МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 4, № 1

Volume 4, No. 1

Одеса – 2014
Odesa – 2014

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration КВ № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

УДК 004.622.612

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 5-13

БЫСТРЫЕ ОРТОГОНАЛЬНЫЕ ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

М.И. Мазурков, А.В. Соколов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alart@stream.com.ua

Разработан метод построения ортогональных преобразований на основе бент-последовательностей, для которого предложена экономичная схема вычисления коэффициентов преобразования. Найдены все минимаксные с точки зрения автокорреляционных свойств бент-последовательности длины $N = 16$.

Ключевые слова: бент-последовательность, ортогональное преобразование, экономичная схема, CDMA.

Введение

Важнейшим классом бинарных сигналов, интенсивно изучающихся в последние десятилетия, стали бент-последовательности, обладающие равномерным спектром Уошла-Адамара, и, соответственно, максимально возможным расстоянием нелинейности в смысле расстояния Хэмминга до кода Рида-Маллера первого порядка [1]. Вышеуказанные последовательности нашли применение во многих областях науки и техники, в том числе в теории передачи информации, криптографии, криптоанализе. Так, благодаря своему равномерному спектру амплитуд, бент-последовательности нашли свое применение в технологиях CDMA (англ. Code Division Multiple Access — множественный доступ с кодовым разделением), где они позволяют существенно уменьшить отношение пиковой и средней мощностей сигнала — пик-фактор, что приводит к более рациональному использованию мощности передатчика [2]. Высокое расстояние нелинейности бент-последовательностей приводит к существенному затруднению их аппроксимации классом аффинных функций, что позволяет наилучшим образом противостоять атакам линейного криптоанализа [3].

Целью настоящей статьи является разработка метода синтеза бинарных матриц Ψ ортогонального преобразования на основе бент-последовательностей и построение быстрого алгоритма вычисления коэффициентов преобразований.

Основная часть

В соответствии с определением [4,5] бинарная последовательность $B = [b_0, b_1, \ldots, b_i, \ldots, b_{n-1}]$, где $b_i \in \{\pm 1\}$ — коэффициенты, четной длины $N = 2^k$, $i = 0,1,\ldots,k-1$, называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша-Адамара $W_B(\omega)$, который представим в матричной форме

$$W_B(\omega) = BA,\ \omega = 0,1,\ldots,N, \qquad (1)$$

где A — матрица Уолша-Адамара порядка N.

Исходя из определения бент-последовательности, каждый спектральный коэффициент последовательности $W_B(\omega=0), W_B(\omega=1),\ldots,W_B(\omega=n-1)$ принимает значения из множества $\{\pm 2^{k/2}\}$.

В настоящее время, для произвольного значения длины N не существует конструктивного алгоритма, позволяющего построить полный класс бент-последовательностей, и даже асимптотических оценок количества существующих в природе бент-последовательностей [1]. Тем не менее, регулярные методы синтеза созданы для некоторых значений N, например, для $N=16$. Так в [5] предложен регулярный метод, позволяющий синтезировать полный класс бент-последовательностей на основе 4-х структур опорных матриц:

$$S_1(4)=\begin{bmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{bmatrix},\quad S_2(4)=\begin{bmatrix}a\\ b\\ c\\ d\end{bmatrix},\quad S_3(4)=\begin{bmatrix}q\\ q\\ s\\ \bar{s}\end{bmatrix},\quad S_4(4)=\begin{bmatrix}r\\ r\\ r\\ \bar{r}\end{bmatrix}, \tag{2}$$

где $\alpha,\beta,\gamma,\delta,a,b,c,d,q,s,r$ — векторы-элементы линейного векторного пространства V_4 векторов длины 4, где

$$V_4=\begin{matrix}\{++++,\ +++-,\ ++-+,\ ++--,\ +-++,\ +-+-,\ +--+,\ +---,\\ -+++,\ -++-,\ -+-+,\ -+--,\ --++,\ --+-,\ ---+,\ ----\}.\end{matrix}$$

Для каждой из матриц (2) существует определенное правило построения подкласса бент-последовательностей.

Так, например, конструкция $S_1(4)$ представляет из себя вертикальную конкатенацию векторов $\alpha,\beta,\gamma,\delta$ — всех четного веса, что отображает конструкцию Мэйорана-МакФарланда [1] и позволяет построить класс из $J_1=384$ бент-последовательностей, которые можем привести в виде 12-ти полиномов Жегалкина [3] с точностью до аффинных термов $\{1,x_1,x_2,x_3,x_4\}$

$$\begin{bmatrix}x_1x_3\oplus x_2x_3\oplus x_1x_4\oplus x_3x_4;\\ x_1x_3\oplus x_2x_3\oplus x_1x_4;\\ x_1x_3\oplus x_2x_3\oplus x_2x_4\oplus x_3x_4;\\ x_1x_3\oplus x_2x_3\oplus x_2x_4;\\ x_1x_3\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4;\\ x_1x_3\oplus x_1x_4\oplus x_2x_4;\end{bmatrix}\quad\begin{bmatrix}x_1x_3\oplus x_2x_4;\\ x_1x_3\oplus x_2x_4\oplus x_3x_4;\\ x_2x_3\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4;\\ x_2x_3\oplus x_1x_4\oplus x_2x_4;\\ x_2x_3\oplus x_1x_4;\\ x_2x_3\oplus x_1x_4\oplus x_3x_4.\end{bmatrix} \tag{3}$$

Аналогичным образом, на основе конструкций $S_2(4)$, $S_3(4)$, $S_4(4)$, где вектора a,b,c,d,q,s,r являются векторами нечетного веса, может быть получено $J_2+J_3+J_4=192+288+32=512$ бент-последовательностей, которые также представим в виде 16-ти полиномов Жегалкина с точностью до аффинных термов

$$\begin{bmatrix} x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_1x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_3x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4; \end{bmatrix} \quad \begin{bmatrix} x_1x_2 \oplus x_1x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_2x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3x_4. \end{bmatrix} \tag{4}$$

Таким образом, 28 полиномов Жегалкина (3) и (4) полностью определяют полный класс бент-последовательностей мощности $J = 896$.

Данные [6, 7] и проведенные исследования позволили установить, что на основе каждой из существующих бент-последовательностей может быть построена бинарная ортогональная матрица преобразования, путем выполнения операции диадного сдвига.

Нетрудно показать, что матрица $Diad(N)$ диадного сдвига (диадной перестановки) строится по рекуррентному правилу

$$Diad(N) = \begin{bmatrix} Diad(N/2) & Diad(N/2) + N/2 \\ Diad(N/2) + N/2 & Diad(N/2) \end{bmatrix}, \tag{5}$$

где $Diad(2) = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$. Например, для значения $N = 16$, получаем

$$Diad(16) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 & 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 & 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 & 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 & 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 & 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 & 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}. \tag{6}$$

Осуществляя перестановку элементов бент-последовательности в соответствии с правилами (строками) построения матрицы диадного сдвига $Diad$ получаем бинарную матрицу Ψ ортогонального преобразования.

Например, пусть задан первый полином Жегалкина из (3), полностью определяющий структуру бинарной бент-последовательности

$$B = \{11111-1-111-11-1-1-111\}, \tag{7}$$

тогда с учетом выражения (6) можем построить бинарную матрицу ортогонального преобразования

$$\Psi = \left[\begin{array}{cccc|cccc|cccc|cccc}
+ & + & + & + & + & - & - & + & + & - & + & - & - & - & + & + \\
+ & + & + & + & - & + & + & - & - & + & - & + & - & - & + & + \\
+ & + & + & + & - & + & + & - & + & - & + & - & + & + & - & - \\
+ & + & + & + & + & - & - & + & - & + & - & + & + & + & - & - \\
\hline
+ & - & - & + & + & + & + & + & - & - & + & + & + & - & + & - \\
- & + & + & - & + & + & + & + & - & - & + & + & - & + & - & + \\
- & + & + & - & + & + & + & + & + & + & - & - & + & - & + & - \\
+ & - & - & + & + & + & + & + & + & + & - & - & - & + & - & + \\
\hline
+ & - & + & - & - & - & + & + & + & + & + & + & + & - & - & + \\
- & + & - & + & - & - & + & + & + & + & + & + & - & + & + & - \\
+ & - & + & - & + & + & - & - & + & + & + & + & - & + & + & - \\
- & + & - & + & + & + & - & - & + & + & + & + & + & - & - & + \\
\hline
- & - & + & + & + & - & + & - & + & - & - & + & + & + & + & + \\
- & - & + & + & - & + & - & + & - & + & + & - & + & + & + & + \\
+ & + & - & - & + & - & + & - & - & + & + & - & + & + & + & + \\
+ & + & - & - & - & + & - & + & + & - & - & + & + & + & + & +
\end{array}\right], \tag{8}$$

В общем случае, матрица Ψ является симметричной ортогональной матрицей [6], т.е.

$$\Psi \cdot \Psi^T = \Psi * \Psi = NI, \tag{9}$$

где T — оператор транспонирования, I — единичная матрица порядка N.

В [7] разработана экономичная схема вычисления коэффициентов ортогональных преобразований на основе совершенных двоичных решеток. Данная схема основана на учете свойств двухпетлевого циклического сдвига, который используются для построения матриц таких преобразований. В настоящей работе установлено, что подобная экономичная схема вычисления коэффициентов ортогонального преобразования может быть построена и для случая произвольной структуры бент-последовательности. Функционирующая модель данной схемы была собрана с помощью интерактивного инструмента имитации и анализа динамических систем Matlab Simulink.

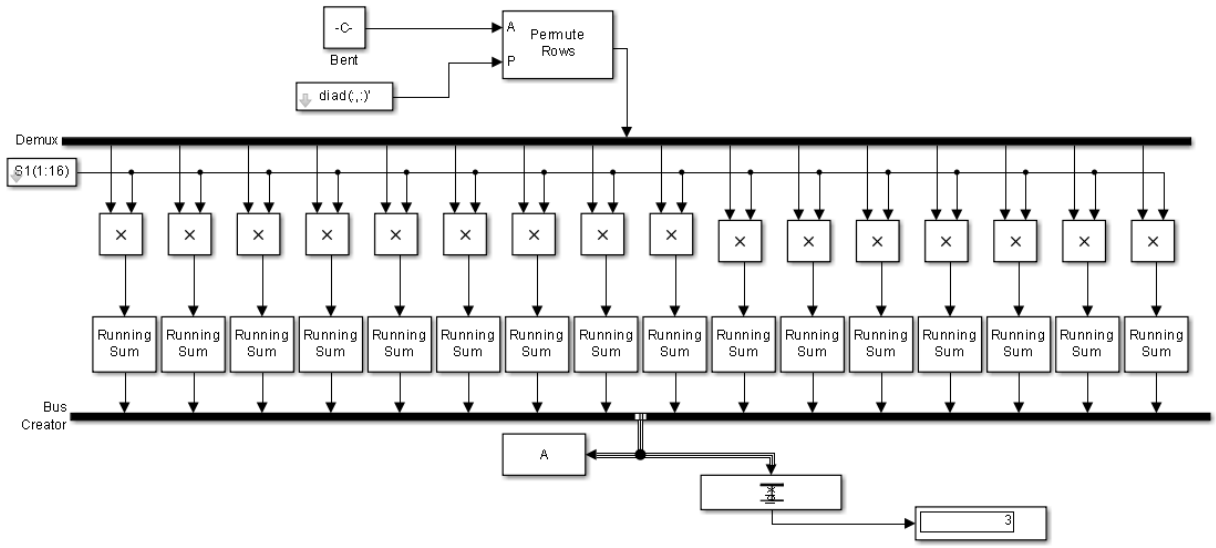


Рис. 1. Экономичная схема вычисления коэффициентов ортогональных преобразований на основе бент-последовательностей длины $N = 16$

На рис. 1 приняты следующие условные обозначения, расшифрованные в табл. 1.

Таблица 1.

Расшифровка условных обозначений схемы (рис. 1)

×	— умножитель;		— дисплей, вывод результата.
Running Sum	— накопительный сумматор;	A	— вывод массива, содержащего результат;
-C- Bent1	— ввод исходной бент-последовательности;	diad(:,:)'	— ввод диадной синхропоследовательности;
A Permute Rows P	— коммутатор входов по правилу диадного сдвига;		— нахождение индекса максимального элемента;

Опишем принцип функционирования экономичной схемы вычисления коэффициентов ортогонального преобразования на основе бент-последовательностей. На вход коммутатора входов по правилу диадных сдвигов подаются элементы исходной бент-последовательности, например (7), а также диадная синхропоследовательность, сформированная в соответствии с (8), которая может храниться в накопителе, либо же формироваться на каждом такте работы схемы. Элементы преобразованной в соответствии с правилом диадной синхропоследовательности бент-последовательности на каждом такте схемы перемножаются с отсчетом сигнала, соответствующим номеру такту, и подаются на вход накопительного сумматора, после чего мультиплексируются. Результирующий вектор подается на решающее устройство, определяющее наиболее правдоподобный переданный сигнал как индекс максимального элемента результирующего вектора преобразования.

Пусть, например, передавался один из ортогональных сигналов, соответствующей 3-й строке матрицы (8), т.е.

$$S(t) = \{1111-111-11-11-111-1-1\}, \quad (10)$$

который под воздействием некоторой помехи в канале связи был искажен, в результате чего на приемник поступила последовательность

$$Y(t) = \{00-22-102-31-11-101-10\}, \quad (11)$$

тогда на выходе схемы мы получим последовательность - корреляционный вектор

$$Z(\tau) = Y \cdot \Psi = \{-408-44-80-4-444-4-444-4\}, \tau = 0,1,\ldots,15, \quad (12)$$

соответственно схема (рис. 1) приняла решение о том, что максимально правдоподобно был передан сигнал соответствующей 3-й строке матрицы (8), что соответствует действительности.

Учитывая определение Дж. фон Неймана [8], будем оценивать сложность реализации предложенной экономичной схемы вычисления коэффициентов ортогональных преобразований на основе бент-последовательностей как число умножителей, как самых сложнореализуемых её компонентов. Очевидно, сложность реализации прямой схемы вычисления коэффициентов ортогонального преобразования на основе бент-последовательностей как матричного произведения можно оценить как $O(N^2)$, тогда как сложность предлагаемой схемы $O(N)$, т.е. имеем выигрыш

$$\gamma = \frac{N^2}{N} = N, \quad (13)$$

что является даже более значительным, чем выигрыш при использовании алгоритмов быстрого преобразования Уолша-Адамара, где сложность оценивается как $O(N \cdot \log_2(N))$. Не вызывает сомнений также тот факт, что предложенная схема может быть легко масштабирована для любых N.

Отметим, что все остальные компоненты схемы, в том числе коммутатор и накопительные сумматоры имеют низкую сложность реализации, и обычно входят в состав современных микросхем PLD (англ. Programmable Logic Device — программируемая логическая интегральная схема) [9].

Вопрос выбора исходной бент-последовательности зависит от конкретных приложений, в которых могут быть использованы предложенные ортогональные преобразования. Например, использование полного класса бент-последовательностей может быть оправдано для реализации концепции оперативной смены ансамбля используемых сигналов для решения задач защиты информации. В задачах же повышения помехоустойчивости могут быть использованы минимаксные [10] бент-последовательности с точки зрения ААКФ (апериодической автокорреляционной функции)

$$r_{ААКФ}(n) = \sum_{l=0}^{2N-2} B(l)B(n+l), n = 0,1,\ldots,2N-2, \quad (14)$$

а также ПАКФ (периодической автокорреляционной функции)

$$r_{ПАКФ}(n) = \sum_{l=0}^{N-1} B(l)B(n+l),\ n = 0,1,\ldots,N-1. \qquad (15)$$

Результаты проведенных исследований позволили установить значения максимумов побочных лепестков автокорреляционных функций сигналов из класса бент-последовательностей, которые, для наглядности, представим в виде таблицы 2.

Таблица 2.

Значения максимумов побочных лепестков автокорреляционных функций класса бент-последовательностей

$\max\limits_{2,3,\ldots,16}\{r_{ААКФ}\}$	3	4	5	7	8	9
Количество бент-последовательностей	344	152	328	56	8	8
$\max\limits_{2,3,\ldots,16}\{r_{ПАКФ}\}$	—	4	—	—	8	—
Количество бент-последовательностей	—	832	—	—	64	—

Отметим, что все минимаксные с точки зрения ААКФ бент-последовательности являются также минимаксными и с точки зрения ПАКФ. Например, минимаксная бент-последовательность может быть представлена в бинарном, двоичном и шестнадцатеричном видах

$$B = [1\,1\,1\,1\,1 - 1\,1 - 1\,1 - 1 - 1\,1\,1\,1 - 1 - 1] \Rightarrow [0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1]_2 \Rightarrow [0563]_h \qquad (16)$$

обладает ААКФ

$$r_{ААКФ} = \begin{Bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 16 & -1 & 4 & 1 & 0 & 1 & -4 & 3 & 0 & -3 & 0 & -1 & 0 & -1 & 0 & 1 \end{Bmatrix}, \qquad (17)$$

и ПАКФ

$$r_{ПАКФ} = \begin{Bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 16 & 0 & 4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & 4 & 0 \end{Bmatrix}, \qquad (18)$$

которые можно представить в виде графиков (рис. 2).

Для краткости приведем все минимаксные бент-последовательности в виде их шестнадцатеричных эквивалентов (жирным шрифтом выделены шестнадцатеричные эквиваленты, соответствующие совершенным двоичным решеткам [5, 10]).

Анализ данных табл. 2 свидетельствует о достаточно большом количестве бент-последовательностей, обладающих хорошими автокорреляционными свойствами.

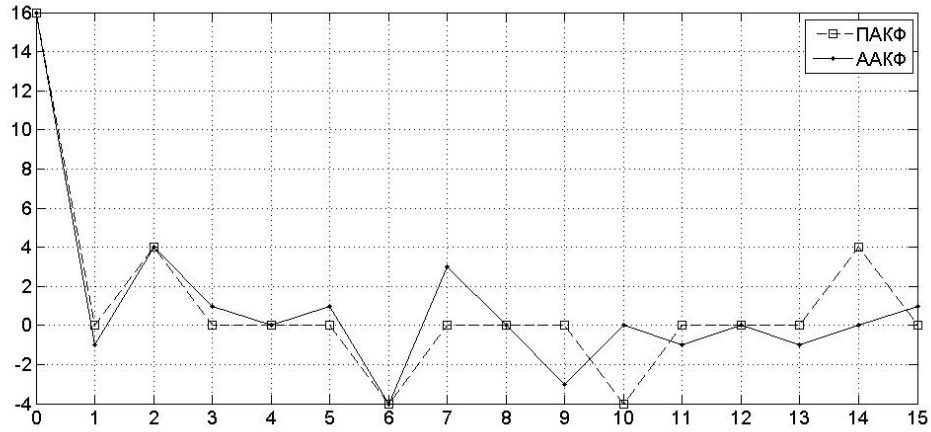


Рис.2. ААКФ и ПАКФ минимаксной бент-последовательности (16)

Таблица 2.

Шестнадцатеричные эквиваленты всех минимаксных бент-последовательностей

0563	059C	**0653**	093A	**095C**	09C5	0A93	**0C56**	**0CA9**	1178
11D2	**12B8**	1427	**14E4**	**1B14**	1BD7	**1D48**	**1DB7**	1E88	1EDD
2147	**218B**	221E	**2287**	2714	**27D7**	281B	**28D8**	**2BDB**	2D11
2D88	**2E7B**	**2EDE**	30A9	**356F**	3650	36AF	395F	39FA	**3A6F**
3AF6	**3F65**	3FA6	4172	**41B1**	442D	**44E1**	**47ED**	482E	**4B11**
4BDD	4D7E	4E7D	**4EBE**	5039	50C9	**53F9**	**5903**	**59FC**	**5C09**
5C90	5F39	5FC6	**603A**	6305	63F5	6503	6A0C	**6ACF**	6C0A
6CF5	6F5C	**6FC5**	7241	**7282**	7412	**747B**	**74DE**	774B	**7822**
78DD	**7B74**	**7BD1**	**7D72**	7DB1	7EB2	**8171**	**8272**	82B1	**8474**
84D1	87BB	**882D**	**88D2**	**8B7B**	**8BDE**	8D41	**8D82**	**8E81**	905C
90C5	9350	950C	**95CF**	9A03	9C05	9C5F	**9F35**	**9FCA**	A063
A309	A390	**A3F9**	A63F	A930	**ACF9**	AF6C	AFC9	B17D	**B1BE**
B411	B477	**B71D**	**B7E2**	**B8ED**	BB78	**BBE1**	BE72	**BEB1**	**C065**
C0A6	**C56F**	C5F6	C65F	C90A	C95F	**CA60**	**CA9F**	CFA9	**D17B**
D1DE	**D288**	D418	D71B	**D7D8**	D814	**D8D7**	**DBD4**	**DD87**	**DE2E**
DE8B	**DED1**	**E144**	**E1BB**	E284	**E414**	E4D7	E7D4	EB27	**EBE4**
EDB8	**EE4B**	**EEB4**	F36A	F536	F593	**F65C**	**F6AC**	**F953**	FA39
FA93	FC65	—	—	—	—	—	—	—	—

Вывод

В заключении отметим основные результаты проведенных исследований:

1. Получила дальнейшее развитие теория синтеза бинарных матриц ортогональных преобразований, в рамках чего разработан метод формирования бинарных матриц ортогональных преобразований на основе бент-последовательностей, которые могут найти свое применение в технологиях передачи информации, таких как CDMA, а также в криптографии и криптоанализе.

