которых продемонстрировали возможность выделения одного аддитивного воздействия на генератор хаотических колебаний при нали-

ции априорной информации о структуре математической модели генератора и о том, каким образом подается внешнее воздействие (то есть как оно вводится в уравнения, описывающие динамику генератора). В работах [16, 17] был предложен более универсальный способ, позволяющий осуществлять детектирование информационных сигналов, осуществляющих модуляцию параметров ДС. Развитие идей реконструкции неавтономных систем было предпринято в [20–22].

Рассмотрим возможность детектирования информационных сообщений на примере генератора хаотических колебаний, моделируемого системой обыкновенных дифференциальных уравнений

$$\frac{d\vec{x}}{dt} = \vec{F}(\vec{x}, \vec{\mu}^0), \quad \vec{x} \in R^n, \quad \vec{\mu}^0 \in R^l, \quad (1)$$

в которой  $\vec{x}$  – вектор состояния,  $\vec{F}$  – вектор правых частей модельной системы,  $\vec{\mu}^0$  – вектор постоянных значений параметров.

Будем осуществлять относительно медленную модуляцию произвольного числа параметров информационными сигналами  $\mu_i(t)$ , то есть введем в рассмотрение переменные величины

$$\mu_i^* = \mu_i^0 + \mu_i(t), \quad (2)$$

что позволит реализовать одновременную передачу нескольких сообщений. В этом случае передаваемый по каналу связи сигнал, представляющий собой одномерную реализацию колебательного процесса генератора хаоса, порождается неавтономной динамической системой вида

$$\frac{d\vec{x}}{dt} = \vec{F}(\vec{x}, \vec{\mu}^0 + \vec{\mu}(t)). \quad (3)$$

Для решения задачи синтеза ДС по наблюдаемой одномерной реализации система (1) должна быть сведена к виду

$$\begin{aligned} \frac{dx_1}{dt} &= x_2, \\ \frac{dx_2}{dt} &= x_3, \\ &\dots\dots \\ \frac{dx_n}{dt} &= f(x_1, x_2, \dots, x_n, \vec{\mu}). \end{aligned} \quad (4)$$

Это значит, что путем замен переменных необходимо преобразовать правые части таким образом, чтобы вместо вектор-функции  $\vec{F}$  осталась только одна скалярная нелинейная функция  $f$ .

Многие базовые модели динамического хаоса (системы Лоренца, Ресслера, модифицированный генератор с инерционной нелинейностью и другие) удовлетворяют этому требованию. Поскольку информационные сигналы обычно являются медленными по сравнению с несущим, можно ввести в рассмотрение интервал времени  $t^*$ , в течение которого значения параметров допустимо считать практически постоянными: для времен порядка  $t^*$  можно не учитывать неавтономность системы (3). Это

дает возможность восстановления текущих значений параметров системы по коротким участкам ее одномерной реализации, то есть воспроизведения информационных сигналов  $\mu_i(t)$ , осуществляющих параметрическую модуляцию генератора хаоса.

Применяя технику реконструкции к одномерной реализации  $x_1(t)$  генератора хаоса, которую можно измерить на выходе передающего устройства, получатель информации, зная общий вид математической модели (1), выделяет полезные сигналы  $\mu_i(t)$ . С этой целью ему необходимо  $n$  раз продифференцировать реализацию  $x_1(t)$ , что позволит определить левые части модельной системы (4). В результате задача определения значений параметров в данный момент времени сводится к необходимости решения алгебраических уравнений с некоторым количеством неизвестных. Поскольку при компьютерной обработке приходится иметь дело не с аналоговым сигналом, а с дискретизованной временной зависимостью  $x_1(i\Delta t)$ , производные определяются в моменты времени  $i\Delta t$  по приближенным формулам численного дифференцирования. Записывая систему  $K$  алгебраических уравнений ( $K = [t^*/\Delta t]$ ) для  $L$  неизвестных ( $L \ll K$ ) и решая ее методом наименьших квадратов, можно осуществить аппроксимацию неизвестных коэффициентов.

Выберем в качестве модельной системы (1) модифицированный генератор с инерционной нелинейностью (ГИН) [23]

$$\begin{aligned}\frac{dx}{dt} &= m_0x + y - xz, \\ \frac{dy}{dt} &= -x, \\ \frac{dz}{dt} &= -g_0z + 0.5g_0(x + |x|)x.\end{aligned}\tag{5}$$

Полагая, что излучаемым сигналом генератора является одномерная реализация  $y(t)$ , осуществим преобразование системы уравнений (5) к виду (4) путем замен переменных

$$Y = y, \quad Z = -x, \quad X = -m_0x - y + xz,\tag{6}$$

в результате которых уравнения генератора приобретают вид

$$\begin{aligned}\frac{dY}{dt} &= Z, \\ \frac{dZ}{dt} &= X, \\ \frac{dX}{dt} &= f(X, Y, Z, \vec{\mu}), \quad \vec{\mu} = (m_0, g_0), \\ f &= \frac{X(X + Y)}{Z} + (m_0g_0 - 1)Z - g_0(X + Y) + 0.5g_0(|Z| - Z)Z^2.\end{aligned}\tag{7}$$

Проиллюстрируем с помощью модели ГИНа возможность одновременной передачи двух независимых информационных сигналов по одному каналу связи. С этой целью параметр  $m_0$  модулировался широкополосным хаотическим сигналом, а параметр  $g_0$  – гармоническим сигналом. В системе (5) были выбраны следующие значения

постоянных величин:  $g_0 = 0.2$ ,  $m_0 = 1.5$ . Для проверки эффективности метода с точки зрения его помехоустойчивости осуществлялось добавление нормально распределенной случайной величины с дисперсией  $10^{-3}$  к информационным сигналам, осуществляющим параметрическую модуляцию, и  $10^{-4}$  – аддитивно к несущему хаотическому сигналу. Зависимости во времени параметров  $m^*$  и  $g^*$  данной системы проиллюстрированы на рис. 1, *а*, *б*. Получатель информации, зная вид нелинейной функции  $f$  в системе (7), принимая сигнал (рис. 1, *в*), восстановит сигналы модуляции (рис. 1, *з*, *д*).

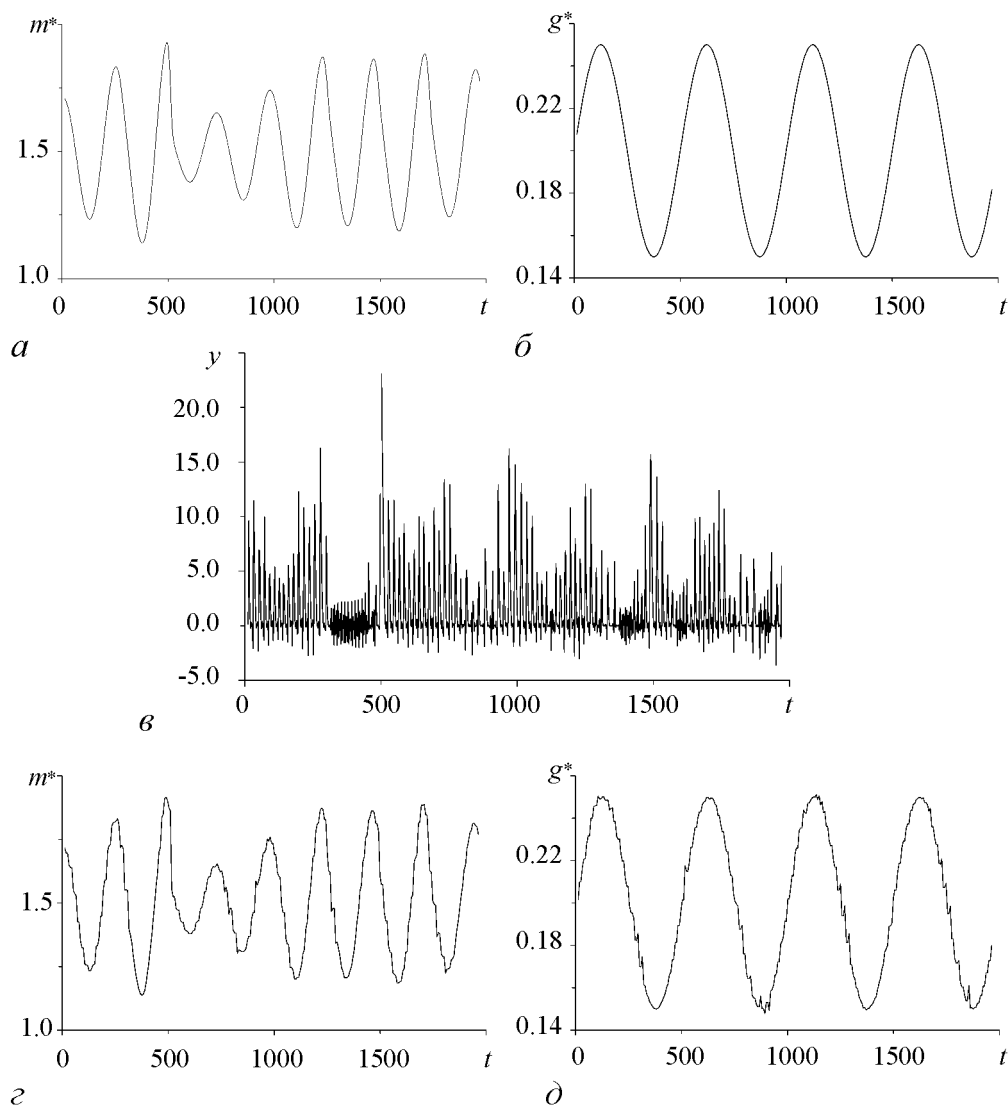


Рис. 1. Пример детектирования на основе техники реконструкции: *а*, *б* – передаваемые сигналы, осуществляющие модуляцию параметров генератора хаотических колебаний; *в* – сигнал в канале связи; *з*, *д* – сигналы, выделенные из хаотического несущего

Дальнейшие исследования проводились на модели Ресслера

$$\begin{aligned}\frac{dx}{dt} &= -(y + z), \\ \frac{dy}{dt} &= x + ay, \\ \frac{dz}{dt} &= b + z(x - c).\end{aligned}\tag{8}$$

Выбрав в качестве несущего сигнала координату  $y(t)$  данной модели, путем замен переменных

$$Y = y, \quad Z = x + ay, \quad X = ax + (a^2 - 1)y - z\tag{9}$$

преобразуем систему уравнений (8) к виду

$$\begin{aligned}\frac{dY}{dt} &= Z, \\ \frac{dZ}{dt} &= X, \\ \frac{dX}{dt} &= -b + (a - c)X - cY + (ac - 1)Z - aY^2 - \\ &\quad - aZ^2 - aXY + XZ + (a^2 + 1)YZ.\end{aligned}\tag{10}$$

Как было показано в [14, 15], существует возможность передавать одновременно, по крайней мере, три информационных сигнала в одном несущем. Теоретически, метод детектирования на основе реконструкции ДС не накладывает ограничений на количество одновременно меняемых параметров. На практике такие ограничения появляются в связи с конечной точностью вычисления  $\mu_i^*$ . К числу достоинств рассматриваемого способа детектирования относятся следующие.