2. Разработана экономичная схема вычисления коэффициентов ортогонального преобразования на основе бент-последовательностей, позволяющая существенно сократить необходимое для её реализации количество компонентов, что имеет

критическое значение при реализации разработанных технологий, например, на мобильных устройствах.

3. Найден полный класс минимаксных с точки зрения боковых лепестков автокорреляционных функций бент-последовательностей длины $N = 16$, который может быть рекомендован к использованию в системах связи.

Список литературы

1. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. — Томск, 2009. — Сер. №1(3). — С. 15—37.
2. Peterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13—17, 2001). Proc. Berlin: Springer, 2002. P.46—71.
3. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. — М: Издательство МЦНМО. — 2004. — 472 с.
4. Rothaus, O.S. On “bent” functions / O.S. Rothaus // J. Comb. Theory Ser. A. — USA: Academic Press Inc, 1976. — №20(3). — P.300—305.
5. Мазурков, М.И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов. — Одесса: Труды ОНПУ, 2013. — С.227—230.
6. Дворников, В.Д. Ортогональные коды на основе бент-последовательностей / В.Д. Дворников. — Доклады БГУИР, Минск, 2003. — С. 110—113.
7. Мазурков, М.И. Быстрые ортогональные преобразования на основе совершенных двоичных решеток / М.И. Мазурков, М.Ю. Герасименко // Известия высших учебных заведений. Радиоэлектроника. – 2006. – Т. 49, N 9. - С. 54-60.
8. Блох, Э.Л. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. — М.: Связь, 1976. — 240 с.
9. Попов, А.Ю. Проектирование цифровых устройств с использованием ПЛИС. — М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. — 80 с.
10. Мазурков, М.И. Системы широкополосной радиосвязи: учеб. пособие для студ. вузов / М.И. Мазурков. — Одесса: Наука и техника, 2010. — 340 с.

ШВИДКІ ОРТОГОНАЛЬНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ БЕНТ-ПОСЛІДОВНОСТЕЙ

М.І. Мазурков, А.В. Соколов

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: alart@stream.com.ua

Розроблено метод побудови ортогональних перетворень на основі бент-послідовностей, для якого запропонована економічна схема обчислення коефіцієнтів перетворення. Знайдено всі мінімаксні з точки зору автокореляційних властивостей бент-послідовності довжини N=16.

Ключові слова: бент-послідовність, ортогональне перетворення, економічна схема, CDMA.

FAST ORTHOGONAL TRANSFORMATIONS BASED ON BENT-SEQUENCES

M.I. Mazurkov, A.V. Sokolov

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alart@stream.com.ua

A method was developed to design orthogonal transformations based on bent sequences. The efficient scheme of computation of transformation coefficients was proposed for the above mentioned method as well. There were found all bent-sequences according to the minimax criterion in terms of autocorrelation properties with the length of $N = 16$

Keywords: bent sequence, orthogonal transformation, efficient scheme, CDMA

УДК 519.876.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 4, pp. 14-25

EFFECTIVENESS OF THE WAVELET FILTERING APPLICATION FOR IDENTIFICATION OF NONLINEAR SYSTEMS BASED ON VOLTERRA MODEL IN FREQUENCY DOMAIN

V.O. Speranskyy, V.D. Pavlenko

Odessa National Polytechnic University,
1, Shevchenko av., Odessa, Ukraine, 65044, e-mail: speranskiyva@ukr.net

The research results of the wavelet filtering efficiency using the interpolation method for nonlinear dynamical systems identification based on the Volterra model in the frequency domain are presented. The accuracy and noise immunity of the amplitude- and phase-frequency characteristics of the first , second and third order determining for nonlinear system using experimental data "input-output" using test polyharmonic signals are investigated. The noise immunity of the identification method have been increased using wavelet filtering of measurement noises of received responses and characteristics of the identifiable system.

Keywords: wavelet filtering, identification, efficiency, noise immunity, nonlinear dynamic systems, Volterra models, multidimensional characteristics, polyharmonic signals.

Introduction

All natural objects in the real world are nonlinear with different level on nonlinearity. The presented method allows building linear and nonlinear models for different nonlinear dynamical systems (NDS). Most dynamical objects are nonlinear stochastic inertial systems. The model in the form of integral Volterra series used to identify them [3, 4]. The nonlinear and dynamic properties of such systems are completely characterized by a sequence of multidimensional weighting functions – Volterra kernels [11].

Building a model of nonlinear dynamic system in the form of a Volterra series lies in the choice of the characteristics for the test impacts. Also the developed algorithm is used and allows determining the Volterra kernels and their Fourier-images for the measured responses (multidimensional amplitude–frequency characteristics (AFC) and phase–frequency characteristics (PFC)) to simulate the NDS in the time or frequency domain, respectively [9].

The formulation of the initial boundary value problem

There are no ideal conditions in real world. Thus the measurements during identification of the systems need to be modelled considering the errors of the measurements that are usually modelled by additive Gaussian noise [10].

The research of noise immunity of the interpolation method of nonlinear dynamical systems identification based on the Volterra model in the frequency domain is proposed. The developed identification toolkit is used to build information model of the test nonlinear dynamic system in the form of the first, second and third order model with respect of measurement noise.

The *aim* of this work is to identify the continuous NDS using Volterra model in the frequency domain, i.e. to determine its multi-frequency characteristics on the basis of the data of the "input-output" experiment [12], using test polyharmonic signals and interpolation method with obtained model coefficients and to research the noise immunity and potential filtering ability of final characteristics.

The scheme of the problem solution

Generally, "input–output" type ratio for nonlinear dynamical system can be presented by Volterra series [8].

$$y[x(t)] = w_0(t) + \int_0^\infty w_1(\tau)x(t-\tau)d\tau + \int_0^\infty\int_0^\infty w_2(\tau_1,\tau_2)x(t-\tau_1)x(t-\tau_2)d\tau_1 d\tau_2 + \\ + \int_0^\infty\int_0^\infty\int_0^\infty w_3(\tau_1,\tau_2,\tau_3)x(t-\tau_1)x(t-\tau_2)x(t-\tau_3)d\tau_1 d\tau_2 d\tau_3 + \ldots = w_0(t) + \sum_{n=1}^\infty y_n[x(t)], \quad (1)$$

where the *n*–th partial component of response of the system is

$$y_n[x(t)] = \int_0^t \underset{n\ times}{\ldots} \int_0^t w_n(\tau_1,\ldots,\tau_n)\prod_{i=1}^n x(t-\tau_i)d\tau_i ,$$

$x(t)$ and $y(t)$ are input and output signals of system respectively; $w_n(\tau_1,\tau_2,\ldots,\tau_n)$ – weight function or n-order Volterra kernel; $y_n[x(t)]$ – n–th partial component of system's response; $w_0(t)$ – denotes free component of the series (for zero initial conditions $w_0(t)=0$; t – current time.

Commonly, the Volterra series are replaced by a polynomial, with only taking several first terms of series (1) into consideration. Nonlinear dynamical system identification in a form of Volterra series consists in n-dimensional weighting functions determination $w_n(\tau_1,\ldots,\tau_n)$ for time domain or it's Fourier transforms $W_n(j\omega_1,\ldots,j\omega_n)$ – n–dimensional transfer functions for frequency domain.

Multidimensional Fourier transform for n-order Volterra kernel (1) is written in a form:

$$W_n(j\omega_1,\ldots,j\omega_n) = F_n\langle w_n(\tau_1,\ldots,\tau_n)\rangle = \int_0^\infty\ldots\int_0^\infty w_n(\tau_1,\ldots,\tau_n)\exp\left(-j\sum_{i=1}^n \omega_i\tau_i\right)\prod_{i=1}^n d\tau_i ,$$

where $F_n\langle\ \rangle$ – n–dimensional Fourier transform; $= j=\sqrt{-1}$. Then the model of nonlinear system based on Volterra model in frequency domain can be represented as:

$$y[x(t)] = \sum_{n=1}^\infty F_n^{-1}\left\langle W_n(j\omega_1,\ldots,j\omega_n)\prod_{i=1}^n X(j\omega_i)\right\rangle_{t_1=\ldots=t_n=t},$$

where $F_n^{-1}\langle\ \rangle$ – inverse *n*–dimensional Fourier transform; $X(j\omega_i)$ – Fourier transform of input signal.

Identification of nonlinear system in frequency domain consists in determination of absolute value and phase of multidimensional transfer function at given frequencies –

multidimensional AFC $|W_n(j\omega_1, j\omega_2, \ldots, j\omega_n)|$ and PFC $\arg W_n(j\omega_1, j\omega_2, \ldots, j\omega_n)$ which are defined by formulas:

$$|W_n(j\omega_1, \ldots, j\omega_n)| = \sqrt{[\mathrm{Re}(W_n(j\omega_1, \ldots, j\omega_n))]^2 + [\mathrm{Im}(W_n(j\omega_1, \ldots, j\omega_n))]^2}, \quad (2)$$

$$\arg W_n(j\omega_1, \ldots, j\omega_n) = \mathrm{arctg}\, \frac{\mathrm{Im}[W_n(j\omega_1, \ldots, j\omega_n)]}{\mathrm{Re}[W_n(j\omega_1, \ldots, j\omega_n)]}, \quad (3)$$

where Re and Im – accordingly real and imaginary parts of a complex function of n variables respectively.

An interpolation method of identification of the nonlinear dynamical system based on Volterra series is used [7–8].

Affirmation 1. Let at input of system test signal of $ax(t)$ kind is given, where $x(t)$ – is arbitrary function and a – is scale coefficient (amplitude of signal), where $0 < |a| \le 1$, then for the selection of a partial component of the n-th order $\hat{y}_n(t)$ from measurement of the response nonlinear system $y[ax(t)]$ in the form of Volterra series, it is necessary to determine n-th partial derivative of the total response amplitude a where $a = 0$

$$\hat{y}_n(t) = \int_0^t \underset{n\ times}{\ldots} \int_0^t w_n(\tau_1, \ldots, \tau_n) \prod_{i=1}^{n} x(t-\tau_i) d\tau_i = \frac{1}{n!} \frac{\partial^n y[a\,x(t)]}{\partial a^n}\bigg|_{a=0} \quad (4)$$

We use the method of extracting the partial components with the help of n-fold differentiation of the response $y[ax(t)]$ with respect to parameter – amplitude a and the use of the derivative value at $a = 0$.

Injecting an input signal $ax(t)$ where a is the scaling factor (signal amplitude), one has the following response of the nonlinear system:

$$y[a \cdot x(t)] = a\int_0^t w(\tau) \cdot x(t-\tau) d\tau + a^2 \int_0^t \int_0^t w_2(\tau_1, \tau_2) x(t-\tau_1) x(t-\tau_2) d\tau_1 d\tau_2 +$$

$$+ a^n \int_0^t \underset{n\ time}{\ldots} \int_0^t w_n(\tau_1, \ldots, \tau_n) \prod_{r=1}^{n} x(t-\tau_r) d\tau_r + \ldots$$

To distinguish the partial component of the n-th order, differentiate the system response n times with respect to the amplitude:

$$\frac{\partial^n y[a \cdot x(t)]}{\partial a^n} = n! \int_0^t \underset{n\ times}{\ldots} \int_0^t w_n(\tau_1, \ldots, \tau_n) \prod_{r=1}^{n} x(t-\tau_r) d\tau_r +$$

$$(n+1)! \cdot a \int_0^t \underset{n+1\ times}{\ldots} \int_0^t w_{n+1}(\tau_1, \ldots, \tau_{n+1}) \prod_{r=1}^{n+1} x(t-\tau_r) d\tau_r + \ldots$$

Taking the value of the derivative at $a = 0$, we finally obtain the expression for the partial component (4).

Formulas for numerical differentiation. Partial derivative should be substituted by form of finite difference for calculation. Differentiation of function, which was set in discrete points, could be accomplished by means of numerical computing after preliminary smoothing

of measured results. Various formulas for the numerical differentiation are known, which differ from each other by means of error.

Let's use universal reception which allows to substitute a derivative of any n order for differential ratio so that the error from such replacement for function $y(a)$ was any beforehand set order of p approximation concerning a step of $h = \Delta a$ of computational mesh on amplitude. Method of undetermined coefficient for equality

$$\frac{d^n y(a)}{da^n} = \frac{1}{h^n} \sum_{r=-r_1}^{r_2} c_r y(a+rh) + O(h^p), \tag{5}$$

where the coefficients c_r are taken not depending on h, $r = -r_1, -r_1+1, ..., -1, 0, 1, \ldots, r_2-1, r_2$, so that equality (5) was fair. The limits of summation $r_1 \geq 0$ и $r_2 \geq 0$ could be arbitrary, but so that the differential relation $h^{-n}\sum c_r y(a+rh)$ of $r_1 + r_2$ order have to satisfy to inequality $r_1 + r_2 \geq n + p - 1$.

To define the c_r it is necessary to solve the following set of equations

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ -r_1 & -r_1+1 & \cdots & r_2 \\ \cdots & \cdots & \cdots & \cdots \\ (-r_1)^{n-1} & (-r_1+1)^{n-1} & \cdots & r_2^{n-1} \\ (-r_1)^{n} & (-r_1+1)^{n} & \cdots & r_2^{n} \\ (-r_1)^{n+1} & (-r_1+1)^{n+1} & \cdots & r_2^{n+1} \\ \cdots & \cdots & \cdots & \cdots \\ (-r_1)^{n+p-1} & (-r_1+1)^{n+p-1} & \cdots & r_2^{n+p-1} \end{bmatrix} \cdot \begin{bmatrix} c_{-r_1} \\ c_{-r_1+1} \\ \cdots \\ c_{-1} \\ c_0 \\ c_1 \\ \cdots \\ c_{r_2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \cdots \\ 0 \\ n! \\ 0 \\ \cdots \\ 0 \end{bmatrix}. \tag{6}$$

If $r_1 + r_2 = n + p - 1$ then inscribed in $n + p$ equality forms linear system concerning the same number of c_r unknown. The determiner of this system is Vandermonde's determiner and differs from zero. Thus, there is only one set of n coefficients, satisfying the system.

If $r_1 + r_2 \geq n + p$, then there are many such sets of coefficients c_r.

On the basis of (6) in [7–8] the formulas of derivative calculation of the first, second and third orders are received at $a = 0$ with use of the central differences for equidistant nodes of the computational grid.

The amplitudes of the test signals $a_i^{(n)}$ and the corresponding coefficients $c_i^{(n)}$ for responses are presented in [9].

The test polyharmonic effects for identification in the frequency domain representing by signals of such type:

$$x(t) = \sum_{k=1}^{n} A_k \cos(\omega_k t + \varphi_k), \tag{7}$$

where n – the order of transfer function being estimated; A_k, ω_k and φ_k – accordingly amplitude, frequency and a phase of k-th harmonics. In research, it is supposed every amplitude of A_k to be equal, and phases φ_k equal to zero.

The test polyharmonic signals are used for identification in frequency domain.

Statement. If test polyharmonic signal is used in form

$$x(t) = A\sum_{k=1}^{n}\cos\omega_k t = \frac{A}{2}\sum_{k=1}^{n}\left(e^{j\omega_k t} + e^{-j\omega_k t}\right),$$

then the n–th partial component of the response of test system can be written in form:

$$y_n(t) = \frac{A^n}{2^{n-1}}\sum_{m=0}^{E(n/2)} C_n^m \sum_{k_1=1}^{n}\ldots\sum_{k_n=1}^{n}\left|W_n\left(-j\omega_{k_1},\ldots -j\omega_{k_m}, j\omega_{k_{m+1}},\ldots j\omega_{k_n}\right)\right|\times$$

$$\times\cos\left(\left(-\sum_{l=0}^{m}\omega_{k_l} + \sum_{l=m+1}^{n}\omega_{k_l}\right)t + \arg W_n\left(-j\omega_{k_1},\ldots -j\omega_{k_m}, j\omega_{k_{m+1}},\ldots j\omega_{k_n}\right)\right),$$

where E – function used to obtain the of integer part of the value.

The component with frequency $\omega_1 + \ldots + \omega_n$ is extracted from the response to test signal (7):

$$A^n\,|W_n(j\omega_1,\ldots,j\omega_n)|\cos[(\omega_1+\ldots+\omega_n)t + \arg W_n(j\omega_1,\ldots,j\omega_n)]. \qquad (8)$$

Certain limitations should be imposed while choosing of frequency polyharmonic test signals in a process determining multidimensional AFC and PFC. This is the reason why the values of AFC and PFC in this unallowable points of multidimensional frequency space can be calculated using interpolation only. In practical realization of nonlinear dynamical systems identification it is needed to minimize number of such undefined points at the range of multidimensional frequency characteristics determination. This was performed to provide a minimum of restrictions on choice of frequency of the test signal. It is shown that existed limitation can be weakened. New limitations on choice of frequency are reducing number of undefined points.

After analyzing the (8) it is defined: to obtain Volterra kernels for nonlinear dynamical system in frequency domain the limitations on choice of frequencies of test polyharmonic signals have to be restricted. These restrictions provide inequality of combination frequencies in the test signal harmonics. The theorem about choice of test signals frequencies is proven.

*The theorem about choice of test signals frequencies***.** For the definite filtering of a response of the harmonics with combination frequencies $\omega_1 + \omega_2 + \ldots + \omega_n$ within the n-th partial component it is necessary and sufficient to keep the frequency from being equal to another combination frequencies of type $k_1\omega_1 + \ldots + k_n\omega_n$, where the coefficients $\{k_i | i = 1,2,\ldots,n\}$ must satisfy the conditions:

- number K of negative value coefficients $(k_i < 0)$ is in $0 \le K \le E(n/2)$ (where E – function used to obtain the of integer part of the value);
- $\sum_{i=1}^{n}|k_i| \le n;$
- $\sum_{i=1}^{n}|k_i| \equiv n\,(mod\ 2),\ n - \sum_{i=1}^{n}|k_i| = 2l, l \in N.$

It was shown that during determination of multidimensional transfer functions of nonlinear systems it is necessary to consider the imposed constraints on choice of the test polyharmonic signal frequencies. This provides inequality of combination frequencies in output signal harmonics: $\omega_1 \ne 0$, $\omega_2 \ne 0$ and $\omega_1 \ne \omega_2$ for the second order identification procedure, and $\omega_1 \ne 0$, $\omega_2 \ne 0$, $\omega_3 \ne 0$, $\omega_1 \ne \omega_2$, $\omega_1 \ne \omega_3$, $\omega_2 \ne \omega_3$, $2\omega_1 \ne \omega_2 + \omega_3$,

$2\omega_2 \neq \omega_1 + \omega_3$, $2\omega_3 \neq \omega_1 + \omega_2$, $2\omega_1 \neq \omega_2 - \omega_3$, $2\omega_2 \neq \omega_1 - \omega_3$, $2\omega_3 \neq \omega_1 - \omega_2$, $2\omega_1 \neq -\omega_2 + \omega_3$, $2\omega_2 \neq -\omega_1 + \omega_3$ and $2\omega_3 \neq -\omega_1 + \omega_2$ for the third order identification procedure.