1. Наличие только одного генератора хаотических сигналов, расположенного в приемном устройстве, и отсутствие проблемы идентичности генераторов приемника и передатчика, являющейся одной из ключевых для систем, использующих принцип синхронизации колебаний.

2. Широкая полоса частот для передачи информационных сообщений. По этому параметру рассматриваемый способ детектирования, как минимум, не уступает принципам детектирования в системах, основанных на эффекте синхронизации хаоса (в случае передачи информационных сигналов путем модуляции управляющих параметров). Реконструкция ДС позволяет проводить оценку параметров по очень коротким участкам переходных процессов, составляющим, например, 1/5 часть базового периода несущего сигнала или даже меньше. Из-за наличия очень большого числа вариантов схем передачи информации, базирующихся на использовании хаотических несущих сигналов, детальное сопоставление технических характеристик каждой из них является отдельной и весьма трудоемкой задачей (которая выходит за рамки настоящей работы). Отметим, что простое сравнение результатов, представленных в статьях [16] и [8] для одновременной передачи двух информационных сигналов (сопоставление отношений частот модуляции и несущего сигнала), демонстрирует, что для рассмотренных примеров подход, основанный на технике реконструкции, обеспечивает почти в 2 раза более широкую полосу частот для передачи

информации. Разумеется, в данном случае речь идет о простом наблюдении, и для того, чтобы проводить более детальное сопоставление технических характеристик, необходимы специальные сравнительные исследования.

Главным (и очень серьезным!) недостатком алгоритма детектирования, базирующегося на реконструкции ДС, является необходимость дифференцирования сигналов, которые на практике всегда являются зашумленными. Вычисление производных при наличии аддитивного шума приводит к существенным ошибкам. Для их уменьшения первоначально [16] было предложено использовать трехступенчатую фильтрацию: фильтрация несущего сигнала в предположении, что сигнал и шум разделены в частотной области (1-й этап), применение метода наименьших квадратов для получения усредненных значений параметров в пределах малого временного окна (2-й этап), сглаживание выделенных сигналов модуляции с учетом медленного изменения параметров по сравнению с несущим хаотическим сигналом (3-й этап). Тем не менее, наличие шума в исходном процессе остается наиболее серьезной проблемой с точки зрения практической реализации метода демодуляции, основанного на технике реконструкции ДС. В данной работе предлагается способ решения этой проблемы путем сочетания техники глобальной реконструкции и дискретного вейвлет-преобразования. К числу достоинств теории вейвлетов относится возможность устранения некорректности операции дифференцирования зашумленных временных рядов путем перехода в пространство вейвлет-коэффициентов.

## 2. Дифференцирование сигналов с применением дискретных вейвлетов

Свойство дифференцирования вейвлет-преобразования можно записать следующим образом [24]:

$$W [\partial_t^p f] = (-1)^p \int_{-\infty}^{\infty} f(t) \partial_t^p [(\psi_{ab}^*(t))] dt. \quad (11)$$

Формула (11) означает, что вместо того, чтобы дифференцировать  $p$  раз сигнал  $f(t)$ , можно продифференцировать  $p$  раз анализирующий вейвлет. Это очень полезное свойство при работе с экспериментальными данными, поскольку функция  $f(t)$  представляет собой ряд чисел (и содержит шум), а анализирующий вейвлет задан формулой (в случае непрерывного вейвлет-преобразования).

С точки зрения непосредственно процедуры вычисления производных функции  $\psi_{ab}^*(t)$  проще пользоваться непрерывными вейвлет-базисами, позволяющими получать аналитические выражения для  $\partial_t^p [(\psi_{ab}^*(t))]$ , что очевидно, например, для базисов, сконструированных на основе производных функции Гаусса,

$$\psi_p(t) = (-1)^p \partial_t^p \left[ \exp \left( -\frac{t^2}{2} \right) \right]. \quad (12)$$

В то же время непрерывное вейвлет-преобразование имеет ряд недостатков в случае его использования при решении задачи определения параметров ДС. Дело в том, что базисы на основе непрерывных вейвлетов, строго говоря, не являются ортонормированными [25, 26], тогда как дискретные вейвлеты приводят к более точному обратному восстановлению сигнала, например, после процедуры сжатия данных.

Для дискретных вейвлетов легче вычислить обратное преобразование, несмотря на то, что они не могут быть записаны в аналитической форме (за исключением Хаар-вейвлета). Дискретные вейвлеты обеспечивают существенный выигрыш в скорости проведения вычислений в рамках процедуры быстрого преобразования, что является одним из важных преимуществ при их использовании для передачи информации (например, в рамках формата видеоданных MPEG).

Прекрасная обзорная статья по теории дискретных вейвлетов была опубликована в 2001 году в «Успехах физических наук» [27]. Приведем некоторые основные сведения, которые потребуются нам в дальнейшем.