Described method was tested using nonlinear test system (fig. 1) represented by Riccati equation:

$$\frac{dy(t)}{dt} + \alpha y(t) + \beta y^2(t) = u(t).$$

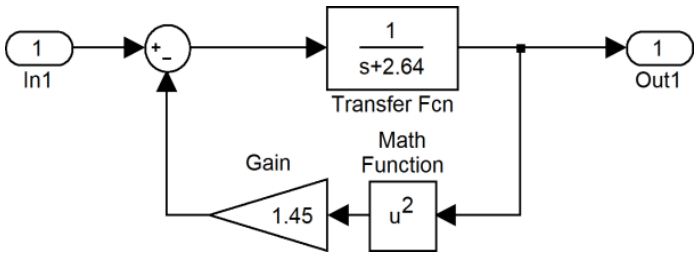


Fig. 1. Simulink–model of the test system

Analytical expressions of AFC and PFC for the first, second and third order model were received in [8].

The main purpose was to identify the multi–frequency performances characterizing nonlinear and dynamical properties of nonlinear test system using the methodic [10]. Volterra model in the form of the 1, 2 and 3 order polynomial is used. Thus, test system properties are characterized by transfer functions of $W_1(j\omega)$, $W_2(j\omega_1, j\omega_2)$, $W_3(j\omega_1, j\omega_2, j\omega_3)$ – by Fourier-images of weight functions $w_1(t)$, $w_2(t_1, t_2)$ and $w_3(t_1, t_2, t_3)$.

Structure chart of identification procedure – determination of the *n*-th order AFC and PFC of NDS is presented in fig. 2.

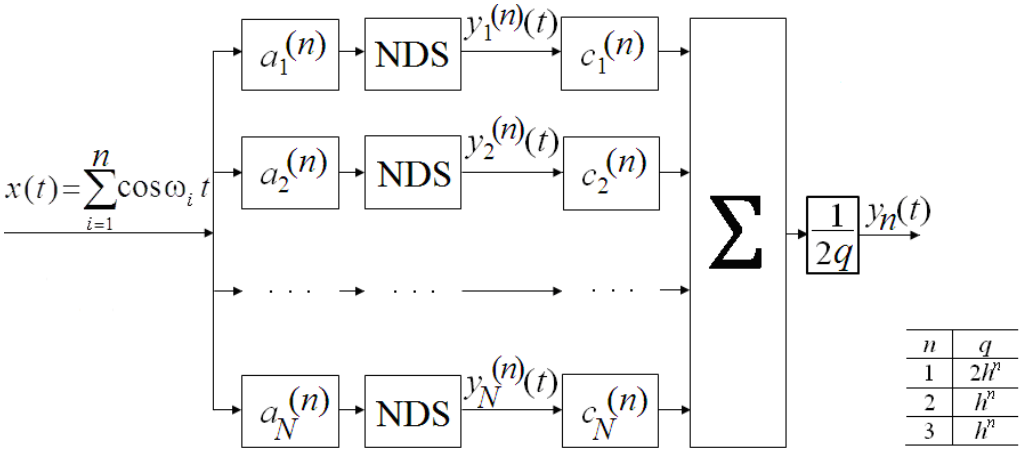


Fig. 2. The structure chart of identification using n-th order Volterra model in frequency domain using interpolation method

The weighted sum is formed from received signals – responses of each group (fig. 2). As a result the partial components of NDS responses $y_1(t)$, $y_2(t)$ and $y_3(t)$ are taken. For each partial component of response the Fourier transform (the FFT is used) is calculated and

only an informative harmonics (which amplitudes represent values of required characteristics of the 1, 2 and 3 order AFCs) are taken from received spectrum.

The first order AFC $|W_1(j\omega)|$ and PFC $\arg W_1(j\omega)$ are received by extracting the harmonics with frequency ω from the spectrum of the CC partial response $y_1(t)$ to the test signal $x(t) = (A/2)\cos\omega t$.

The second order AFC $|W_2(j\omega, j(\omega+\Omega_1))|$ and PFC $\arg W_2(j\omega, j(\omega+\Omega_1))$ having $\omega_1 = \omega$ and $\omega_2 = \omega + \Omega_1$ were received by extracting the harmonics with summary frequency $\omega_1 + \omega_2$ from the spectrum of the NDS partial response $y_2(t)$ to the test signal $x(t) = (A/2)(\cos\omega_1 t + \cos\omega_2 t)$.

The third order AFC $|W_3(j\omega, j(\omega+\Omega_1), j(\omega+\Omega_2))|$ and PFC $\arg W_3(j\omega, j(\omega+\Omega_1), j(\omega+\Omega_2))$ having $\omega_1 = \omega$, $\omega_2 = \omega + \Omega_1$ and $\omega_3 = \omega + \Omega_2$, were received by extracting the harmonics with summary frequency $\omega_1 + \omega_2 + \omega_3$ from the spectrum of the NDS partial response $y_3(t)$ to the test signal $x(t) = (A/2)(\cos\omega_1 t + \cos\omega_2 t + \cos\omega_3 t)$.

The results (first, second and third order AFC and PFC which had been received after procedure of identification) and the second and third order surfaces for AFC and PFC received after procedure of the test system identification are presented in [8].

The surfaces are built from sub–diagonal cross-sections which were received separately. Ω_1 was used as growing parameter of identification with different value for each cross–section in second order characteristics. Fixed value of Ω_2 and growing value of Ω_1 were used as parameters of identification to obtain different value for each cross-section in third order characteristics.

Numerical values of identification accuracy as a percentage RMSE using interpolation method for the test system are represented in Table 1, where: n – order of the estimated Volterra kernel, N – approximation order/number of interpolation knots (number of experiments). The comparisons to previous works are given in [9].

Table 1.

Numerical values of identification accuracy using interpolation method

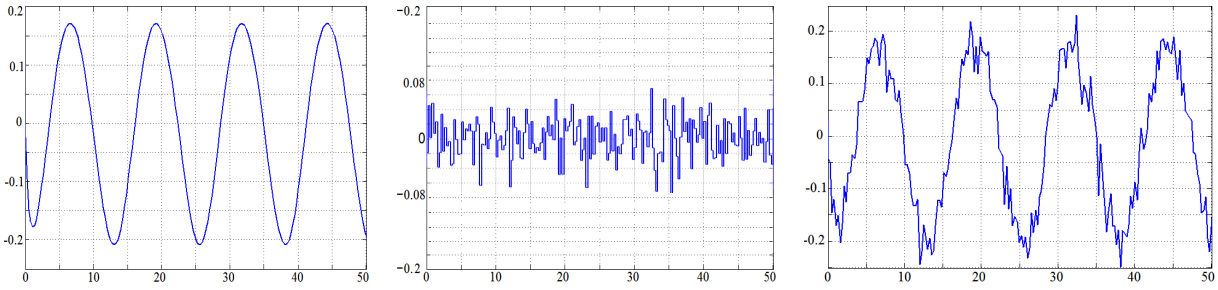
n	N	RMSE for AFC, %	RMSE for PFC, %
1	2	2.8853	2.1005
	4	0.5180	2.3964
	6	0.4075	2.3663
2	2	29.7526	89.3218
	4	2.0103	5.1023
	6	3.0488	7.8248
3	4	2.9299	11.0100
	6	11.0285	5.9724

Experimental researches of the noise immunity of the identification method were performed. The simulations with the test model were performed. Different noise levels were defined for different order of the Volterra model.

The main purpose was the studying of the noise impact (noise means the inexactness of the measurements) to the characteristics of the test system model using interpolation method of identification in frequency domain.

The first step was the measurement of the level of useful response signal (harmonic cosine test signal shown in fig. 3a) after test system (Out2 in fig. 4). The amplitude of this signal was defined as the 100% of the signal power.

After that procedure the Random Noise signal (with the form shown in fig. 3b) where added to the test system output signal. This steps where performed to simulate inexactness of the measurements in the model. The sum of these two signals for the linear test model signal is shown in fig. 3c.



a **b** **c**

Fig. 3. The sum of two signals for the linear test model signal: a – the NDS subchannel response, b – random noise with 50% amplitude of max amplitude of the response, c – "noised" responce of the test system

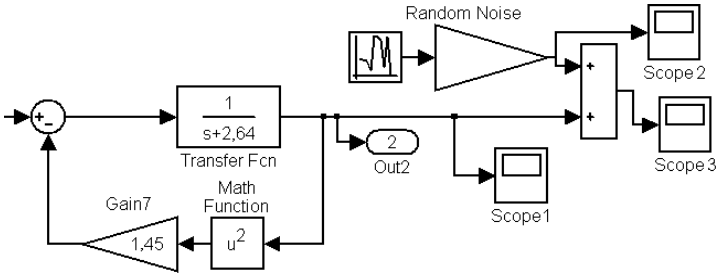
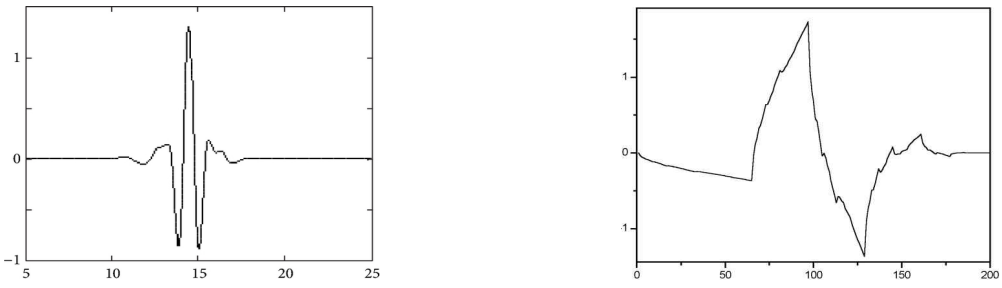


Fig. 4. The Simulink model of the test system with noise generator and osillosopes

After series of test researches it was decided to use Coiflet and Daubechie wavelets [2, 5, 7] due to its minimal distortion impact on form of filtered signal with RMSE minimization. The wavelet filtering was used to reduce the noise impact on final characteristics of the test system. The Coiflet-4 and Daubechie-3 of the 3 level were chosen (fig. 5) and used for the AFC and PFC filtering respectively.



a **b**

Fig. 5. The Coiflet (a) and Dubechie (b) and wavelet function

The first order (linear) model was tested with the level of noise 100% and 10% and showed excellent level of noise immunity. The standard, noised and de-noised (filtered) (fig. 6) characteristics (AFC and PFC) with level of noise 100% are presented.

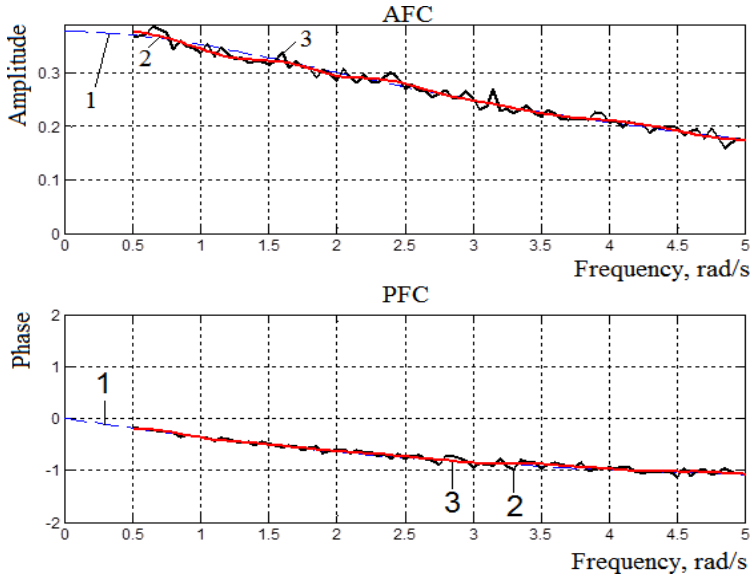


Fig. 6. The standard (1), noised (2) and denoised (3) characteristics (AFC – top, PFC – bottom) of the 1 order model of the test system with level of noise 100%

The second order (nonlinear) model was tested with the level of noise 10% and 1% and showed good level of noise immunity. The standard, noised and de-noised (filtered) (fig. 7) characteristics (AFC and PFC) with level of noise 10% are presented.

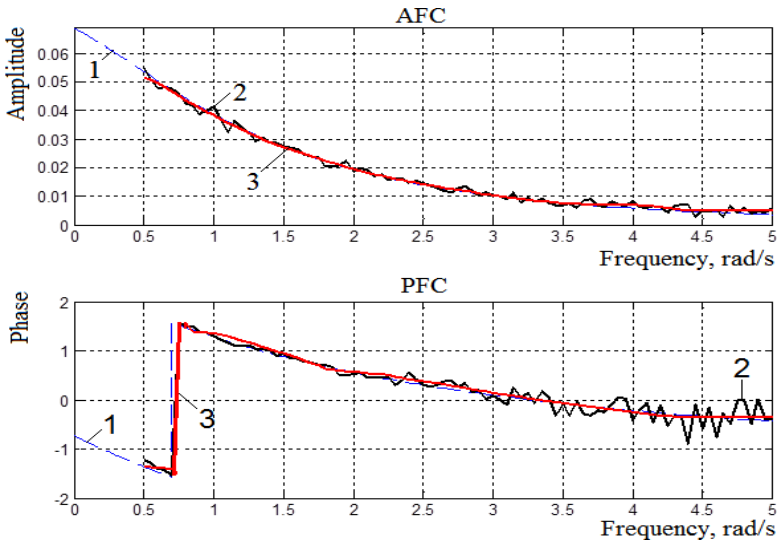


Fig. 7. The standard (1), noised (2) and denoised (3) characteristics (AFC – top, PFC – bottom) of the 2 order model of the test system with level of noise 10%

The third order (nonlinear) model was tested with the level of noise 10% and 1% and showed good level of noise immunity. The standard, noised and de-noised (filtered) (fig. 8) characteristics (AFC and PFC) with level of noise 1% are presented.

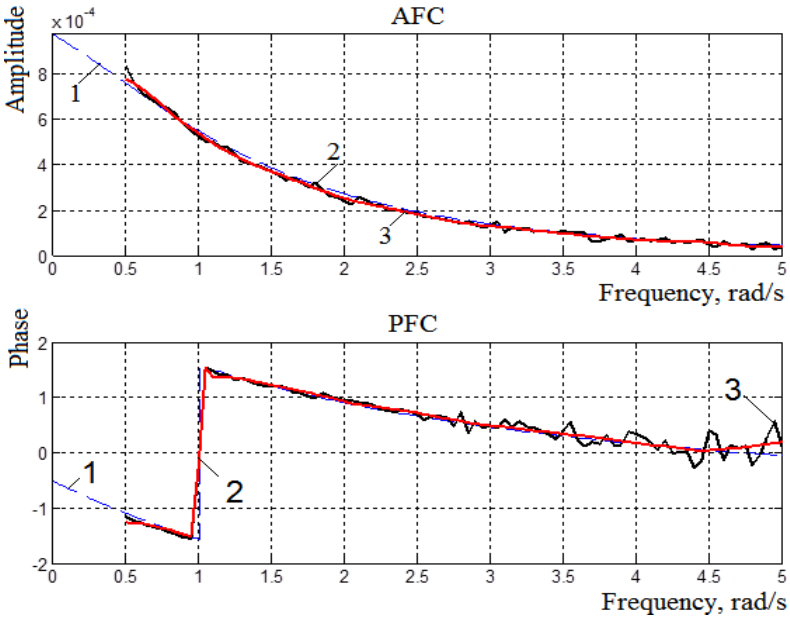


Fig. 8. The standard (1), noised (2) and denoised (3) characteristics (AFC – top, PFC – bottom) of the 3 order model of the test system with level of noise 0,1%

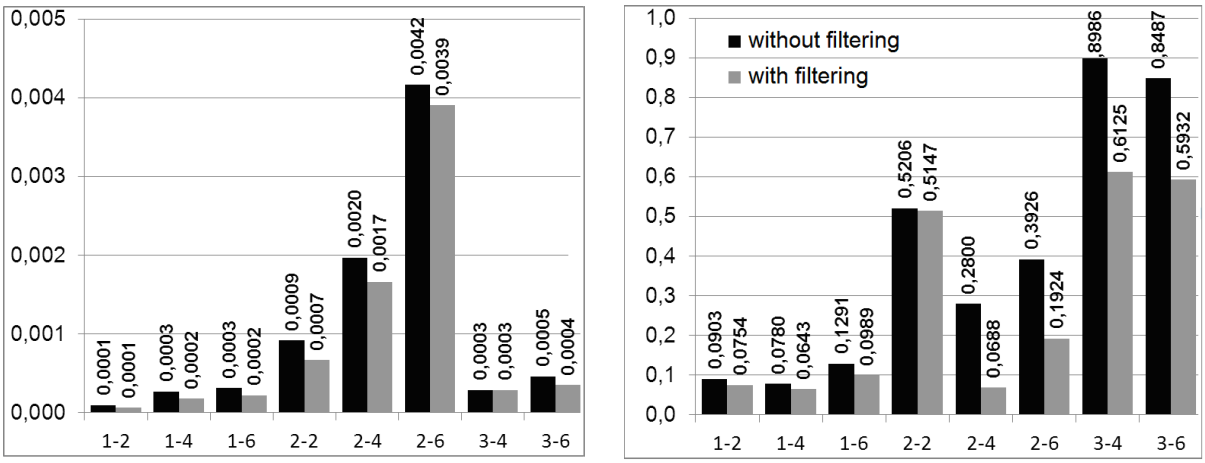
The numerical values of RMSE of the identification accuracy before and after wavelet filtering procedure are presented in Table 2.

Table 2.

Standard deviation for interpolation method with noise impact

n	*N*	Noise level = 10%		Noise level = 0,1%		Improvement	
		RMSE for AFC	RMSE for PFC	RMSE for AFC	RMSE for PFC	for AFC, times	for PFC, times
		(without / with filtering)					
1	2	0.000097 / 0.000063	0.09031 / 0.07541	–	–	1.540	1.198
	4	0.000271 / 0.000181	0.07804 / 0.06433	–	–	1.497	1.213
	6	0.000312 / 0.000223	0.12913 / 0.09889	–	–	1.399	1.306
2	2	0.000920 / 0.000670	0.52063 / 0.51465	–	–	1.373	1.012
	4	0.001972 / 0.001663	0.28004 / 0.06877	–	–	1.186	4.072
	6	0.004165 / 0.003908	0.39260 / 0.19237	–	–	1.066	2.041
3	4	–	–	0.000288 / 0.000288	0.89857 / 0.61251	1.003	1.467
	6	–	–	0.000461 / 0.000352	0.84868 / 0.59319	1.310	1.431

The diagrams showing the improvement of RMSE for identification accuracy using the wavelet filtering of the received characteristics for AFC and PFC are shown in fig. 9a and fig. 9b respectively.



a **b**

Fig. 9. RMSE changing for AFC (a) and PFC (b) using wavelet-filtering

Conclusion

The interpolation method used for nonparametric model building is based on Volterra model. The polyharmonic test signals are used for identification the nonlinear dynamical systems. The method based on linear combination of responses to the test signals with different amplitudes is used to differentiate the responses of system for partial components.

The provided results have confirmed nonlinearity of the test system. Selected values of test signal amplitudes and corresponding coefficients are raising greatly the accuracy of identification in compare to amplitudes and coefficients written in [1, 9]. The accuracy of identification of nonlinear part of the test system as RMSE is less than 3% for AFC and less than 6 % for PFC in best cases. This characterizes method as excellent one.

The noise immunity of the method is very high for the linear part and high enough for the nonlinear part of the model. The RMSE of noised characteristics doesn't overgrow 10% in best cases with 10% measurement inaccuracy. The wavelet filtering of the response and final characteristics of the nonlinear dynamical system is very effective and gives the possibility to improve the identification accuracy of the inexact measurements up to 1.54 and 4.07 times for the AFC and PFC respectively.

References

1. Danilov, L.V. The theory of nonlinear electrical circuits / L.V. Danilov, P.N. Mathanov, E.S. Philipov // Published Energoatomizdat, Leningrad – 1990 – 396 p.
2. Donoho, D.L. Threshold selection for wavelet shrinkage of noisy data / D.L. Donoho, I.M. Johnstone // Proc. 16th Annual Conf. of the IEEE Engineering in Medicine and Biology Society, 24a–25a, IEEE Press – 1994 – PP.128–139.
3. Doyle, F.J. Identification and Control Using Volterra Models / F.J. Doyle, R.K. Pearson, B.A. Ogunnaike // Published Springer Technology & Industrial Arts – 2001 – 420 p.
4. Giannakis, G.B. Bibliography on nonlinear system identification and its applications in signal processing, communications and biomedical engineering / G.B. Giannakis, E.A. Serpedin // Signal Processing, EURASIP, Elsevier Science B.V. 81(3) – 2001 – PP. 533-580.
5. Goswami, J.G. Fundamentals of Wavelets: Theory, Algorithms, and Applications / J.G. Goswami, A.K.Chan // Publishing John Wiley&Sons Inc – 1999 – 289 p.
6. Misiti, M. Wavelets Toolbox Users Guide / M. Misiti, Y. Misiti, G. Oppenheim, J-M. Poggi // The MathWorks Inc. Wavelet Toolbox, for use with MATLAB – 2000 – 137 p.

7. Pavlenko, V.D. Interpolation Method of Nonlinear Dynamical Systems Identification Based on Volterra Model in Frequency Domain / V.D. Pavlenko, S.V. Pavlenko, V.O. Speranskyy // Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013), 15–17 September 2013, Berlin, Germany – 2013. PP.173–178.
8. Pavlenko, V.D. Analysis of identification accuracy of nonlinear system based on Volterra model in frequency domain / V.D. Pavlenko, V.O. Speranskyy // American Journal of Modeling and Optimization – Vol.1, No.2 – 2013. PP.11–18. DOI: 10.12691/ajmo-1-2-2.
9. Pavlenko, V.D. Communication Channel Identification in Frequency Domain Based on the Volterra Model / V.D. Pavlenko, V.O. Speranskyy // Recent Advances in Computers, Communications, Applied Social Science and Mathematics. Proceedings of the International Conference on Computers, Digital Communications and Computing (ICDCC'11), Barcelona, Spain, September 15-17, 2011. Published by WSEAS Press – 2011. PP.218–222.
10. Sergeev, A.G. Metrologija / A.G. Sergeev, V.V. Krohin // M. : Logos, 2000. – 407 p.
11. Schetzen, M. The Volterra and Wiener Theories of Nonlinear Systems // Wiley&Sons, New York – 1980 – 245 p.
12. Westwick, D.T. Methods for the Identification of Multiple–Input Nonlinear Systems // Departments of Electrical Engineering and Biomedical Engineering, McGill University, Montreal, Quebec, Canada – 1995 – 312 p.

ЭФЕКТИВНІСТЬ ЗАСТОСУВАННЯ ВЕЙВЛЕТ–ФІЛЬТРАЦІЇ ДЛЯ ІДЕНТИФІКАЦІЇ НЕЛІНІЙНИХ СИСТЕМ НА ОСНОВІ МОДЕЛЕЙ ВОЛЬТЕРРА В ЧАСТОТНІЙ ОБЛАСТІ

В.О. Сперанський, В.Д. Павленко

Одеський національний політехнічний університет,
пр. Шевченка, 1, Одеса, Україна, 65044, e-mail: speranskiyva@ukr.net

Наведено результати досліджень ефективності вейвлет-фільтрації при застосуванні інтерполяційного метода ідентифікації нелінійних динамічних систем на основі моделі Вольтерра в частотній області. Досліджено точність та завадостійкість визначення амплітудно– і фазо–частотних характеристик першого, другого и третього порядків нелінійної системи за даними експерименту «вхід-вихід» за допомогою тестових полігармонічних сигналів. Підвищення завадостійкості методу ідентифікації досягнуто за допомогою вейвлет-фільтрації шумів вимірювань відгуків та отримуваних характеристик системи, що ідентифікують.

Ключові слова: вейвлет-фільтрація, ідентифікація, ефективність, завадостійкість, нелінійні динамічні системи, моделі Вольтерра, багатомірні АЧХ і ФЧХ, полігармонічні сигнали.

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ВЕЙВЛЕТ–ФИЛЬТРАЦИИ ДЛЯ ИДЕНТИФИКАЦИИ НЕЛИНЕЙНЫХ СИСТЕМ НА ОСНОВЕ МОДЕЛЕЙ ВОЛЬТЕРРА В ЧАСТОТНОЙ ОБЛАСТИ

В.А. Сперанский, В.Д. Павленко

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, Украина, 65044, e-mail: speranskiyva@ukr.net

Приводятся результаты исследования эффективности вейвлет-фильтрации при применении интерполяционного метода идентификации нелинейных динамических систем на основе модели Вольтерра в частотной области. Исследуется точность и помехоустойчивость определения амплитудно– и фазо–частотных характеристик первого, второго и третьего порядков нелинейной системы по данным эксперимента «вход-выход» с помощью тестовых полигармонических сигналов. Повышение помехоустойчивости метода идентификации достигается с помощью вейвлет-фильтрации шумов измерений откликов и получаемых характеристик идентифицируемой системы.

Ключевые слова: вейвлет-фильтрация, идентификация, эффективность, помехоустойчивость, нелинейные динамические системы, модели Вольтерра, многомерные АЧХ и ФЧХ, полигармонические сигналы.

УДК 681.3.067

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 26-34

ДОСЛІДЖЕННЯ СТАТИСТИЧНОЇ БЕЗПЕКИ МЕТОДІВ ВІДКРИТОГО РОЗПОДІЛУ СЕКРЕТНИХ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Ю.Є. Яремчук

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: yurevyar@vntu.net

Проведено дослідження статистичної безпеки методів відкритого розподілу секретних ключів відповідно на основі рекурентних U_k та V_k –послідовностей та здійснено їх порівняння з відомим методом Діффі-Хеллмана. Результати аналізу показали, що найвищий рівень статистичної безпеки має метод на основі V_k – послідовностей, пройшовши вдвічі більшу кількість тестів порівняно з методом Діффі-Хеллмана, у той же час метод на основі U_k –послідовностей пройшов у 1.5 рази більшу кількість тестів, ніж відомий аналог.

Ключові слова: криптографія, розподіл секретних ключів, криптостійкість, статистична безпека, рекурентні послідовності.

Вступ

Відкритий розподіл ключів [1] дозволяє двом сторонам виробляти спільний секретний ключ шляхом обміну відкритими повідомленнями без використання будь-якої заздалегідь виробленої спільної секретної інформації. При цьому жодна із сторін не може наперед визначити значення ключа, так як ключ залежить від повідомлень, що безпосередньо передаються в процесі обміну.

Вперше метод відкритого розподілу секретних ключів був запропонований Діффі та Хеллманом [2].

В роботі [3] представлено метод розподілу секретних ключів відкритим каналом, який базується на рекурентних V_k^+ та U_k –послідовностях. У порівнянні з відомим методом розподілу ключів Діффі-Хеллмана запропонований метод забезпечує для кожного користувача майже вдвічі меншу складність обчислень, а також має простішу процедуру завдання параметрів.

В роботі [4] запропоновано метод відкритого розподілу секретних ключів на основі математичного апарату лише рекурентних V_k –послідовностей, який, у порівнянні з методом представленим у роботі [3], забезпечив підвищення криптографічної стійкості розподілу ключів за рахунок отримання спільного ключа на завершальному етапі розподілу у вигляді елементу послідовності, обчисленого за мультиплікативним, а не адитивним способом зміни індексу.

При цьому актуальним залишається визначення рівня практичної стійкості шляхом дослідження статистичної безпеки запропонованих у [3] та [4] методів відкритого розподілу секретних ключів та порівняння їх з відомим аналогом.

Метою роботи є дослідження статистичної безпеки запропонованих у [3] та [4] методів відкритого розподілу секретних ключів на основі рекурентних U_k та V_k –послідовностей та порівняння їх з відомим методом Діффі-Хеллмана.

Дослідження статистичної безпеки методів розподілу секретних ключів на основі U_k та V_k –послідовностей

На сьогодні одним з кращих пакетів для статистичного тестування криптографічних схем та протоколів є розроблений у 1999 році пакет NIST STS (National Institute of Standard and Technologies Statistical Test Suite) [5], який був розроблений в рамках проекту AES (Advanced Encryption Standard) і включає у себе набір з 16 статистичних тестів, які на сьогодні найкращим чином відповідають висунутим вимогам щодо статистичного тестування криптографічних схем/протоколів.

Для дослідження методів розподілу ключів використаємо пакет NIST STS за такою методикою. Нехай задана двійкова послідовність S довжиною n бітів, тобто $S = \{S_1, S_2, ..., S_n\}$, $S_i \in \{0,1\}$. Для фіксованого значення n формуємо множину з m двійкових послідовностей. Сформована вибірка при цьому складатиме $N = m \times n$.

Далі будемо тестувати за допомогою пакету NIST STS кожну послідовність сформовану методом, в результаті якого отримаємо статистичний портрет сформованого секретного ключа.

Статистичний портрет послідовності являє собою масив розмірністю $m \times q$, де m – кількість послідовностей, що тестуються; q – кількість статистичних тестів, які використовуються для тестування кожної послідовності. Елементи масиву $P_{i,j} \in [0,1]$, де $i = \overline{1,m}$, $j = \overline{1,q}$, являють собою значення ймовірності, що отримана в результаті тестування i-ї послідовності j-м тестом.

За отриманим статистичним портретом визначаємо долю послідовностей, які пройшли кожен статистичний тест. Для цього задають рівень значимості $\alpha \in [0{,}001; 0{,}01]$ і здійснюють підрахунок значень імовірності P, що перевищує заданий рівень α для кожного з q тестів. У результаті формується вектор коефіцієнтів $R = \{r_1, r_2, ..., r_q\}$, елементи якого характеризують у процентному співвідношенні проходження послідовності S_i усіх статистичних тестів. Після цього здійснюється статистичний аналіз статистичного портрету. Отримані значення ймовірностей P_{ij} повинні задовольняти рівномірному закону розподілу на інтервалі $[0,1]$.

Заключний висновок стосовно методу розподілу секретними ключами будемо приймати таки чином. Вважатимемо, що метод розподілу секретних ключів G пройшов статистичне тестування пакетом NIST STS, якщо значення коефіцієнтів r_j для усіх $j = \overline{1,q}$ знаходяться всередині довірчого інтервалу $[r_{\max}, r_{\min}]$, де

$$r_{\max(\min)} = \hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}}, \text{ для } \hat{p} = 1 - \alpha, \qquad (1)$$

і дотримується умова $\chi^2 > 0.0001$ для усіх $j = \overline{1,q}$, де χ^2 – критерій підкорення результатів рівномірному закону розподілу на інтервалі $[0,1]$.

Тестування буде проходити для різних довжин ключів, а саме 1024, 2048 та 4096 бітів. Довжина послідовностей, які будуть отримуватись у результаті виконання

розподілу ключів буде 1024, 2048 та 4096 бітів відповідно. Дана довжина послідовностей дозволяє виконувати тестування лише для 11 тестів, що виключає тест на перевірку шаблонів, що перекриваються, універсальний тест Маурера, тест на перевірку стискання за алгоритмом Лемпеля-Зіва, тест на перевірку випадкових відхилень та модифікований тест на перевірку випадкових відхилень, так як необхідна довжина послідовностей, що проходять тестування, є недостатньою для успішного проходження чи отримання достовірних результатів даних тестів.

Для виконання тестування було обрано такі параметри:

- довжина послідовності n, що тестується, дорівнює 1024, 2048 та 4096 бітів відповідно до довжини ключа;
- кількість послідовностей, які тестуються для кожної довжини ключа, $m = 100$;
- кількість тестів $q = 159$;
- рівень значимості $\alpha = 0.01$ та $\alpha = 0.001$ відповідно у першому та другому експериментах.

Таким чином маємо: об'єм вибірки 102400, 204800 та 409600 бітів при тестуванні методу розподілу секретних ключів Діффі-Хеллмана; 204800, 409600 та 919200 бітів при тестуванні методу на основі U_k –послідовностей; 307200, 614400 та 1228800 бітів при тестуванні методу на основі V_k –послідовностей. Статистичний портрет коду для кожної довжини ключа буде вміщувати у собі 15900 значень імовірності P.

Застосовуючи правило довірчого інтервалу для r_j, обчислюємо значення нижньої границі за формулою (1). Тоді для $\alpha = 0.001$ та $\hat{p} = 1 - \alpha = 0.999$ $r_{\min}$ складе

$$r_{\min} = 0.999 \pm 3\sqrt{\frac{0.999(1-0.999)}{100}} = 0.98952,$$

а для $\alpha = 0.01$ та $\hat{p} = 1 - \alpha = 0.99$ $r_{\min}$ складе

$$r_{\min} = 0.99 \pm 3\sqrt{\frac{0.99(1-0.99)}{100}} = 0.96015.$$

Вибір додаткових параметрів зроблено у відповідності з рекомендаціями описаними в NIST STS [5].

На основі цих початкових даних проаналізуємо отримані результати тестування послідовностей. У таблицях 1 і 2 наводяться дані про проходження результуючих ключів з розміром 1024, 2048 та 4096 бітів усіма тестами згідно описаної методики.

З таблиць 1 та 2 видно, що при довжині ключа 1024 біти відсотки проходження тестів доволі малі. Такі низькі показники зумовлені малою довжиною послідовності, а більшість тестів розраховані на довжину від 100000 біт. Проте вже видно, що методи розподілу ключів на основі рекурентних послідовностей мають кращі показники порівняно з відомим методом Діффі–Хеллмана. Відсоток проходження тестів за методами на основі V_k та U_k –послідовностей при порозі проходження $\alpha = 0.01$ має незначне відхилення від відсотку проходження за методом на основі протоколу Діффі–Хеллмана, проте, у разі пониження порогу до $\alpha = 0.001$, відсоток проходження у 1.5 рази перевищує відсоток проходження методу на соснові протоколу Діффі–Хеллмана. Такі результати досягаються завдяки успішному проходженню більшості тестів для тесту перевірки шаблонів, які не перекриваються.

Таблиця 1.

Результати тестування методів розподілу ключів згідно описаної методики для $\alpha = 0.01$ та різних довжин ключів

Метод	Кількість тестів, які успішно пройшли тестування більше 99% послідовностей			Кількість тестів, які успішно пройшли тестування більше 96% послідовностей		
	1024 бітів	2048 бітів	4096 бітів	1024 бітів	2048 бітів	4096 бітів
Діффі-Хеллмана	8 (5.03%)	6 (3.77%)	12 (7.55%)	69 (43.40%)	67 (42.14%)	112 (70.44%)
U_k	5 (3.14%)	15 (9.43%)	18 (11.32%)	69 (43.40%)	115 (72.33%)	130 (81.76%)
V_k	6 (3.77%)	15 (9.43%)	24 (15.09%)	56 (35.22%)	116 (72.96%)	134 (84.28%)

Таблиця 2.

Результати тестування методів розподілу ключів згідно описаної методики для $\alpha = 0.001$ та різних довжин ключів

Метод	Кількість тестів, які успішно пройшли тестування більше 99% послідовностей			Кількість тестів, які успішно пройшли тестування більше 98% послідовностей		
	1024 бітів	2048 бітів	4096 бітів	1024 бітів	2048 бітів	4096 бітів
Діффі-Хеллмана	30 (18.87%)	59 (37.11%)	86 (54.09%)	75 (47.17%)	112 (70.44%)	136 (85.53%)
U_k	53 (33.33%)	83 (52.20%)	92 (57.86%)	113 (71.07%)	135 (84.91%)	141 (88.68%)
V_k	48 (30.19%)	81 (50.94%)	101 (63.52%)	99 (62.26%)	128 (80.50%)	150 (94.34%)

З таблиць 1 та 2 також видно, що при довжині ключа 2048 бітів спостерігається значний приріст у відсотках проходження тестів послідовностями згідно методів на основі U_k та V_k–послідовностей. Задаючи порогове значення $\alpha = 0.01$, тестування результату ключового розподілу для методів на основі як U_k так і V_k–послідовності показало набагато більший відсоток проходження тестів (у 2.5 рази) порівняно з послідовностями на основі протоколу Діффі-Хеллмана. Зі зменшенням порогового значення у 10 разів ($\alpha = 0.001$) відсоток проходження тестів послідовностями за методом Діффі-Хеллмана зріс, проте усе одно становив нижче (у 1.5 рази) за відсотки проходження тестів послідовностями на основі методів, що базуються на U_k та V_k–послідовностях.

При тестуванні послідовностей з довжиною ключа 4096 бітів відсотки проходження тестів збільшуються. З таблиць 1 і 2 видно, що відсоток проходження тестів послідовностями на основі V_k та U_k–послідовностей відповідно у 2 та 1.5 рази перевищує відсоток проходження тестів послідовностями для методу Діффі–Хеллмана при найжорсткішому порозі проходження (проходженням 99% послідовностей тестів для $\alpha = 0.01$).

Порівняємо коди з рівнем значимості $\alpha = 0.01$ до оцінки за приведеною методикою. В таблиці 3 наведено результати порівняння для різних довжин ключів.

Таблиця 3.

Відсотки проходження кожного з 11 тестів для $\alpha = 0.01$ та різних довжин ключів

№ тесту	Назва статистичного тесту	1024 бітів			2048 бітів			4096 бітів		
		Д-Х	U_k	V_k	Д-Х	U_k	V_k	Д-Х	U_k	V_k
1	Частотний (монобітний) тест	100%	100%	100%	100%	100%	100%	99%	99%	100%
2	Частотний тест всередині блоку	98%	99%	99%	100%	100%	98%	100%	99%	100%
3	Послідовний тест	97%	99%	97%	96%	99%	100%	99%	98%	99%
4	Перевірка максимальної довжини серії в блоці	100%	100%	99%	98%	99%	99%	98%	100%	98%
5	Перевірка рангу двійкової матриці	100%	95%	97%	99%	98%	100%	100%	99%	98%
6	Спектральний тест на основі дискретного перетворення Фур'є	100%	98%	100%	95%	98%	96%	100%	99%	99%
7	Перевірка шаблонів, які не перекриваються	96%	96%	95%	96%	97%	97%	97%	98%	98%
8	Перевірка лінійної складності	94%	93%	97%	94%	98%	95%	95%	99%	100%
9	Перевірка серій	99%	98%	98%	99%	99%	100%	97%	99%	100%
10	Ентропійний тест	96%	100%	98%	97%	100%	100%	100%	98%	98%
11	Перевірка накоплених сум	100%	100%	100%	100%	100%	100%	100%	100%	100%

Як видно з результатів табл. 3, найкращі показники знову отримав метод на основі V_k –послідовностей. Найслабкішим метод виявився у тестах на перевірку лінійної складності, спектральному тесті на основі дискретного перетворення Фур'є та тесті перевірці шаблонів, які не перекриваються. В останніх тестах метод Діффі-Хеллмана має ще нижчі показники (94–97%) порівняно з методами на основі U_k (93–100%) та V_k (95–100%) – послідовностей, хоча при розмірі ключа 2048 бітів метод на основі U_k –послідовностей показав найгірші (93%) показники в тесті перевірки

лінійної складності, що свідчить про те, що отриманий в результаті тестування розподіл відрізняється від очікуваного.

Отримано також результати проходження тестів і для $\alpha = 0.001$, які показали більші відсотки проходження тестів. Проведено також порівняння, яке показало, що метод Діффі-Хеллмана має нижчі показники (94–99%) порівняно з методами на основі U_k (99–100%) та V_k (99–100%) – послідовностей у тестах на перевірку шаблонів, що не перекриваються та перевірку лінійної складності. Хоча, при розмірі ключа 4096 біт, 100% проходження усіх тестів отримав саме метод на основі V_k –послідовностей, що говорить про його кращу статистичну безпеку.

Узагальнимо результати тестування, показавши частку проходження для кожного тесту із статистичного пакету NIST. На рисунках 1–3 показані графіки з узагальненими результатами тестування по кожному тесту для кожного методу та довжини ключа.