При дискретном вейвлет-анализе сигнала  $f(t)$  рассматриваются *скейлинг-функция* (или *масштабная функция*)  $\varphi(t)$  и *базисный вейвлет*  $\psi(t)$ , определяемые следующим образом:

$$\begin{aligned}\varphi(t) &= \sqrt{2} \sum_{k=0}^{2M-1} h_k \varphi(2t - k), \\ \psi(t) &= \sqrt{2} \sum_{k=0}^{2M-1} g_k \varphi(2t - k), \\ g_k &= (-1)^k h_{2M-k-1},\end{aligned}\tag{13}$$

где  $h_k$  – коэффициенты. Масштабирование и смещение указанных функций задаются выражениями

$$\begin{aligned}\varphi_{j,k} &= 2^{j/2} \varphi(2^j t - k), \\ \psi_{j,k} &= 2^{j/2} \psi(2^j t - k).\end{aligned}\tag{14}$$

В рамках *многомасштабного* анализа функции  $\varphi_{j,k}$  и  $\psi_{j,k}$  служат высокочастотными и низкочастотными фильтрами, соответственно. Из общих свойств скейлинг-функций и вейвлетов однозначно определяются коэффициенты  $h_k$ . Пример их вычисления для вейвлета Добеши ( $D^4$ ) приведен в [27].

Применение вейвлетов упрощает исследование многих математических операторов, что позволяет решать с их помощью дифференциальные уравнения. Рассмотрим в качестве иллюстрации оператор дифференцирования 1-го порядка. Основываясь на матричном представлении, рассмотренном в работе [27], запишем следующее выражение для матричного элемента оператора:

$$\tau_l = \int_{-\infty}^{\infty} \varphi(t) \frac{d}{d\tau} \varphi(t - l) dt.\tag{15}$$

С учетом (13) получим

$$\begin{aligned}\tau_l &= \int_{-\infty}^{\infty} \sum_{j=0}^{2M-1} h_j \varphi(2t + j) \frac{d}{d\tau} \left[ \sum_{k=0}^{2M-1} h_k \varphi(2t - 2l + k) \right] dt = \\ &= \sum_{j=0}^{2M-1} \sum_{k=0}^{2M-1} h_j h_k \int_{-\infty}^{\infty} \varphi(2t + j) \frac{d}{d\tau} \varphi(2t - 2l + k) dt = \\ &= \sum_{j=0}^{2M-1} \sum_{k=0}^{2M-1} h_j h_k \tau_{2l-k+j}.\end{aligned}\tag{16}$$



Это уравнение связывает матричные элементы на соседних уровнях. Для вейвлетов Добеши ( $D^4$ ) получим следующее матричное уравнение:

$$\begin{bmatrix} \tau_{-3} & \tau_{-2} & \tau_{-1} & \tau_0 & \tau_1 & \tau_2 & \tau_3 \end{bmatrix}^T = \quad (17)$$

$$= \begin{bmatrix} \sum h_i h_{i+3} & 0 & 0 & 0 & 0 & 0 & 0 \\ \sum h_i h_{i+1} & \sum h_i h_{i+2} & \sum h_i h_{i+3} & 0 & 0 & 0 & 0 \\ \sum h_i h_{i-1} & \sum h_i h_i & \sum h_i h_{i+1} & \sum h_i h_{i+2} & \sum h_i h_{i+3} & 0 & 0 \\ \sum h_i h_{i-3} & \sum h_i h_{i-2} & \sum h_i h_{i-1} & \sum h_i h_i & \sum h_i h_{i+1} & \sum h_i h_{i+2} & \sum h_i h_{i+3} \\ 0 & 0 & \sum h_i h_{i-3} & \sum h_i h_{i-2} & \sum h_i h_{i-1} & \sum h_i h_i & \sum h_i h_{i+1} \\ 0 & 0 & 0 & 0 & \sum h_i h_{i-3} & \sum h_i h_{i-2} & \sum h_i h_{i-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & \sum h_i h_{i-3} \end{bmatrix} \begin{bmatrix} \tau_{-3} \\ \tau_{-2} \\ \tau_{-1} \\ \tau_0 \\ \tau_1 \\ \tau_2 \\ \tau_3 \end{bmatrix}.$$

При вычислении первой производной  $\tau_{-j} = -\tau_j$  [27]. Решение матричного уравнения позволяет вычислить элементы оператора дифференцирования. По аналогии можно определить матричные элементы дифференциальных операторов более высоких порядков. Пример вычислений для базиса вейвлетов Добеши ( $D^8$ ) представлен в таблице (расчеты приведены из работы [27]). В исследованиях, проводимых в рамках данной работы, использовались коэффициенты  $h_k$  и матричные элементы операторов дифференцирования, вычисленные с высокой точностью (64 разряда) сотрудниками Отделения теоретической физики ФИАН и любезно предоставленные О.В. Ивановым.

Таблица

$k$	$h_k$	$\tau_k$
-6	0	0.00000084
-5	0	-0.00017220
-4	0	-0.00222404
-3	0	0.03358020
-2	-0.07576571	-0.19199897
-1	-0.02963552	0.79300950
0	0.49761866	0
1	0.80373875	-0.79300950
2	0.29785779	0.19199897
3	-0.09921954	-0.03358020
4	-0.01260396	0.00222404
5	0.03222310	0.00017220
6	0	-0.00000084

### 3. Детектирование информационных сигналов с использованием дискретных вейвлетов

Вернемся к системе уравнений (10), полученной путем замен переменных в модели Ресслера, и будем решать задачу определения текущих значений параметров  $a$ ,  $b$  и  $c$ , используя те возможности, которые предоставляет вейвлет-анализ. Существует несколько вариантов решения данной задачи. Один из них состоит в том, что вместо вычисления производной функции  $y(t)$ , то есть несущего хаотического сигнала, осуществляется переход в пространство коэффициентов прямого вейвлет-преобразования с использованием матричных элементов дифференциального оператора первого порядка  $\tau_k$ . Затем с помощью обратного вейвлет-преобразования (с использованием коэффициентов  $h_k$ ) получается временная зависимость функции  $dy(t)/dt$ . Данный подход, предусматривающий прямое и обратное вейвлет-преобразование с разными коэффициентами, имеет несомненное преимущество по сравнению с численным дифференцированием сигнала  $y(t)$  по приближенным математическим формулам. Соответствующий пример изображен на рис. 2. Если к анализируемому сигналу (рис. 2,  $a$ ) добавляется нормально распределенный случайный процесс