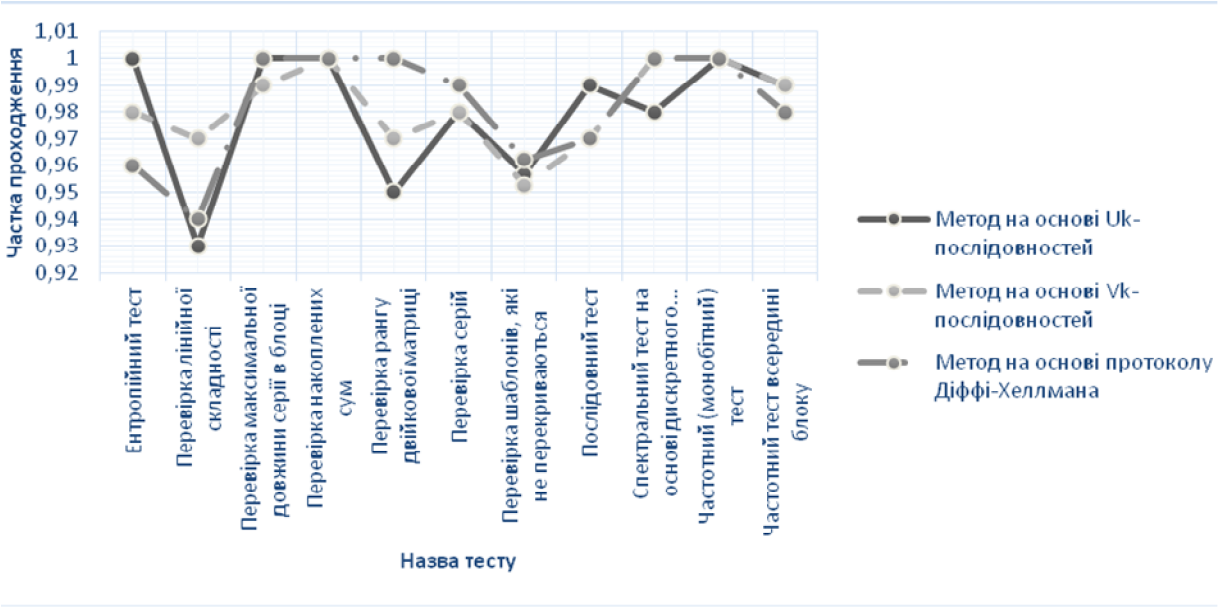


Рис. 1. Частка проходження тестів для послідовностей з розміром ключа 1024 біти

Як видно з графіку рис. 1, методи на основі U_k та V_k –послідовностей для довжини ключа 1024 бітів показали кращі результати в усіх тестах окрім тесту на перевірку рангу двійкової матриці. В усіх інших тестах отримані результати кращі, або на такому ж рівні, як і в методі Діффі-Хеллмана. Найгірше себе показав метод на основі U_k –послідовностей у тесті на перевірку лінійної складності та перевірку рангу двійкової матриці, а метод на основі V_k –послідовностей в усіх тестах мав показники або найвищі, або такі, що мали незначно менше значення за найвищий показник. Тобто метод розподілу секретних ключів на основі V_k –послідовностей для довжини ключа у 1024 бітів має найкращі показники як генератора ПВП.

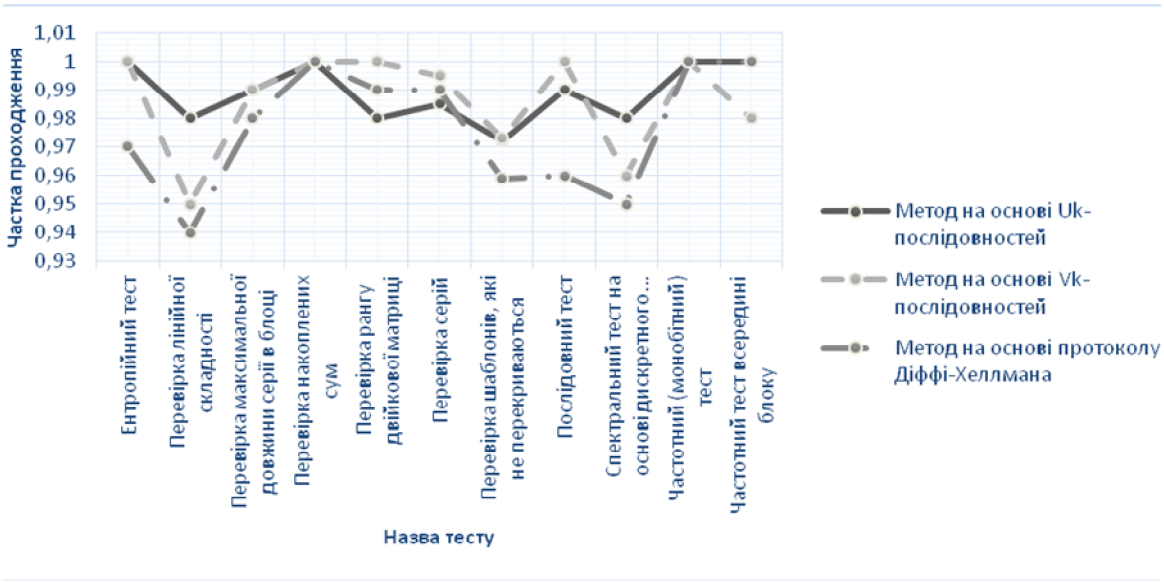


Рис. 2. Частка проходження тестів для послідовностей з розміром ключа 2048 біти

Як видно з рис. 2, при збільшені довжини ключа частка проходження усіх тестів збільшується, що є гарним показником, який свідчить про якісне збільшення статистичної безпеки створених ключів. При цьому метод Діффі-Хеллмана має найгірші (на 0.01 менші) показники вже з більшості тестів порівняно з попереднім розміром ключа у 1024 біти. В таких тестах як перевірка лінійної складності та спектральний тест на основі дискретного перетворення Фур'є найвищі показники (на 0.02–0.03 більше) показав метод на основі U_k–послідовностей. У більшості тестах частка проходження тестів послідовностями на основі V_k–послідовностей мають однакові з іншими або вищі (на 0.01) частки проходження тестів. В середньому, за рівномірною ламаною часток проходження можна прийняти рішення, що послідовності на основі V_k–послідовностей мають більш рівномірні характеристики, що є гарним показником як для генератора ПВП.

З рис. 3 видно, що послідовності за методом Діффі-Хеллмана продовжують програвати послідовностям за методами на основі U_k та V_k–послідовностей, показуючи найнижчу частку проходження у 0.95 не лише в одному тесті перевірки лінійної складності, а й усього графіка в цілому. Частки проходження тестів послідовностями за методом на основі U_k–послідовностей є рівномірними (0.98–1), проте місцями мають найгірші результати (послідовний тест і частотний тест в середині блоку). В більшості тестах частка проходження тестів послідовностями за методом на основі V_k–послідовностей також коливається у діапазоні 0.98–1, проте найгірший результат присутній тільки в одному тесті, а саме перевірці рангу бінарної матриці. В усіх інших результатах метод на основі V_k–послідовностей показує або однакові або кращі показники, що свідчить про високий рівень статистичної безпеки.

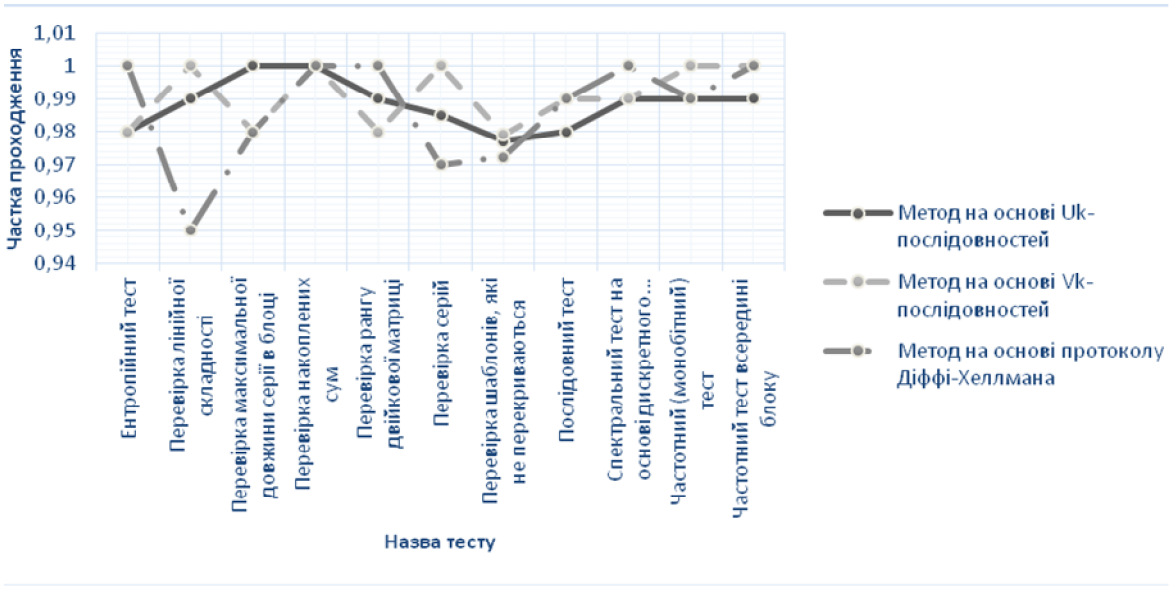


Рис. 3. Частка проходження тестів для послідовностей з розміром ключа 4096 біти

Висновки

Дослідження показало, що зі збільшенням довжини ключа в методах на основі V_k та U_k –послідовностей суттєво збільшується і статистична безпека отриманих послідовностей. Так, якщо при довжині ключа у 1024 біти послідовності успішно пройшли лише 6 (3.77%) та 5 (3.14%) тестів відповідно, то при ключі у 2048 біти ці показники зросли у 2.5 рази і вже становили 15 (9.43%) в обох випадках. При тестуванні з більш жорстким рівнем значимості $\alpha = 0.01$ та рівнем проходження тестів у 99% метод розподілу секретних ключів на основі V_k –послідовностей з довжиною ключа 4096 бітів пройшов 24 тести з 159 тестів, в той час як метод на основі протоколу Діффі-Хеллмана лише 12, що вдвічі перевищує рівень статистичної безпеки відомого аналогу. При цьому метод на основі U_k –послідовностей показав нижчі результати порівняно з методом на основі V_k –послідовностей (18 з 159 тестів), проте і вони кращі за результати тестування методу Діффі-Хеллмана, що робить методи на основі V_k та U_k –послідовностей одними з кращих аналогів щодо стійкості серед існуючих методів розподілу секретних ключів.

При порівнянні результатів тестування з рівнем значимості $\alpha = 0.01$ найкращі показники показав метод на основі V_k –послідовностей. Найменшу статистичну стійкість має метод Діффі-Хеллмана з показниками (94–97%) порівняно з методами на основі U_k (93–100%) та V_k (95–100%) – послідовностей.

У цілому результати тестування показують, що запропоновані методи розподілу секретних ключів на основі V_k та U_k –послідовностей мають високі показники статистичної безпеки порівняно з відомим методом Діффі-Хеллмана. Найвищий рівень статистичної безпеки має метод на основі V_k –послідовностей, який пройшов удвічі більшу кількість тестів порівняно з методом Діффі-Хеллмана, при цьому метод на основі U_k –послідовностей пройшов у 1.5 рази більшу кількість тестів, що теж є гарним результатом.

Список літератури

1. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone – CRC Press, 2001. – 816 p.
2. Diffie, W. New directions in cryptography / W. Diffie, M.E. Hellman. // IEEE Transactions on Information Theory. – №22, 1976. – Pp. 644–654.
3. Яремчук, Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем / Ю.Є. Яремчук // Захист інформації. – №4, 2012. – С. 120–127.
4. Яремчук, Ю.Є. Метод відкритого розподілу секретних ключів на основі рекурентних послідовностей / Ю.Є. Яремчук // Інформаційна безпека. – №2, 2013. – С. 177–183.
5. NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / [A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo]. – National Institute of Standards and Technology, 2010. – 131 p.

ИССЛЕДОВАНИИЕ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ МЕТОДОВ ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ СЕКРЕТНЫХ КЛЮЧЕЙ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю.Е. Яремчук

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: yurevyar@vntu.net

Проведены исследования статистической безопасности методов открытого распределения секретных ключей соответственно на основе рекуррентных U_k и V_k –последовательностей и осуществлено их сравнение с известным методом Диффи-Хеллмана. Результаты анализа показали, что наиболее высокий уровень статистической безопасности имеет метод на основе V_k –последовательностей, который прошёл вдвое большее количество тестов по сравнению с методом Диффи-Хеллмана, в то же время метод на основе U_k –последовательностей прошел в 1.5 раза большее количество тестов, чем известный аналог.

Ключевые слова: криптография, распределение секретных ключей, криптостойкость, статистическая безопасность, рекуррентные последовательности.

RESEARCH A STATISTICAL SECURITY METHODS OF PUBLIC DISTRIBUTION OF SECRET KEYS BASED ON RECURRENT SEQUENCES

Yuri E. Yaremchuk

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: yurevyar@vntu.net

The research are conducted for statistical security of public distribution of secret keys based on recurrent U_k and V_k sequences and performed their comparison with the known method of Diffie-Hellman. The analysis showed that the highest level of security is a statistical method based on V_k sequences, having twice the number of tests compared with the Diffie-Hellman method, while at the same time, the method based on the U_k sequences was 1.5 times greater number of tests than the known analogue.

Keywords: cryptography, distribution of secret keys, cryptographic reliability, statistical security, recurrent sequences

УДК 004.056:004.7

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 35-43

ДИНАМІКА КІЛЬКОСТІ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

І.В. Кононович

Одеська національна академія харчових технологій
вул. Канатна, 112, м. Одеса, 650039, Україна; e-mail: kononovich@mail.ru

В статті розглядається динаміка інцидентів інформаційної безпеки інфокомунікаційних мереж, запропоновано гіпотезу щодо її коливального характеру та розроблена модель «зловмисник-захисник» на основі моделі Лоткі – Волтерра. Отримані результати дозволяють підвищити ефективність роботи систем інформаційної безпеки та формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем інформаційної безпеки інфокомунікацій з використанням методів нелінійної динаміки.

Ключові слова: інформаційна безпека, інциденти, нелінійна динаміка, комп'ютерне моделювання, інформаційно-комунікаційні мережі

Вступ

Інформаційна безпека критично важливих інфраструктур держави, зокрема, кібербезпека інформаційно-комунікаційних систем (інфокомунікацій), увійшла в число найбільш значимих задач науки і практики. Інфокомунікації стали складними і постійно змінюються. Динамічний характер об'єкта захисту приводить до труднощів аналітичного описання систем інформаційної безпеки. Це ставить, за словами Д. У. Гіббса, «одною з головних цілей теоретичного дослідження – знайти точку зору, з якої предмет представляється найбільш простим [1; епіграф до § 1.2]». Методичною основою для створення моделей і теорії динаміки кількості інцидентів інформаційної безпеки можуть стати нелінійна динаміка та комп'ютерне моделювання.

Основними математичними моделями в теорії захисту інформації, які з 90-х років минулого століття є «доказовою теоретичною базою для побудови сучасних систем захисту інформації» і класифікація яких дана в [2; § 4.4], стали: для дискреційної політики безпеки – модель Харісона – Руззо – Ульмана, модель Take-Grant; для мандатної політики та моделей безпеки інформаційних потоків – модель конфіденційності Белла-ЛаПадула, модель цілісності Біба, модель Байба, модель Кларка Вілсона, див. [3; § 3.3-3.5]; для ймовірнісних моделей – модель системи безпеки з повним перекриттям, ігрова модель, ланкова модель Байба. Популяризуються також моделі, що дозволили внести нові вклади Юдіним О.К., Корченко О.Г. та Конаховичем Г.Ф. у оцінку ефективності захисту інформаційних ресурсів – узагальнені концепції побудови систем безпеки інформації, структурні моделі організації систем безпеки мереж, див. [4; § 7.2-7.5], та інші.

В цілому моделі охоплюють функціональні аспекти, детермінований та, частково, стохастичний характер функціонування систем безпеки. Динамічні аспекти процесів, характерні для процесів різних видів безпеки та катастроф, розглядаються із застосуванням методів нелінійної динаміки у піонерській роботі російських вчених під редакцією Малінецького Г.Г. [1].

Перелік літератури з нелінійної динаміки (синергетики), починаючи з робіт її основоположників Г. Хакена та І. Пригожина і до робіт нинішньої пори, див. [5], став

неоглядним. При цьому, багато дослідників відмічають застосовність методів нелінійної динаміки до вирішення задач у багатьох галузях на стику фізики і хімії [6], біології, екології [7], соціології й економіки [8], психології, управління [9]. Успішність побудови основ математичної теорії безпеки та ризику [1], феноменологічних моделей не рівноважних соціально-економічних систем [8], та багатьох інших, обумовлені переносом моделей фізико-хімічних реакцій у дані галузі та використанням нелінійної динаміки й комп'ютерного моделювання.

Що стосується досліджень загальної динаміки процесів забезпечення інформаційної безпеки та кібербезпеки у складних інформаційно-комунікаційних системах (ІКС) та мережах, то таких досліджень поки що не достатньо.

Метою даної роботи є підвищення ефективності розробки систем інформаційної безпеки ІКС за рахунок створення й аналізу моделей нелінійної динаміки інцидентів інформаційної безпеки.

Обґрунтування методики досліджень

Застосування методів нелінійної динаміки для моделювання процесів забезпечення інформаційної безпеки надає ряд можливостей та умов. Система інформаційної безпеки ІКС є складною системою. Для спрощення моделі застосовують процедури редукції. «В основі таких процедур – поділ динамічних змінних на групи у відповідності з характерними у часі перемінами змінних, оцінюваних у рамках окремо взятого рівняння із повної системи, див. [10; вступ, с. 26]». У системі виділяють дуже швидкі за часом та дуже повільні процеси. Тоді повільно змінювані процеси можна вважати стаціонарними і в описаннях моделі повільно змінювані змінні замінити на їх стаціонарні значення. Таким способом вдається звести змістовне описання об'єкта до двох – трьох диференційних рівнянь. «Хорошою рисою таких моделей ... являється наявність невеликого числа базових моделей, дослідження яких дозволяє ефективно будувати та вивчати великі класи моделей різноманітних явищ. ... Можна будувати вкрай прості нелінійні математичні моделі, які являються глибокими і змістовними [11; с. 19]».

«Існує практичний спосіб редукції системи рівнянь (великої розмірності) до рівнянь набагато меншої розмірності, що надає можливість дати змістовне описування об'єкта на основі усього тільки двох-трьох диференційних рівнянь. Принцип редукції сотень, рівнянь до системи рівнянь набагато меншої розмірності основується на принципі простоти, див. [8; вступ, § 4] принципі мінімуму та «вузького місця», див. [8; вступ, § 2]». У таких системах можуть виникати структури колективної поведінки ... та можливі автоколивальні процеси, див. [8; вступ, § 6], а також «мають місце степенні закони розподілу та явища самоорганізованої критичності, див. [1; глава 2, § 3]».

Система інформаційної безпеки ІКС є відкритою не рівноважною системою в тому смислі, що вона активно обмінюється із своїм оточенням інформацією. Основним математичним апаратом є якісна теорія диференційних рівнянь. Синергетичний підхід та відповідні моделі можуть стати важливим елементом досліджень масштабних систем інформаційної безпеки.

Розглянемо однорідну мережу із K об'єктів (комп'ютерів). Нехай на кожному з об'єктів є L уразливостей. Так що у мережі сумарно є

$$z = K \cdot L \qquad (1)$$

уразливостей. Візьмемо систему, яка складається із множини об'єктів захисту на вузлах мережі, які мають вразливості, із зловмисників, які створюють потік атак на мережу, із працівників служби безпеки, які виявляють і протидіють атакам та ліквідують виявлені вразливості. Атака закінчується зломом системи, якщо у мережі знаходиться хоча б

одна із уразливостей, відповідно. Інтерес успішних зловмисників полягає у тому, щоб було багато вразливостей (і працівників служби безпеки, бо число останніх свідчить про цінність інформаційних ресурсів, які захищаються). Інтерес одного працівника служби безпеки полягає у відсутності зловмисників. Інтерес корпорації працівників служби безпеки вимагає деякої малої кількості зловмисників для підтримки професійного рівня працівників. Повна відсутність зловмисників приводить до ліквідації служби безпеки. «Інтерес» уразливостей вимагає, щоб працівників служби безпеки було мало. Задача працівників служби безпеки полягає у ліквідації вразливостей. Інтерес усієї системи вимагає підтримання мінімальної чисельності зловмисників, працівників служби безпеки і вразливостей. У такій постановці задача схожа на задачі, які вирішуються у класичній моделі «хижак - жертва». У біології ця модель вивчається з метою визначення умов, за яких підтримується екологічно рівноважна кількість взаємозалежних популяцій при заданих природних ресурсах та екологічної рівноваги. У нашому випадку представляє інтерес аналіз умов за яких мінімізується кількість уразливостей і, відповідно, атак.

Конструювання моделі динамічних процесів інформаційної безпеки

Відносно змінної z – сумарної кількості вразливостей у мережі (1), можна сказати наступне. Відомо, за даними ЗМІ, що кількість помилок, які залишались у перших версіях операційної системи (ОС) Windows, було близько 200. У сучасних версіях ОС помилок, які призводять до вразливостей від атак, значно більше за об'єктивних причин. Доказом цього є нескінченний потік оновлень, які розсилаються на комп'ютери легальних користувачів. Розміри програмного коду стали настільки гігантськими, що повне тестування ОС стало неможливим за показниками часу і вартості [12; § 9.2, рис. 9.1]. А методи автоматизованого генерування надійних програм та методологія створення проактивних систем інформаційної безпеки, розвинуті поки що недостатньо [13,14]. З моменту початку експлуатації ОС число помилок у системі поступово зменшується. Помилки знаходять і виправляють розробники, а також добросовісні користувачі. За помилками полюють зловмисники. Потік спроб зловмисників знайти вразливість є стохастичним. Але слід вважати, що якщо у мережі є вразливість, то вона, рано чи пізно, буде знайдена і використана для атаки. Тому функцію потоку атак будемо пов'язувати із функцією числа вразливостей не стохастичними, а детермінованими залежностями.

У пропонованій моделі динамічних процесів інформаційної безпеки ресурсом будемо вважати вразливості системи інформаційної безпеки, характеристикою яких буде загальне число вразливостей (незалежно від їх типу). Початкову кількість уразливостей можемо обчислювати за формулою $z = n \cdot N$, де n – кількість уразливостей в ОС; N – кількість інсталяцій даної операційної системи. Між хакерами та персоналом служби безпеки йде боротьба за кінчений ресурс. Хакери споживають ресурс-вразливості для здійснення атак. Служби безпеки виявляють атаки, аналізують вразливості й закривають або ліквідують ресурс-вразливості.

Система, що розглядається, є системою із запізнюванням. Запізнювання виникає внаслідок проведення роботи по аналізу атак: виділення характерного «синдрому» вірусу чи атаки, виявлення та ліквідація вразливості тощо. Запізнення виникає і як соціально-психологічне явище, наприклад, за необхідності навчання користувачів, фахівців та осіб, що приймають рішення. «Тут ми стикаємося з ефектом Касандри, про який майже завжди згадують очевидці найбільших лих – багато, а інколи й більшість людей не слідують застереженням, ігнорують попередження щодо небезпеки і завчасно не розпочинають ніяких заходів, які допомогли б їм врятуватись, див. [1; вступ, § 3]». Тут мало знати закономірності, передбачати інциденти з безпекою, створювати механізми захисту. Треба домогтись, щоб це було зрозуміло людям і ними

використано. Ще однією причиною запізнювання є прискорення зміни технологій і звикання до них. Згідно концепції лауреата Нобелівської премії Алвіна Тоффлера «... існує гранична швидкість сприймання людиною змін [1; глава 1, § 3]». А за час одного покоління зараз змінюють одна одну декілька технологій. Люди, особливо старшого віку, можуть мати труднощі з перенавчанням і сприйманням нових загроз.

У даному разі може постати питання, чи правомірний перехід до розгляду мережі, а точніше до «колективу» об'єктів захисту, замість того, щоб надійно захистити кожен об'єкт окремо. Тоді, так здавалося б, що й загальна безпека буде забезпечена. Але стан інформаційної безпеки сьогодні не дозволяє самостійно забезпечити надійний захист. Виявлення та протидія атакам на комп'ютерну мережу не під силу окремим її вузлам. Крім того, «поняття безпеки є системним. Воно залежить від того, які системи ми аналізуємо, а які для нас байдужі та розглядаються як зовнішнє оточення. ... Під системою будемо розуміти циклічну або поліциклічну систему зв'язків, здатну підтримувати власне існування. Здатність до такої самопідтримки або гомеостазу за допомогою циклічної структури зв'язків і будемо розглядати як основну прикмету системи. ...

Безпекою системи будемо називати відсутність можливих порушень (або відсутністю причин, що викликають порушення) гомеостазу системи на протязі деякого проміжку часу [1; глава 2, § 4]». Там же стверджується: «Якщо останню сукупність (мережу, – K) розглядати як складне системоутворююче середовище, то прийдемо до висновку, що прості системи можуть існувати лише у складному середовищі, а у простих середовищах системи повинні бути складними. ... Для підтримки гомеостазу, тобто для компенсації несприятливих зовнішніх впливів (або для розривання небажаних зв'язків), системі потрібна деяка мінімальна складність. Певне, чим складніша система, тим більше впливів вона здатна компенсувати. Якщо система не достатньо складна, щоб вижити у ризикованому середовищі, то вона виживає не одиничними особинами, а колоніями, великими групами. ... Мабуть, таким чином добирається потрібна складність. Цінність однієї особини невелика, смертність висока, колонія існує за рахунок високої швидкості розмноження. ... Дещо такого роду відтворюють моделі типу хижак-жертва».

Також, згідно закону У. Росс Ешбі щодо необхідного різноманіття: «Кількість регулювання має бути не меншою різноманіття збурень, проти якого направлене регулювання [15; глава 11/8-11/10, гл.13/1]». Складність поведінки системи протидії повинна перевищувати складність поведінки атакуючої системи. Звідси випливає і висловлювання Є.А. Касперського щодо «важливості складних технологій в епоху складних атак [16]». Підтвердженням сказаного може служити протікання боротьби з вірусами, під час якої нормалізувати ситуацію (за виключенням «бойових вірусів») вдалося, створивши централізовані служби, де концентровані досвідчені спеціалісти з аналізу вірусів, і розгалужену систему розсилки актуальних баз даних «синдромів» цих вірусів й оперативної модифікації засобів антивірусного захисту.

Оскільки загрози стали виходити від багатоелементної системи, то для аналізу систем протидії природним є використати методи синергетики або нелінійної динаміки. Саме синергетика як теорія сумісних дій, вивчає виникнення у складної системи, що складається із взаємодіючих елементів, нових властивостей, якими окремі елементи не володіють.

Історично першою найпростішою лінійною моделлю у цій області була модель народонаселення, запропонована у 1798 р. Т. Мальтусом, і вирішеною ще у 1202 р. Л. Фібоначчі [10; глава 2.3, пример 2]:

$$\frac{dN}{dt} = \alpha N,\ N(0) = N_0,\ \alpha = const > 0. \qquad (2)$$

Фізичний смисл моделі у тому, що швидкість росту населення, за відсутності стримуючих факторів або протидії, пропорційна чисельності населення N. Вирішенням цього рівняння є $N(t) = N_0 e^{\alpha t}$. Вирішення має сингулярність: $N(t) \to \infty$ при $t \to \infty$. Модель можна застосувати для описування росту населення, біологічних вірусів, а також росту числа комп'ютерних вірусів в умовах, коли нема ніякого антивірусного захисту й віруси мають необмежений доступ до потрібних їм ресурсів середовища.

В реальних умовах є обмеження росту – або закінчуються ресурси, коли заражені всі комп'ютери, або віруси знищуються, коли проти них ведеться боротьба. «У 1835 р. Л.А. Кетле і П.Ф. Ферхюльст, а в 1920 р. повторно Р. Пірл і Л.Д. Рід, відкрили, що чисельність виду N змінюється у відповідності з законом, який задається логістичним рівнянням

$$\dot{N} = r\left(1 - \frac{N}{K}\right)N, \tag{3}$$

де K – середній розмір популяції;

N – чисельність популяції;

r – мальтузіанський коефіцієнт лінійного росту.

Середній розмір популяції – K залежить від ємності середовища, тобто від кількості їжі, розміру ареалу заселення. Логістичний закон добре описує динаміку росту простих біологічних і комп'ютерних вірусів, див. [1; глава 9, § 1.1]». Але логістичний закон не застосовний для моделювання більшості інших видів атак на комп'ютерні мережі, бо не враховує фактор запізнення.

Результати, отримані в нелінійній динаміці, дозволяють сформулювати наступну гіпотезу.

Довгострокові процеси забезпечення інформаційної безпеки, як і процеси у численних складних природних системах, можуть мати коливальний, циклічний характер і мають періоди зростання і спадання. Одним із механізмів коливальності пов'язаний з тим, що система забезпечення інформаційної безпеки являється системою із запізненням. В них результат впливу позначається не відразу, а через певний час h – час запізнення. На вироблення заходів протидії та їх впровадження витрачається певний час. Так, хвилі нових вірусів встигають розповсюдитись, поки не будуть оновлені всі антивірусні засоби.

Для описування систем, що схильні до різких циклічних коливань «у 1948 р. Г.Хатчинсон запропонував наступне узагальнення рівняння (3):

$$\dot{N} = r\left(1 - \frac{N(t-h)}{K}\right)N(t), \tag{4}$$

де h – час запізнення.

Введення додатної постійної h – це спроба врахувати фактор запізнення. Рівняння описує наступну ситуацію: вид заселений у однорідному середовищі, міграційні фактори не суттєві, мається задана кількість їжі, яка відновлюється при зменшенні численності популяції, див. [1; гл.9, § 1.1, формула (3)]». Ситуація з комп'ютерним вірусом описується у такій моделі так: комп'ютерний вірус розповсюджується у однорідній комп'ютерній мережі, є задана кількість комп'ютерів, які можуть бути заражені. Рішення рівняння (4) має періодичний коливальний характер. Його аналіз є предметом іншої роботи. Тут лише зробимо зауваження, що період коливальних процесів у системах із запізненням може бути значно більшим, ніж час запізнення. Для випадку, що розглядається у цій роботі, більш придатна модель

«хижак - жертва». Існують численні добре вивчені модифікації цієї моделі. Задача зводиться до вибору модифікації моделі, удосконалення її та адекватної інтерпретації у термінах систем інформаційної безпеки.

Із декількох різновидів моделі «хижак-жертва» (див. [1; § 5.1, формула (29)] та [17; упражнения 1.15, 4.9, 4.12]) оберемо як зразок модель Лоткі – Волтерра, удосконалений варіант якої описано та проаналізовано аналітично у [1, ; глава 9, § 5.1, формула (29)] та [18; формула 1]. Покажемо, що цю модель можна удосконалити, перетворивши її у модель «хакер - захисник». Позначимо за x – кількість атак на комп'ютерну мережу, що виконуються зловмисниками, це аналог «жертв»; за y – кількість операцій, що виконуються захисниками комп'ютерної мережі, це аналог «хижаків»; за z – кількість уразливостей у мережі, ця змінна характеризує «ресурси». Кількість уразливостей у комп'ютерах, які можуть бути атаковані, враховується у «ресурсах» за формулою (1). Середнє значення цих величин позначимо великими буквами, відповідно – X_c, Y_c, Z_c. Динаміку чисельності взаємодіючих популяцій захисника $x(t)$ та хижака $y(t)$ будемо моделювати системою рівнянь

$$\begin{cases} \dot{x}(t) = r_x\left[1 + a\left(1 - \dfrac{y(t)}{Y_c}\right) - \dfrac{x(t-h_x)}{X_c}\right]x(t) \\ \dot{y}(t) = r_y\left[\dfrac{x(t)}{X_c} - \dfrac{y(t-h_y)}{Y_c}\right]y(t) \end{cases}, \tag{5}$$

де r_x та r_y – мальтузіанські коефіцієнти росту;

h_x та h_y – середній час затримки, відповідно, аналізу (планування) атаки хакером й впровадження засобів протидії та пошуку вразливості захисником;

X_c та Y_c – середні кількості операцій для атак та з ліквідації атак, відповідно;

a – коефіцієнт тиску захисників на хакерів, який визначає ефективне зменшення середньої кількості дій хакерів за умови збільшення активності захисників (хижаків);

Коефіцієнт тиску захисників на хакерів – a визначає ефективне зменшення кількості операцій хакерів по плануванню, підготовці та здійснення атак. Його можна визначити неявним чином

$$X_c(a) = \frac{X_c(0)}{1+a}. \tag{6}$$

На практиці кількість уразливостей мережі поступово зменшується внаслідок діяльності служби безпеки та вдосконалення теорії безпеки. Але часта зміна технологій і потік нових версій підвищують стрибкоподібно число вразливостей. Кількість уразливостей доводиться вважати поновлюваним ресурсом.

Проведемо аналіз цієї моделі при початкових умовах на інтервалі часу $\{h_x \ldots 0\}$ від: $x(0) = 1$, $y(0) = 1$, які були характерні на початку масового використовування комп'ютерів в Україні.

Аналіз моделі динаміки кількості інцидентів інформаційної безпеки

Фізичний смисл моделі, яка представлена системою рівнянь (5), можна зрозуміти порівнявши її з іншими моделями. Так, якщо виключити члени, які описують взаємні зв'язки, система рівнянь розпадається. При цьому, якщо нема захисників ($a = 0$), то перше рівняння перетворюється на рівняння Хатчинсона (4). Якщо, крім того,

виключити запізнення ($h_x = 0$), то маємо логістичне рівняння. А якщо, крім того, далі зняти самообмеження на ріст кількості атак ($X_c \to \infty$), то перше рівняння стає рівнянням мальтузіанського росту. Якщо нема хакерів ($x(t) = 0$), що важко собі уявити, та виключити фактор запізнювання, то із другого рівняння (5) випливає, що захисники поступово «вимирають». Якщо у моделі, тобто системі рівнянь (5), виключити запізнення з обох рівнянь ($h_x = 0; h_y = 0$), то модель стає канонічною, яка ретельно проаналізована аналітично та чисельно, див. [11; глава 8, пример 1] та [7; глава 2, § 3]. Блок-схема Simulink для моделі Лоткі-Волтерра наведена у [7; приложение А.4]. Щодо моделі із запізненням (5), то вона досліджена значно менше. У [17; глава 4 и упражнение 4.9] розроблена методика розрішення диференційних рівнянь із запізненням та надано приклад розрахунку для простої моделі «хижак-жертва», що схожа на модель (5).

Для спрощення моделі (5) при чисельному розрахунку зменшують кількість параметрів за допомогою заміни. Слідуючи [17; формули (3), (4)], робимо заміни: $t = h_x\tau$, $x(h_x\tau) = X_c N_1(\tau)$, $y(h_y\tau) = Y_c N_2(\tau)$ і далі, позначивши $\lambda_1 = r_x h_x$, $\lambda_2 = r_y h_y$, $h = h_y / h_x$, та перепозначивши τ через t , отримуємо

$$\begin{cases} \dot{N}_1(t) = \dfrac{\lambda_1}{1+a}\left[1 + a\left(1 - N_2(t)\right) - N_1(t-1)\right]N_1(t), \\ \dot{N}_2(t) = \lambda_2\left[N_1(t) - N_2(t-h)\right]N_2(t). \end{cases} \qquad (7)$$

З практичних міркувань для моделювання нами була створена програма проведення розрахунків за формулою (5).

Результати одного з прогонів моделі при $r_x = 1.28$, $r_y = 0.99$, $a = 0.9$, $h_x = 1$, $h_y = 0.4$, $X_c = 35$, $Y_c = 25$, показані на рис. 1.

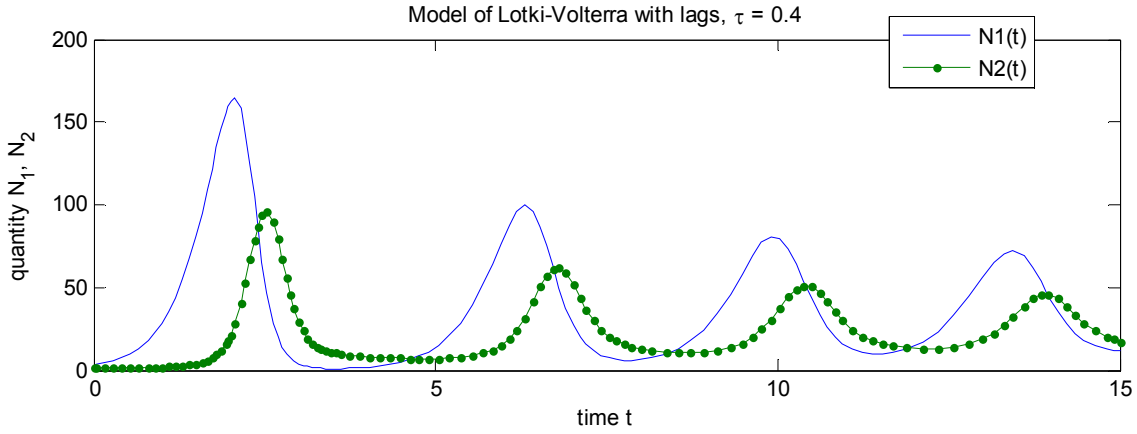


Рис. 1. Розрахунки моделі Лоткі-Волтерра в середовищі MATLAB

До недоліків розглянутої моделі динаміки кількості інцидентів інформаційної безпеки можна віднести її якісний характер. «Число функціонально значимих «резонансів» у реальних сигналах (системах) ... може досягати декількох сотень. При цьому, внаслідок взаємозв'язків у системі та впливів сторонніх факторів різного виду, у тому числі, випадкових, продуцьовані системою сигнали нестаціонарні, див. [10; вступ, с. 27]». Це стосується й великих систем інформаційної безпеки. Продовжуємо цитату: «Всі ці фактори «маскують» чисто хаотичні компоненти

сигналів. ... Таке різноманіття динамічних факторів неможливо врахувати у рамках модельного розгляду».

Висновки

Запропонована у даній статті модель «зловмисник-захисник» на основі моделі Лоткі-Волтерра підтвердила гіпотезу щодо коливального характеру динаміки інцидентів інформаційної безпеки та дозволяє чітко визначити напрямки подальших досліджень щодо розробки методів та побудови систем захисту інформації, а також створити концептуальні моделі попередження атак та формалізувати, на основі методів нелінійної динаміки, можливості превентивних систем для підвищення ефективності їх вибору й формулюванню вимог при їх проектуванні та розробки. Розроблена модель взаємовпливу порушника і захисника в системах захисту інформації дозволяє визначити сукупність заходів різного характеру для організації комплексної системи інформаційної безпеки в інформаційно-комунікаційних системах. Вибір адекватної моделі та розрахунок її кількісних характеристик на основі експериментальної статистики й розробка прогнозу є метою подальшої роботи.

Список літератури

1. Управление риском / [Электронный ресурс] под ред. Г.Г. Малинецкого. – М.: РАН, 2000. – 249 с. – Режим доступа: http://risk.keldysh.ru/risk/risk.htm.
2. Гайворонський, М. В. Безпека інформаційно-комунікаційних систем / М.В. Гайворонський, О.М. Новіков. – К.: Видавнича група ВНУ, 2009. – 608 с.
3. Богуш, В.М. Теоретичні основи захищених інформаційних технологій: навч. посіб. / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.
4. Юдін, О.К. Захист інформації в мережах передачі даних / Юдін О.К., Корченко О.Г., Конахович Г.Ф. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.
5. Гленсдорф, П. Термодинамическая теория структуры, устойчивости и флуктуаций: Пер с англ. / Гленсдорф П Пригожин И. Изд. 2-е. – М.: Едиториал УРСС, 2003. – 280 с. (Синергетика: от прошлого к будущему).
6. Малинецкий, Г.Г. Нелинейная динамика и хаос. Основные понятия: Учебное пособие. / Г.Г. Малинецкий. - М.: КомКнига, 2006. – 240 с. (Синергетика: от прошлого к будущему).
7. Тарасевич, Ю.Ю. Математическое и компьютерное моделирование. Вводный курс: Учебное пособие. / Ю.Ю. Тарасевич. – М.: Эдиториал УРСС. 2004. 2004. – 152 с.
8. Милованов, В.П. Неравновесные социально-экономические системы: синергетика и самоорганизация. / В.П. Милованов. – М.: Эдиториал УРСС, 2001. – 264 с.
9. Колесников, А.А. Синергетические методы управления сложными системами: Теория системного синтеза. / А.А. Колесников. – М.: КомКнига, 2006. – 240 с.
10. Тимашев, С.Ф. Фликер-шумовая спектрскопия: информация в хаотических сигналах. / С.Ф. Тимашев. – М.: ФИЗМАТЛИТ, 2007. – 248 с.
11. Малинецкий, Г.Г. Математические основы синергетики. Хаос, структура, вычислительный експеримент. / Г.Г. Малинецкий. – М.: КомКнига, 2005. – 312 с. (Синергетика : от прошлого к будущему).
12. Шураков, В.В. Надежность программного обеспечения систем обработки данных: Учебник. / В.В. Шураков. – М.: Финансы и статистика, 1987. – 272 с.
13. Петренко, С.А. Вычисления с памятью критически важных информационных систем в условиях кибератак / С.А. Петренко, А.Г. Ломако, О.Н. Омелченкова, А.В. Зотова // Защита информации. INSIDE, – № 6, 2012. – с. 58-69.
14. Казарин, О.В. Методология обеспечения проактивной безопасности комп'ютерных систем / О.В. Казарин, В.Ю. Скиба // Защита информации. INSIDE, – № 2, 2013. – с. 52-60.
15. Эшби, У.Р. Введение в кибернетику / У. Р. Эшби; [Пер. с англ. Д.Г. Ламути. Под ред. В.А. Успенського]. – М.: Изд-во „Иностр. лит.", 1959. – 432 с.
16. Отчет «Лаборатории Касперского»: Java под ударом – эволюция эксплойтов в 2012-2013 гг. – 26 с. – Режим доступа: http://www.securelist.com/ru/analysis/208050816/Otchet_Laboratorii_Kasperskogo_Java_pod_udarom_evolyutsiya_eksploytov_v_2012_2013_gg.