с дисперсией 0.05, то формальное применение формул численного дифференцирования, основанных на интерполяционных многочленах Ньютона, приведет к большим погрешностям оценки производных (рис. 2, б). Рассматриваемый подход на основе вейвлетов обеспечивает, как минимум, на порядок меньшую величину погрешности

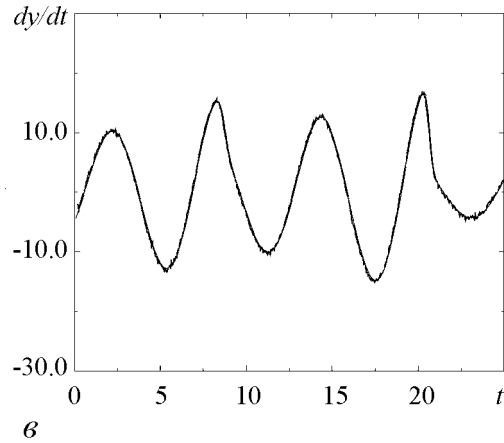
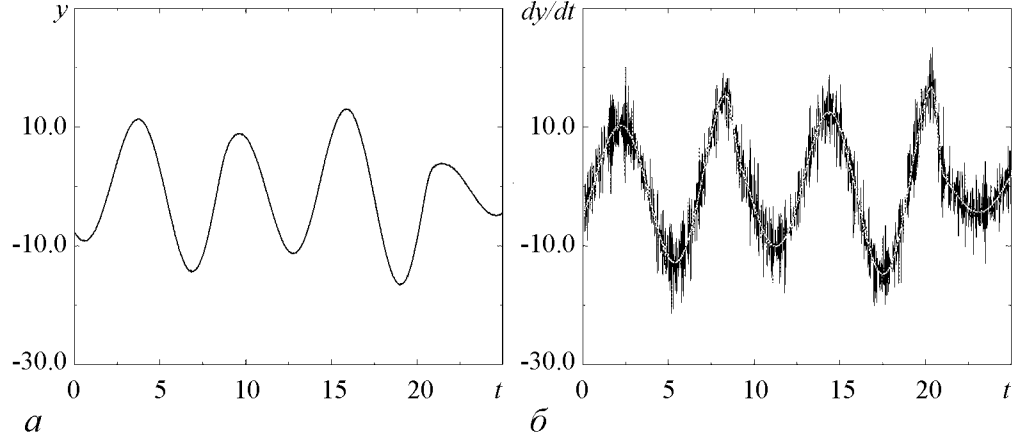


Рис. 2. Исходный сигнал системы Ресслера (а), к которому добавляется шум с дисперсией 0.05; результаты вычисления первой производной зашумленного процесса по приближенным формулам численного дифференцирования (б) и с помощью вейвлет-анализа (в). Серым цветом на рисунке (б) показаны точные значения производной для сигнала без шума

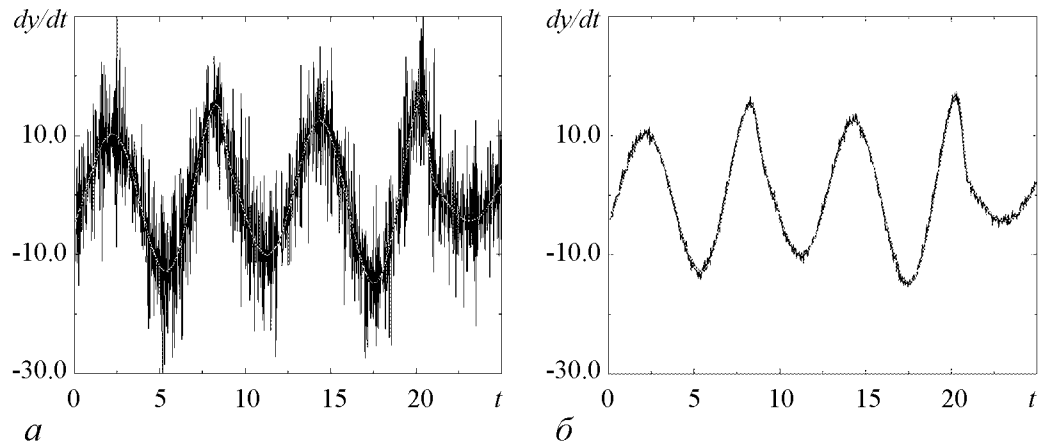


Рис. 3. Результаты вычисления первой производной сигнала, изображенного на рис. 2, а, при добавлении шума с дисперсией 0.1: а – по приближенным формулам численного дифференцирования; б – с помощью вейвлет-анализа

(рис. 2, в), и эта погрешность может быть уменьшена еще сильнее путем выбора подходящего вейвлет-базиса. Аналогичные результаты для другого уровня шума (с дисперсией 0.1) приведены на рис. 3. Вычисление производных  $d^2y(t)/dt^2$  и  $d^3y(t)/dt^3$  будет приводить к значительно более существенным ошибкам для обычного численного дифференцирования по сравнению с вейвлетами. Вместо многократного применения формул дифференциального оператора 1-го порядка можно вычислить элементы дифференциальных операторов 2-го и 3-го порядков, что позволит проводить одновременное вычисление всех необходимых производных.