17. Шампайн, Л.Ф. Решение обыкновенных дифференциальных уравнений с использованием МАТЛАБ: Учебное пособие / Л.Ф. Шампайн, И. Гладвел, С. Томпсон. Пер. с англ. – СПб.: Издательство «Лань», 2009. – 304 с. (Учебники для вузов. Специальная литература).
18. Кащенко, С.А. Релаксационные колебания в системе с запаздываниями, моделирующей задачу «хищник-жертва» / С.А. Кащенко // Моделирование и анализ информационных систем. Т.20, № 1 (2013). 52 – 98 с.

ДИНАМИКА КОЛИЧЕСТВА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.В. Кононович

Одесская национальная академия пищевых технологий
ул. Канатная, 112, г. Одесса, 650039, Украина; e-mail: kononovich@mail.ru

В статье рассматривается динамика инцидентов информационной безопасности инфокоммуникационных сетей, предложена гипотеза относительно ее колебательного характера и разработана модель «злоумышленник-защитник» на основе модели Лотки – Волтерра. Полученные результаты позволяют повысить эффективность работы систем информационной безопасности и формализовать направления дальнейших исследований по разработке новых эффективных систем информационной безопасности инфокоммуникаций с использованием методов нелинейной динамики.
Ключевые слова: информационная безопасность, инциденты, нелинейная динамика, компьютерное моделирование, информационно-коммуникационные сети

DYNAMICS OF THE NUMBER OF INFORMATION SECURITY INCIDENTS

Irina V. Kononovich

Odessa National Academy of Food Technologies
112, Kanatnaja str., Odessa, 650039, Ukraine; e-mail: kononovich@mail.ru

The dynamics of incidents of informative security of communication networks is examined in the article, a hypothesis is offered in relation to its oscillatory nature was proposed. The simulator «hacker-defender» on the basis of the model is Lotki –Volterra was developed. The obtained results allow to improve the efficiency of information security systems and formalize directions for further research to develop new effective information security systems of communication using the methods of nonlinear dynamics.
Keywords: information security, incidents, nonlinear dynamics, computer simulation, infocommunication networks

УДК 004.056.5: 518: 512.624.3

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 44-49

SINGULAR VALUES DECOMPOSITION AS A TOOL ENHANCING THE EFFICIENCY OF STEGANOGRAPHIC ALGORITHM

M.A. Melnyk

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: ritochek@yandex.ua

A technique for singular value decomposition of blocks of a cover matrix was improved to enhance the efficiency of decoding the additional information by a "robust to compression attacks" steganographic algorithm which has been developed earlier by the author. The proposed algorithm design ensures reliability of perception of the image. The results of computational experiment are presented to confirm the decrease in sensitivity of the formed stego message to computational error.

Keywords: steganographic algorithm, singular values decomposition, computational error, robustness against lossy compression, matrix

Introduction

In her earlier work [1], the author has proposed $A2$, a "robust against lossy compression, in particular, with significant coefficients" steganographic algorithm based on perturbations of singular vectors (SNVC) corresponding to maximum singular values (SNVL) of blocks of a cover matrix obtained by standard decomposition [2]. It was established that the main disturbing impact for the stego message (SM) obtained with the help of $A2$ and affecting the decoding of auxiliary information (AI; otherwise called secret message) is caused not by compression but by rounding operations involved in generation of the SM. Let us assume that B is an 8×8 block (submatrix) of a cover matrix, $\overline{B}$ is a result of embedding AI in B, $\overline{\overline{B}}$ is a SM block that corresponds to B. In the general case $\overline{\overline{B}} \neq \overline{B}$. This is due to the rounding of values of $\overline{B}$ elements to integers within 0 to 255 range during generation of the SM. It is the computational error that is mostly responsible for errors when decoding AI with the $A2$ algorithm [1].

In her earlier work [3], the author has proposed a technique to reduce the influence of rounding errors on the robustness of the $A2$ algorithm. Let us assume that $\sigma_1 \geq ... \geq \sigma_8 \geq 0$ are singular values (SVs) of an arbitrary B block. The technique involves what is called a singular value decomposition (SVD). Given the fact that post-stego-transformation rounding-off operations disturb mostly the SNVCs corresponding to the smallest SNVLs [4] due to low separateness of these SNVLs (here, by separateness $svdgap(i,B)$ of SNVL σ_i of B matrix we understand $svdgap(i,B) = \min\limits_{i\neq j}\left|\sigma_j(B) - \sigma_i(B)\right|$ [5]), the reduction in the sensitivity of such SNVCs (and, therefore, that of a stego message in total) was obtained through artificial increase in the separateness of $\sigma_6, \sigma_7, \sigma_8$ by changing them to

$$\sigma_5 - h, \sigma_5 - 2h, \sigma_5 - 3h, \qquad (1)$$

where $h = (\sigma_5 - \sigma_8)/3$ did not affect the reliability of image perception. However, the results of testing the modified $A2$ algorithm [3] have shown that the value of influence of rounding-off operations on the efficiency of decoding AI in this algorithm requires further reduction.

Purpose of the Work and Problem Setting-up

The *purpose* of the work is improve the efficacy of decoding AI with $A2$, an earlier developed "robust against lossy compression" steganographic algorithm, by reducing the sensitivity of stego message generated by this algorithm to computational errors.

To accomplish the purpose, the following *problems* are to be solved:

1. To determine the causes of remaining (as per [3]) sensitivity of stego message to rounding-off errors, and find the way to further reduction of this sensitivity,
2. To refine the SVD technique, given the requirement to ensure the appropriate reliability of perception of the resultant image.

Body of the Work

In general, the SVD technique proposed in [3] showed some improvement as it ensured the increase in efficiency of decoding AI with the $A2$ algorithm. However, the meticulous investigation of SVD operation related to a separate block has established that reduction of the sensitivity to computational errors occurs not in all the cases. Indeed, if the pattern presented in Fig. 1(a) is observed in the block, than, with the SVD operation performed as per formula (1), the separateness of non-minimal SNVL is reduced (refer to Fig.1b, SNVL σ_6), thus impairing the sensitivity of the block. Therefore, the SVD technique proposed in [3] requires improvement, with the proposed procedure given below.

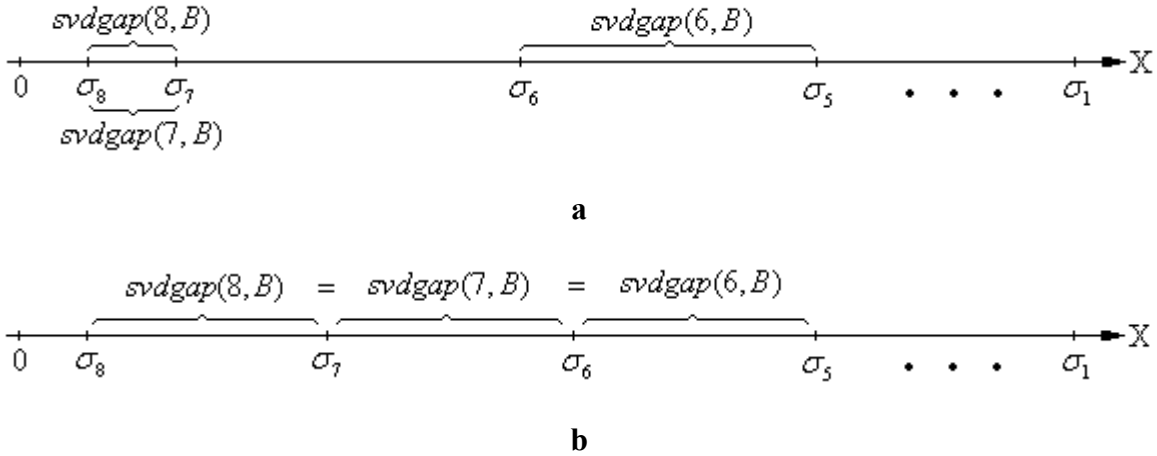


Fig. 1. Possible results of SVD operation: a – SNVL of the block of original digital image; b – SNVL of this block after performance of the SVD operation

In the original digital image, generally, SNVLs of practically all the blocks are non-zero (i.e, positive), and of the smallest separateness are σ_7, σ_8 (Table 1). Given this, to avoid the situation presented in Fig.1, we propose to perform the SVD operation in one of the two following ways.

1. For convenience, we shall denote post-SVD SNVLs of the block by $\overline{\sigma}_i, \overline{svdgap}(i,B),\ i = \overline{1,8}$. In an arbitrary case, the increase in the separateness of all SNVLs

will be ensured only by increasing the distance between each two SNVLs with consecutive indices. This may be made as per the following formula:

$$\overline{\sigma}_i = \sigma_i + (8-i)h, \;\; i = \overline{1,8}. \qquad (2)$$

Table 1.

Mean values of separatenesses belonging to blocks singular values, received as a result of computing experiment with 200 DI

Mean value $svdgap(i,B)$							
$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$
712.4564	23.1111	7.9843	3.0004	1.4232	0.7125	0.4667	0.5781

Relationship (2) makes it possible to increase the distance between each two SNVLs σ_i, σ_{i+1} by h, while h must be selected given the requirement for reliability of the perception of post-SVD image. The significant increase in efficiency of decoding with $A2$ stego algorithm occurs when h is comparable with 10; however, in this case, the amount of increase in SNVL value will result in the increase in energy of the image, and, consequently, may result in lightening (Fig. 2c) and even the development of evident artifacts (Fig. 2d).

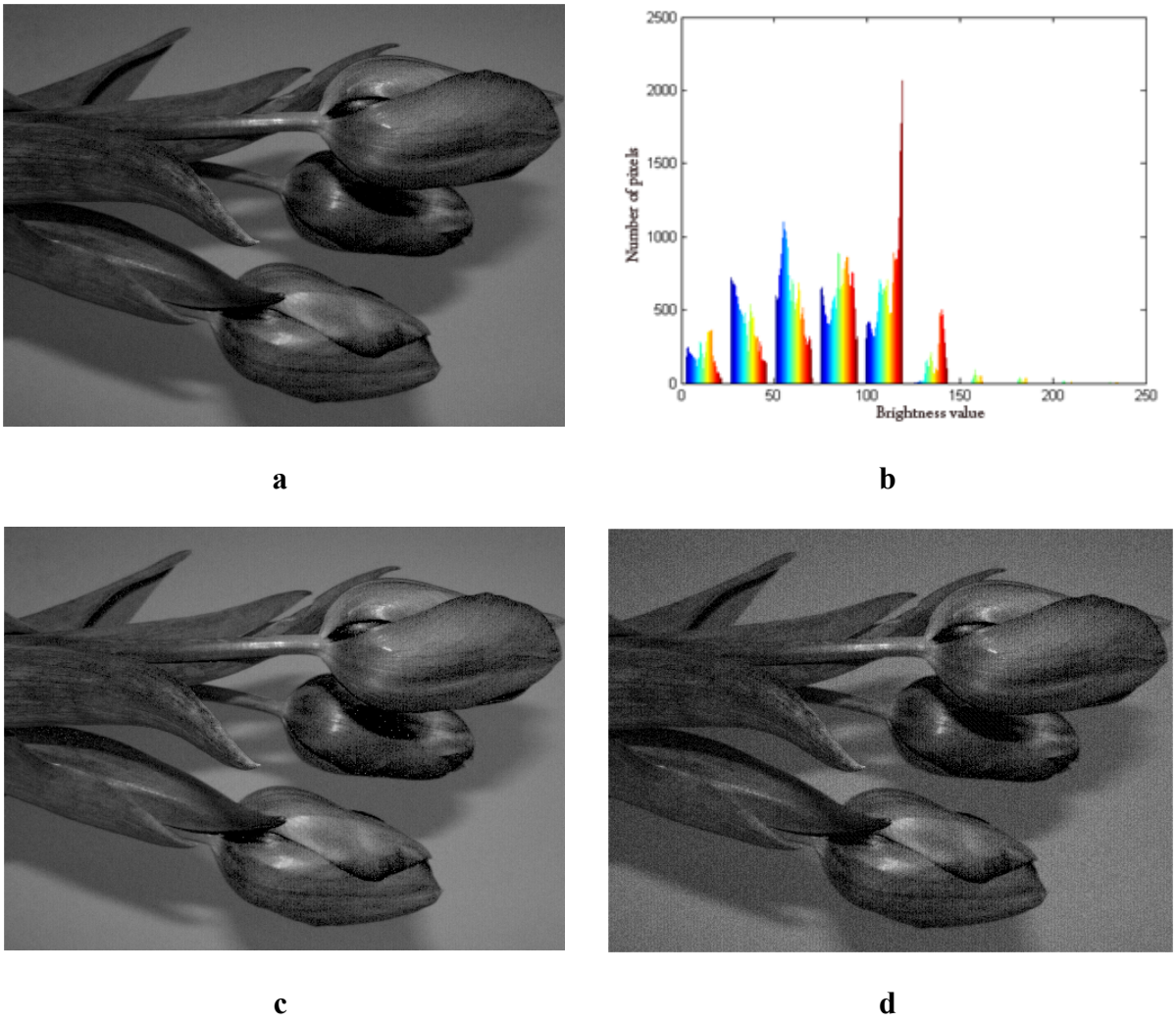


Fig. 2. SVD result showing steadily increase in separateness of every SNVL. a – initial image; b – histogram of DI pixels brightness values; c, d – SVD results

As the computational experiment shows, such situation often occurs in shaded digital images with the pixel brightness histograms similar to that shown in Fig. 2b. Therefore, in practice, we propose to use $h \approx 2$.

2. Considering possible violation of reliability of perception of the DI at SVD when using method 1, in order to enhance efficiency of $A2$ it is proposed to provide SVD via nullification of σ_8, without changing the position of other SNVL (Figure 3a and Figure 3b respectively). This will ensure the increase of $svdgap(8, B)$ without attenuation in separatenesses of all other SNVL, although $svdgap(7, B)$ may not experience changes (Figure 3c and Figure 3d respectively). Method 2 guarantees reliability of perception of the image, although it is much less optimal from the point of $A2$ efficiency enhancing (Table 2).

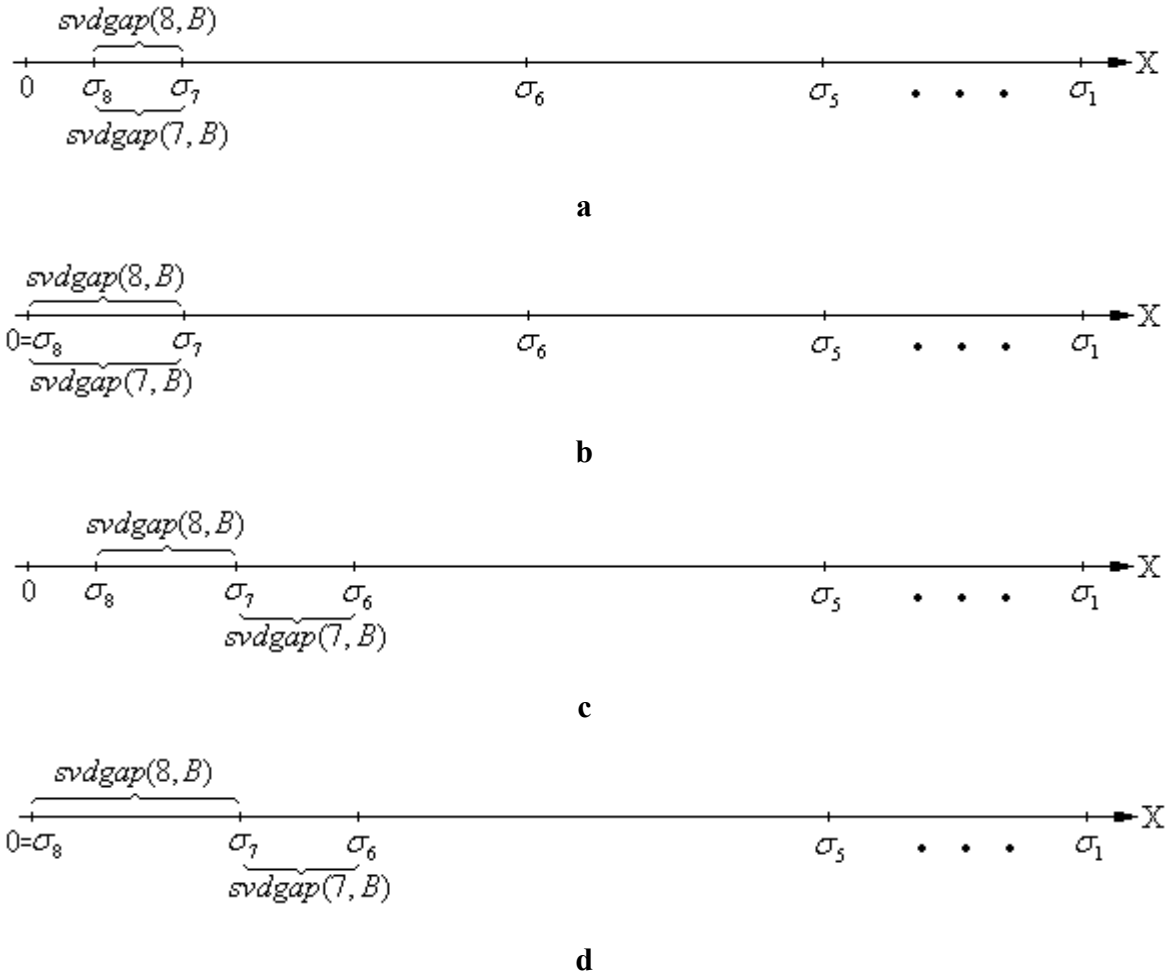


Fig. 3. Result of carrying out SVD using method 1: a, c – SV state in the initial block B; b, d – SNVL state after SVD when using method 1

Results of the computing experiment, involving 300 digital images, shown in Table 2, testify the decoding efficiency increase at the cost of SVD in $A2$, that was evaluated regularly according to correlation coefficient (NC), defined in accordance with [6]: $NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p}_i'}{t}$, where $p_1, p_2, ..., p_t$, и $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $p_i, \overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$, — correspondingly, secret message inserted in the container and decoded from steganography message, $p_i' = 1, \overline{p}_i' = 1$, if $p_i = 1, \overline{p}_i = 1$, and $p_i' = -1, \overline{p}_i' = -1$, if $p_i = 0, \overline{p}_i = 0$. Therefore, the value $p_i' \times \overline{p}_i' \in \{1, -1\}$ is received.

Table 2.

Results of AI decoding using the $A2$ steganography algorithm

SM format		TIF	JPEG			
			$QF = 80$	$QF = 30$	$QF = 20$	$QF = 10$
Mean value NC	Without SVD	0.9603	0.9577	0.9498	0.9454	0.9359
	SVD with method 1 $h = 10$	0.9801	0.9767	0.9634	0.9484	0.9409
	SVD with method 1 $h = 2$	0.9706	0.9617	0.9569	0.9465	0.9386
	SVD with method 2	0.9621	0.9587	0.9507	0.9453	0.9375

Conclusions

In the present paper, a technique for singular value decomposition of blocks of a cover matrix was improved considering requirements for reliability of perception of the image received as a result. The efficiency of decoding the auxiliary information was improved by a "robust to compression attacks" steganographic algorithm $A2$ due to decrease in sensitivity of the formed stego message to computational error.

References

1. Мельник, М.А. Sign-нечувствительность сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / М.А.Мельник // Інформатика та математичні методи в моделюванні. – 2013. – Т.3, №2. – С.116-126.
2. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М.: Техносфера, 2006. — 1070 с.
3. Кобозева, А.А. Стеганографический алгоритм, основанный на sign-нечувствительности сингулярных векторов матрицы изображения / А.А.Кобозева, М.А. Мельник // Системи обробки інформації. – 2013. – Вип. 3(110), том 2. – С.90-94.
4. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А.Кобозева, М.А.Мельник // Збірник наукових праць Військового інституту Київського нац-го ун-ту ім.Т.Шевченка. – 2012. Вип.38. – С.193-203.
5. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
6. Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin et al. // Expert Systems with Applications. — 2009. — Vol. 36, Iss. 9. — PP. 11509–11516.