Пример детектирования информационных сигналов на основе сочетания техники реконструкции ДС и дискретного вейвлет-анализа изображен на рис. 4. В дан-

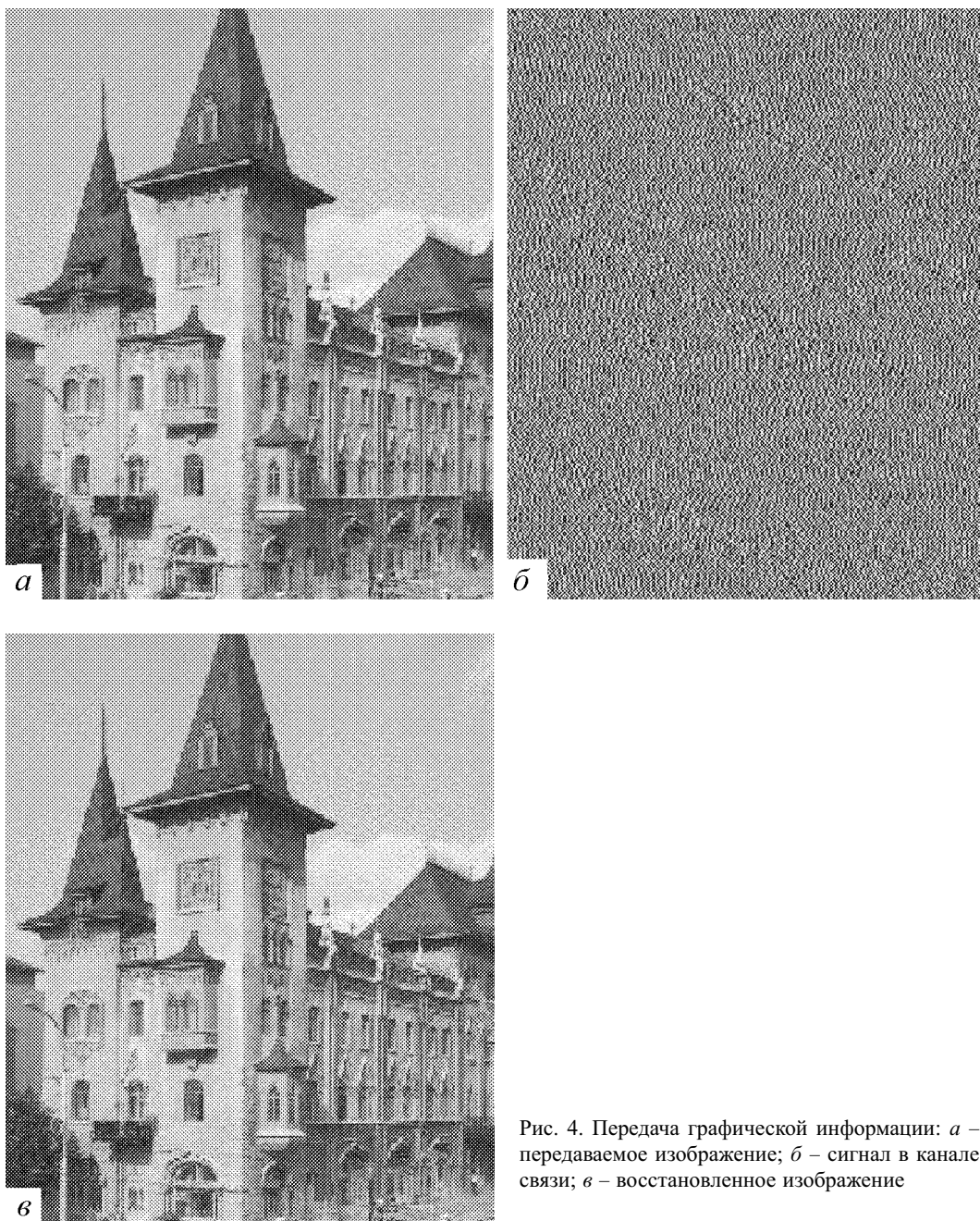


Рис. 4. Передача графической информации: *а* – передаваемое изображение; *б* – сигнал в канале связи; *в* – восстановленное изображение

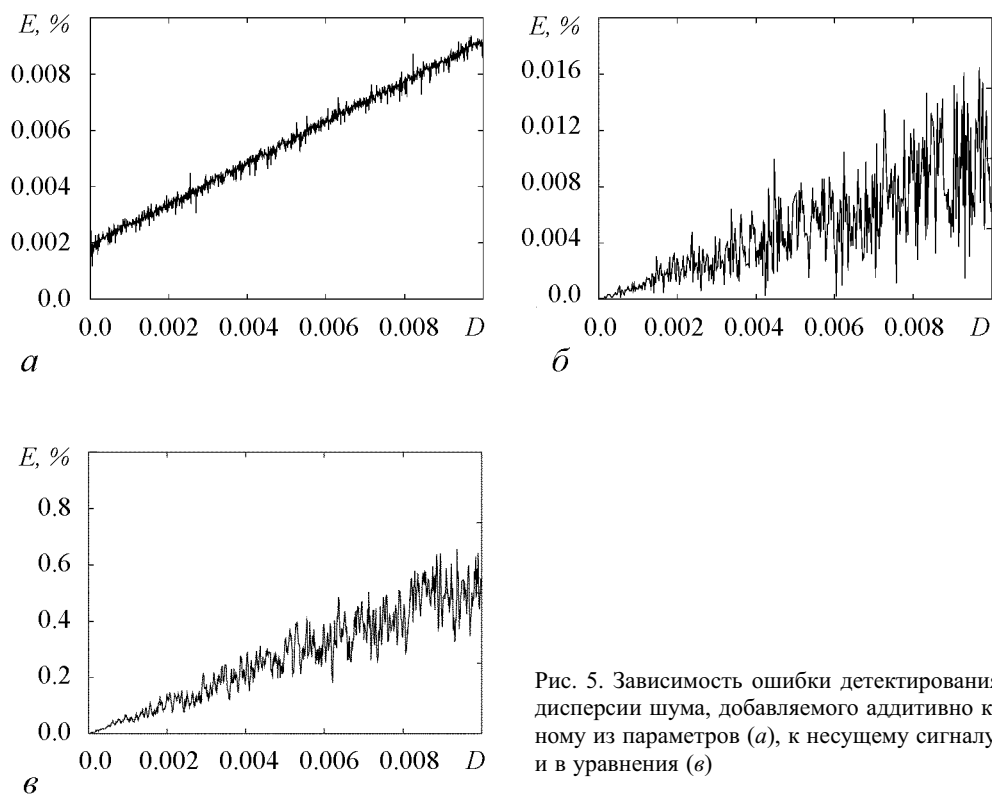


Рис. 5. Зависимость ошибки детектирования от дисперсии шума, добавляемого аддитивно к одному из параметров (*a*), к несущему сигналу (*б*) и в уравнения (*в*)

ном случае проводилась одновременная модуляция трех параметров для передачи информации об оттенках трех цветов (красный, синий, зеленый), формирующих цветное изображение. Применение дискретных вейвлетов позволило повысить точность определения текущих значений параметров и решить данную задачу, рассматривая 256 оттенков цветов. Рис. 5 иллюстрирует, как ошибка вычисления зависит от интенсивности шума, добавляемого аддитивно одному из параметров (рис. 5, *a*), к несущему сигналу (рис. 5, *б*) и вводимого в правые части уравнений модели (рис. 5, *в*).

Для повышения скорости вычислений можно видоизменить методику определения текущих значений параметров. Вместо проведения прямого и обратного вейвлет-преобразований можно перейти в пространство вейвлет-коэффициентов и непосредственно в этом пространстве решать задачу определения параметров путем решения алгебраических уравнений. Этот подход не имеет принципиальных отличий от рассмотренного выше и представляет собой альтернативный вариант технической стороны процедуры детектирования.

### Заключение

Важным обстоятельством для дальнейшего прогресса в области использования динамического хаоса в коммуникациях является формулировка иных принципов модуляции и детектирования информационных сообщений – чем более разнообразными являются подходы к решению данной проблемы, тем более высокая степень

защиты передаваемых сообщений может быть обеспечена. В данной работе предложен метод выделения передаваемых сообщений из хаотического несущего сигнала, основанный на сочетании техники реконструкции динамических систем и дискретных вейвлетов. Несомненным достоинством вейвлет-преобразования является возможность устранения некорректности операции дифференцирования зашумленных временных рядов путем перехода в пространство коэффициентов.

Ошибки, возникающие при использовании приближенных формул численного дифференцирования, основанных на интерполяционных многочленах Ньютона, могут быть уменьшены за счет использования специальных приемов, например, предварительной цифровой фильтрации и последующего применения сплайнов, обеспечивающих непрерывность нескольких производных. Такой прием также имеет недостатки, например, если не обеспечивается качественная фильтрация, то применение сплайнов к зашумленным данным будет приводить к ошибкам интерполяции. Отметим, что данный прием достаточно тесно связан со скейлинг-функциями дискретного вейвлет-преобразования, но преимущество вейвлетов состоит в возможности ускорить процедуру вычислений за счет применения быстрых (пирамидальных) алгоритмов, обеспечивающих существенный выигрыш в скорости (по аналогии с быстрым преобразованием Фурье). Это один из принципиальных моментов с точки зрения коммуникаций.

По сравнению с использованием техники реконструкции в том варианте, который был представлен в [16,17], подход, предлагаемый в данной работе, обеспечивает не только существенный выигрыш в скорости вычислений, но и значительно более высокую помехоустойчивость (в проводимых вычислениях ошибку определения текущих значений параметров удавалось уменьшить на 1-2 порядка).

*Автор выражает искреннюю признательность О.В. Иванову за многочисленные обсуждения и предоставленные высокоточные расчеты коэффициентов  $h_k$  и матричных элементов операторов дифференцирования. Работа выполнена при поддержке CRDF (грант № ВР4М06) и в рамках аналитической ведомственной целевой программы Министерства образования и науки РФ «Развитие научного потенциала высшей школы».*

## **Библиографический список**

1. Cuomo K.M., Oppenheim A.V. Circuit implementation of synchronized chaos with applications to communications // Phys. Rev. Lett. 1993. Vol. 71. P. 65.
2. Kocarev L., Halle K.S., Eckert K., Chua L.O., Parlitz U. Experimental demonstration of secure communications via chaotic synchronization // Int. J. Bifurcation Chaos. 1992. Vol. 2. P. 709.
3. Wu C.W., Chua L.O. A simple way to synchronize chaotic systems with applications to secure communication systems // Int. J. Bifurcation Chaos. 1993. Vol. 3. P. 1619.
4. Parlitz U., Chua L.O., Kocarev L., Halle K.S., Shang A. Transmission of digital signals by chaotic synchronization // Int. J. Bifurcation Chaos. 1992. Vol. 2. P. 973.
5. Cuomo K.M., Oppenheim A.V., Strogatz S.H. Synchronization of Lorenz-based chaotic circuits with application to communications // IEEE Trans. Circuits Syst. 1993. Vol. 40. P. 626.

6. *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.* 1993. Vol. 40. P. 634.
7. *Parlitz U.* Estimating model parameters from time series by autosynchronization // *Phys. Rev. Lett.* 1996. Vol. 76. P. 1232.
8. *Parlitz U., Kocarev L.* Multichannel communication using autosynchronization // *Int. J. Bifurcation Chaos.* 1996. Vol. 6. P. 581.
9. *Дмитриев А.С., Панас А.И.* Динамический хаос. Новые носители информации для систем связи. М: Физматлит, 2002.
10. *Starkov S.O., Yemetz S.V.* Digital communication systems, using chaos // *Proc. Int. Conf. Control of Oscillations and Chaos.* St.Peterburg, 1997. Vol. 2. P. 207.
11. *Dmitriev A.S., Kyarginsky B.Ye., Panas A.I., Starkov S.O.* Experiments on ultra wideband direct chaotic information transmission in microwave band // *Int. J. Bifurcation and Chaos.* 2003. Vol. 13. P. 1495.
12. *Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е.* Способ скрытой передачи информации, основанный на явлении обобщенной синхронизации // *Известия РАН. Серия физическая.* 2008. Т. 72, № 1. С. 143.
13. *Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е.* Способ секретной передачи информации // Патент на изобретение No. 2295835. Москва: ФИПС, 2007.
14. *Anishchenko V.S., Pavlov A.N., Janson N.B.* Global reconstruction in the presence of *a priori* information // *Chaos, Solitons and Fractals.* 1998. Vol. 9. P. 1267.
15. *Janson N.B., Pavlov A.N., Anishchenko V.S.* // *Chaos and its reconstruction* / Edited by G. Gouesbet, S. Meunier-Guttin-Cluzel. New York: Novascience publishers, 2003. P. 287.
16. *Anishchenko V.S., Pavlov A.N.* Global reconstruction in application to multichannel communication // *Phys. Rev. E.* 1998. Vol. 57. P. 2455.
17. *Анищенко В.С., Павлов А.Н., Янсон Н.Б.* Реконструкция динамических систем в приложении к решению задачи защиты информации // *Журнал технической физики.* 1998. № 12. С. 1.
18. *Gribkov D.A., Gribkova V.V., Kuznetsov Yu.I., Rzhanov A.G.* Global dynamical modeling of time series and application to restoration of broadband signal characteristics // *Chaotic, fractal and nonlinear signal processing* / Edited R.A. Katz. Mystic, Juli, 1995. P. 181. (AIP Conference Proceedings 375. New York: AIP Press).
19. *Грибков Д.А., Грибкова В.В., Кузнецов Ю.И.* Восстановление внешнего воздействия по реализации одной переменной автостохастической системы // *Вестн. Моск. ун-та. Сер. 3, Физика, Астрономия.* 1995. Т. 36, № 1. С. 76.
20. *Bezruchko B.P., Smirnov D.A.* Constructing nonautonomous differential equations from experimental time series // *Phys. Rev. E.* 2001. Vol. 63. P. 016207.
21. *Bezruchko B.P., Dikanev T.V., Smirnov D.A.* Role of transient processes for reconstruction of model equations from time series // *Phys. Rev. E.* 2001. Vol. 64. P. 036210.

22. Безручко Б.П., Смирнов Д.А., Сысоев И.В., Селезнев Е.П. Реконструкция моделей неавтономных систем с дискретным спектром воздействия // Письма в ЖТФ. 2003. № 19. С. 69.
23. Anishchenko V.S., Astakhov V.V., Neiman A.B., Vadivasova T.E. and Schimansky-Geier L. Nonlinear Dynamics of Chaotic and Stochastic Systems. Tutorial and Modern Development. Berlin, Heidelberg: Springer, 2007.
24. Астафьева Н.М. Вейвлет-анализ: основы теории и примеры применения // Успехи физических наук. 1996. Т. 166. С. 1145.
25. Daubechies I. Ten Lectures on Wavelets. Philadelphia: S.I.A.M., 1992.
26. Meyer Y. Wavelets: Algorithms and Applications. Philadelphia: S.I.A.M., 1993.
27. Дремин И.М., Иванов О.В., Нечитайло В.А. Вейвлеты и их применение // Успехи физических наук. 2001. Т. 171. С. 465.

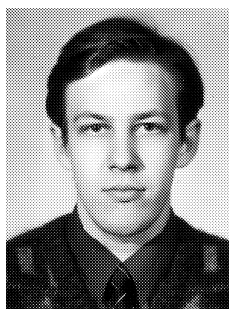
*Саратовский государственный  
университет им. Н.Г. Чернышевского*

*Поступила в редакцию 13.03.2008*

**DETECTION OF INFORMATION SIGNALS BASED  
ON RECONSTRUCTION OF DYNAMICAL SYSTEMS  
AND DISCRETE WAVELET-TRANSFORM**

*A.N. Pavlov*

An approach to extract transmitted messages from the chaotic carrying signal is proposed based on the combination of dynamical systems reconstruction and the discrete wavelet-transform. It is shown that discrete wavelets allow one to increase the stability to noise of the detecting algorithm that deals with the reconstruction technique.



*Павлов Алексей Николаевич – родился в Саратове (1973). Окончил физический факультет Саратовского университета по специальности радиофизика и электроника (1995). Кандидат физико-математических наук (1998). В настоящее время работает доцентом на кафедре радиофизики и нелинейной динамики. Область научных интересов: анализ временных рядов. Имеет более 80 работ, опубликованных в отечественной и зарубежной печати.  
E-mail: pavlov@chaos.ssu.runnet.ru*