РОЗПОДІЛ СИНГУЛЯРНИХ ЧИСЕЛ ЯК ІНСТРУМЕНТ, ЩО ПІДВИЩУЄ ЕФЕКТИВНІСТЬ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ

М.О. Мельник

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: ritochek@yandex.ua

У роботі шляхом удосконалення способу розподілу сингулярних чисел блоків матриці цифрового зображення-контейнера підвищена ефективність декодування додаткової інформації розробленого автором раніше стійкого до атаки стиском стеганографічного алгоритму. Запропонована розробка забезпечує дотримання надійності сприйняття зображення. Наведені результати обчислювального експерименту, що підтверджують зменшення чутливості зформованого стеганоповідомлення до обчислювальної похибки.

Ключові слова: стеганографічний алгоритм, розподіл сингулярних чисел, обчислювальна похибка, стійкість до атаки стиском, матриця.

РАЗДЕЛЕНИЕ СИНГУЛЯРНЫХ ЧИСЕЛ КАК ИНСТРУМЕНТ, ПОВЫШАЮЩИЙ ЭФФЕКТИВНОСТЬ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА

М.А. Мельник

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: ritochek@yandex.ua

В работе путем усовершенствования способа разделения сингулярных чисел блоков матрицы цифрового изображения-контейнера повышена эффективность декодирования дополнительной информации разработанного автором ранее устойчивого к атаке сжатием стеганографического алгоритма. Предложенная разработка обеспечивает соблюдение надежности восприятия изображения. Приведены результаты вычислительного эксперимента, подтверждающие уменьшение чувствительности формируемого стеганосообщения к вычислительной погрешности.

Ключевые слова: стеганографический алгоритм, разделение сингулярных чисел, вычислительная погрешность, устойчивость к атаке сжатием, матрица.

УДК 004.415

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 50-56

МОДЕЛИРОВАНИЕ ВЛИЯНИЯ МЕСТОПОЛОЖЕНИЯ ВХОДНОГО ПЕРЕНОСА НА СЛОЖНОСТЬ СХЕМЫ СУММАТОРА

О.Н. Паулин

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: paolenic@yandex.ua

Работа посвящена определению зависимости сложности логической схемы сумматора от местоположения входного переноса. Из проведенного исследования вытекает возможность дополнительной оптимизации сумматора, а также умножителя, построенного на сумматорах.

Ключевые слова: моделирование, фрагмент, местоположение переноса, сумматор, аппаратные затраты

Введение

Для параллельной обработки больших потоков данных используются методы, которые показали свою эффективность в смысле минимальной задержки на такую обработку. При этом потоки данных могут быть интерпретированы как многорядные арифметические двоичные коды (МРК), а обработка – как свёртка МРК, причём под свёрткой понимается обобщение бинарной операции сложения на случай множества рядов кодов [1]. Множество бит, составляющих МРК, в работе называется областью бит (ОБ).

Для свёртки МРК при большом числе рядов кодов используется разбиение (декомпозиция) множества рядов кодов на слои (их фрагменты) и свёртка полученных слоёв (их фрагментов), а далее – свёртка рядов полученных результатов. ОБ может быть разбита на фрагменты [2], регулярные (например, прямоугольники, ромбы и др.) и нерегулярные; здесь же приведены теоремы о количестве переносов из данного фрагмента.

Необходимость разбиения ОБ определяется быстрым нарастанием сложности компрессора при использовании многооперандных структур: она пропорциональна квадрату числа разрядов и экспоненциальной функции от числа сжимаемых рядов [3]. Разбиение должно быть проведено таким образом, чтобы процедура свёртки и компрессор для её реализации соответствовали критерию минимальной задержки.

В то же время при разных разбиениях возможна вариация ширины (разрядности) фрагмента и, следовательно, местоположения переноса из фрагмента. При этом сложность логической схемы сумматора существенно зависит от местоположения входного для него переноса, возникающего при сворачивании кодов фрагмента на предыдущем этапе процедуры свёртки.

Целью моделирования является определение влияния местоположения переноса из фрагмента бит предыдущего этапа процедуры свёртки при вариации его разрядности на сложность сумматора, обрабатывающего фрагмент данного этапа процедуры.

Исследование и его результаты

В работе выдвинута гипотеза о зависимости сложности сумматора от местоположения переноса в обрабатываемый сумматором фрагмент битов. Для её подтверждения проводятся эксперименты, которые заключаются в следующем. Рассматриваются бинарные сумматоры различной разрядности с описанием базового формата в виде [2..22], что означает двухрядный двоичный код заданной разрядности. Далее рассматриваются вариации местоположения h бита переноса (его номера), входного относительно базового формата описания исходного сумматора. Для базового формата и для форматов с вариацией h строятся таблицы функционирования сумматора, по которым вычисляются его аппаратные затраты $V = f(h)$. Отметим, что при изменении h быстродействие сумматора не изменяется.

Функционирование сумматора описывается с помощью таблиц (таблиц функционирования – ТФ) сумм и внешних относительно заданного формата переносов, заполняемых индексами симметрических функций. При этом функции суммы и переноса вычисляются без явного вычисления внутренних переносов по разработанной программе «Расчёт таблиц разрядных индексов» [4]. Для определения количества внешних переносов предварительно определяем максимально возможное значение суммы $Q_{\max}$ всех бит фрагмента при условии, что все они принимают значение 1. Имеем

$$Q_{\max} = \sum_{i=1}^{n} 2^{i-1} a_i \,, \tag{1}$$

где i — номер разряда,

n — количество разрядов сумматора,

a_i — количество бит в i-м разряде.

Расчёт сложности по Квайну синтезируемой схемы сумматора (его каскада) осуществляется отдельным программным модулем «Вычисление сложности» по минимизированным поразрядным ТФ в соответствии с алгоритмом:

1. Для каждой поразрядной таблицы суммируются значения сложности всех её n строк.
2. Сложность i-ой строки определяется следующим образом:
   - для каждого j-го столбца определяется количество m_{ij} вариантов РИ как число индексов в данной клетке (например, если в клетке записано 2-4, то ей соответствует 3 варианта). Если в клетке стоит символ X, то столбец с этим символом игнорируется;
   - если в строке имеется t_i символов X, то количество учитываемых столбцов равно $k_i = k - t_i$, где k — количество столбцов данной ТФ;
   - числа вариантов по i-ой строке перемножаются, а полученный результат домножается на число учитываемых столбцов.

   Для l-ой ТФ её сложность равна:

$$Q_l = \sum_{i=1}^{n} k_i \prod_{j=1}^{k} m_{ji} \,. \tag{2}$$

3. Суммируются значения сложности всех поразрядных таблиц РИ.

Отметим, что сложность симметрических функций не учитывается, поскольку она не зависит от h.

Рассмотрим вначале влияние местоположения переноса относительно базового сумматора вида $[2\,2\,2]$ (три разряда, два ряда кодов), на сложность его схемотехнической реализации. Проведём расчёт таблиц разрядных индексов (ТРИ) для сумматоров $[2\,2\,2]$ (базовое значение), а также $[2\,2\,3]$, $[2\,3\,2]$, $[3\,2\,2]$, в которых h последовательно принимает значения 1, 2, 3, и вычислим аппаратные затраты на сумматоры. Результаты расчётов ТРИ сведены в табл. 1 – 4. Рассчитанные значения сложности рассмотренных сумматоров представлены в табл. 5.

Таблица 1.

Сумматор вида $[2\,2\,2]$, $Q_{\max} = 14$

P_1			S_3			S_2		S_1
3p	2p	1p	3p	2p	1p	2p	1p	1p
1	1	2	0.2	1	2	0.2	2	1
1	2	X	0.2	2	X	1	0.1	
2	X	X	1	0	X			
			1	1	0.1			

Таблица 2.

Сумматор вида $[2\,2\,3]$, $Q_{\max} = 15$

P_1			S_3			S_2		S_1
3p	2p	1p	3p	2p	1p	2p	1p	1p
1	1	2.3	0.2	1	2.3	0.2	2.3	1.3
1	2	X	0.2	2	X	1	0.1	
2	X	X	1	0	X			
			1	1	0.1			

Таблица 3.

Сумматор вида $[2\,3\,2]$, $Q_{\max} = 16$

P_2			P_1			S_3			S_2		S_1
3p	2p	1p	3p	2p	1p	3p	2p	1p	2p	1p	1p
2	3	2	0	3	2	0.2	1	2	1.3	0.1	1
			1	1	2	0.2	2	X	0.2	2	
			1	2.3	X	0.2	3	0.1			
			2	0.2	X	1	0	X			
			2	3	0.1	1	1	0.1			
						1	3	2			

Таблица 4.

Сумматор вида $[3\,2\,2]$, $Q_{\max} = 18$

P_2			P_1			S_3			S_2		S_1
3p	2p	1p	3p	2p	1p	3p	2p	1p	3p	2p	1p
3	1	2	1	1	2	0.2	1	2	0.2	2	1
3	2	X	1	2	X	0.2	2	X	1	0.1	
			2.3	X	X	1.3	0	X			
						1.3	1	0.1			

Таблица 5.

Аппаратные затраты для 3-разрядного сумматора

Вид сумматора	Выходные функции					Суммарные затраты
	P_2	P_1	S_3	S_2	S_1	
$[2\,2\,2]$	–	5	18	8	1	33
$[2\,2\,3]$	–	9	20	12	2	43
$[2\,3\,2]$	3	22	36	12	1	74
$[3\,2\,2]$	2	7	26	8	1	44

Рассмотрим далее базовый сумматор вида $[2\,2\,2\,2]$, а также сумматоры с учётом входного переноса ($h=1,2,3,4$): $[2\,2\,2\,3]$, $[2\,2\,3\,2]$, $[2\,3\,2\,2]$, $[3\,2\,2\,2]$. Результаты расчётов ТРИ для данных сумматоров представлены в таблицах 6 – 10. Рассчитанные аппаратные затраты для рассмотренных сумматоров занесены в табл. 11.

Таблица 6.

Сумматор вида $[2\,2\,2\,2]$, $Q_{\max}=30$

P_1				S_4				S_3			S_2		S_1
4р	3р	2р	1р	4р	3р	2р	1р	3р	2р	1р	2р	1р	1р
1	1	1	2	0.2	1	1	2	0.2	1	2	0.2	2	1
1	1	2	X	0.2	1	2	X	0.2	2	X	1	0.1	
1	2	X	X	0.2	2	X	X	1	0	X			
2	X	X	X	1	0	X	X	1	1	0.1			
				1	1	0	X						
				1	1	1	0.1						

Таблица 7.

Сумматор вида $[2\,2\,2\,3]$, $Q_{\max}=31$

P_1				S_4				S_3			S_2		S_1
4р	3р	2р	1р	4р	3р	2р	1р	3р	2р	1р	2р	1р	1р
1	1	1	2.3	0.2	1	1	2.3	0.2	1	2.3	0.2	2.3	1.3
1	1	2	X	0.2	1	2	X	0.2	2	X	1	0.1	
1	2	X	X	0.2	2	X	X	1	0	X			
2	2	2	X	1	0	X	X	1	1	0.1			
2	2	X	X	1	1	0	X						
2	X	X	X	1	1	1	0.1						

Таблица 8.

Сумматор вида $[2\ 2\ 3\ 2]$, $Q_{\max} = 32$

P_2				P_1				S_4				S_3			S_2		S_1
4p	3p	2p	1p	4p	3p	2p	1p	4p	3p	2p	1p	3p	2p	1p	2p	1p	1p
2	2	3	2	0	2	3	2	0.2	0	3	2	0.2	1	2	0.2	2	1
				1	0	3	2	0.2	1	2.3	X	0.2	2	X	1.3	0.1	
				1	1	1	2	0.2	2	0.2	X	0.2	3	0.1			
				1	1	2.3	X	0.2	2	3	0.1	1	0	X			
				1	2	X	X	1	0	0.2	X	1	1	0.1			
				2	0.1	X	X	1	0	3	0.1						
				2	2	0.2	X	1	1	0	X						
				2	2	3	0.1	1	1	1	0.1						
								1	2	3	2						

Таблица 9.

Сумматор вида $[2\ 3\ 2\ 2]$, $Q_{\max} = 34$

P_2				P_1				S_4				S_3			S_2		S_1
4p	3p	2p	1p	4p	3p	2p	1p	4p	3p	2p	1p	3p	2p	1p	2p	1p	1p
2	3	2	X	0	3	1	2	0.2	1	1	2	0.2	1	2	0.2	2	1
				0	3	2	X	0.2	1	2	X	0.2	2	X	1	0.1	
				1	1	1	2	0.2	2	X	X	1.3	0	X			
				1	1	2	X	0.2	3	0	X	1.3	1	0.1			
				1	2.3	X	X	0.2	3	1	0.1						
				2	0.2	X	X	1	0	X	X						
				2	3	0	X	1	1	0	X						
				2	3	1	0.1	1	1	1	0.1						

Таблица 10.

Сумматор вида $[3\ 2\ 2\ 2]$, $Q_{\max} = 38$

P_2				P_1				S_4				S_3			S_2		S_1
4p	3p	2p	1p	4p	3p	2p	1p	4p	3p	2p	1p	3p	2p	1p	2p	1p	1p
3	1	1	2	1	1	1	2	0.2	1	1	2	0.2	1	2	0.2	2	1
3	1	2	X	1	1	2	X	0.2	1	2	X	0.2	2	X	1	0.1	
3	2	X	X	1	2	X	X	0.2	2	X	X	1	0	X			
				2	X	X	X	1.3	0	X	X	1	1	0.1			
				3	0	X	X	1.3	1	0	X						
				3	1	0	X	1.3	1	1	0.1						
				3	1	1	0.1										

Таблица 11.

Аппаратные затраты для 4-разрядного сумматора

Вид сумматора	Выходные функции						Суммарные затраты
	P_2	P_1	S_4	S_3	S_2	S_1	
[2 2 2 2]	–	10	31	18	8	1	68
[2 2 2 3]	–	19	39	20	12	2	92
[2 2 3 2]	4	41	86	30	12	1	174
[2 3 2 2]	3	35	53	26	8	1	126
[3 2 2 2]	9	23	44	18	8	1	103

Аналогично проведены расчёты таблиц РИ и для исходных сумматоров вида [2 2 2 2 2] и [2 2 2 2 2 2]. Рассчитанные для них аппаратные затраты приведены в табл. 12 и 13.

Таблица 12.

Аппаратные затраты для 5-разрядного сумматора

Вид сумматора	Выходные функции							Суммарные затраты
	P_2	P_1	S_5	S_4	S_3	S_2	S_1	
[2 2 2 2 2]	–	15	47	31	18	8	1	120
[2 2 2 2 3]	–	20	57	39	20	12	2	150
[2 2 2 3 2]	5	65	134	110	30	12	1	357
[2 2 3 2 2]	9	48	124	53	26	8	1	269
[2 3 2 2 2]	12	41	81	44	18	8	1	205
[3 2 2 2 2]	2	34	66	31	18	8	1	160

Таблица 13.

Аппаратные затраты для 6-разрядного сумматора

Вид сумматора	Выходные функции								Суммарные Затраты
	P_2	P_1	S_6	S_5	S_4	S_3	S_2	S_1	
[2 2 2 2 2 2]	–	21	66	47	31	18	8	1	192
[2 2 2 2 2 3]	–	27	78	57	39	24	12	2	239
[2 2 2 2 3 2]	6	59	260	154	88	33	12	1	613
[2 2 2 3 2 2]	11	52	163	124	53	26	8	1	438
[2 2 3 2 2 2]	15	47	121	81	44	18	8	1	335
[2 3 2 2 2 2]	18	43	103	66	31	18	8	1	288
[3 2 2 2 2 2]	20	41	92	47	31	18	8	1	258

Выводы

Проведено 22 эксперимента по определению сложности сумматоров с различными параметрами. Результаты экспериментов сведены в таблицы 5, 11-13. Анализ этих таблиц показывает, что для обработки дополнительного бита переноса на разных позициях h сумматор требует больших аппаратных затрат, чем в случае

сумматора без переноса. При перемещении бита переноса справа налево сложность сумматора резко возрастает, если бит переноса находится на 2-й позиции, а затем постепенно уменьшается до величины, определяемой параметрами обрабатываемого фрагмента ОБ (разрядность и рядность с учётом местонахождения битов переноса).

Аналитическая зависимость суммарных затрат от перемещения бита переноса (позиция h) явно не просматривается, т.е. для каждого конкретного случая проектирования сумматора необходимы дополнительные исследования.

Из проведенного исследования вытекает возможность дополнительной оптимизации сумматора, а также умножителя, построенного на сумматорах, обрабатывающих фрагменты ромба бит частичных произведений.

Список литературы

1. Паулін, О.М. Методологічні основи проектування компонент комп'ютерних систем паралельної обробки багаторядних кодів з використанням природної симетрії даних: автореф. дис. ... д-ра техн. наук : 05.13.05 / О.М. Паулін; Одес. нац. політехн. ун-т. — О., 2012. — 36 с.
2. Паулин, О.Н. К построению быстродействующих арифметических устройств / О.Н. Паулин // Искусственный интеллект. — 2002. — № 3. — С. 314–322.
3. Ляховецький, О.М. Методи функціонально-логічного проектування швидкодіючих арифметичних пристроїв на основі симетричних булевих функцій: Автореф. дис... канд. техн. наук / О.М. Ляховецький; Одес. держ. політехн. ун-т. — О., 1999. — 19 с.
4. Паулин, О.Н. О параллельной обработке потока данных, адаптированной к области бит произвольной конфигурации / О.Н. Паулин // Искусственный интеллект. — 2010. — № 3. — С. 127–133.

МОДЕЛЮВАННЯ ВПЛИВУ МІСЦЕПОЛОЖЕННЯ ВХІДНОГО ПЕРЕНОСУ НА СКЛАДНІСТЬ СХЕМИ СУМАТОРА

О.М. Паулін

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна

Робота присвячена визначенню залежності складності логічної схеми суматора від місця розташування вхідного переносу. Із проведеного дослідження випливає можливість додаткової оптимізації суматора, а також умножителя, побудованого на суматорах.

Ключові слова: моделювання, фрагмент, місцеположення переносу, суматор, апаратні витрати

MODELLING THE RELATIONSHIP BETWEEN COMPLEXITY OF THE ADDER SCHEME AND CARRY IN POSITION

Oleg N. Paulin

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine

The purpose of the work was to establish the relationship between the complexity of the logical scheme of the adder and the carry in position. The investigation performed provides the possibility for further optimization both of the adder and adder-based multiplier.

Keywords: modeling, fragment, adder, carry position, hardware costs

УДК 519.876.5; 004.738.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 57-67

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕОРЕТИЧЕСКИХ ПОДХОДОВ МОДЕЛИРОВАНИЯ ТРАФИКА С ТОЧКИ ЗРЕНИЯ СООТВЕТСТВИЯ СЕТЯМ НОВОГО ПОКОЛЕНИЯ

О.А. Сиропятов, В.Я. Чечельницкий

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: saa5511@ukr.net

В работе проведен анализ теоретических подходов к моделированию трафика. В результате проведенных исследований показаны принципы и основные этапы технологии моделирования высокоскоростного трафика коммерческих сетей. Показана необходимость применения комбинированного подхода для статистического описания трафика современных сетей. Вероятностное распределение анализируемых сигналов может иметь вид аддитивной смеси двух или более распределений с различными наборами параметров.

Ключевые слова: глобальные сети, сетевой трафик, моделирование трафика, матрица трафика

Введение

Современные теоретические методы и подходы описания процессов в информационных системах и сетях разнообразны и требуют научного осмысления для применения на практике. Все большее значение приобретают теоретико-вероятностные методы исследований, основанные на вероятностной трактовке протекающих в информационных системах процессов. Статистический подход позволяет более полно учесть состояние динамической системы, характер управляющих и возмущающих воздействий, результирующее поведение информационных потоков в многофункциональных сетях и во многих случаях более адекватен для решения различных практических задач [1].

Круг вытекающих из указанного подхода проблем достаточно широк: описание математических моделей случайных процессов в информационных системах, формирование на их базе статистических методов проверки гипотез и обнаружения, оценивания и фильтрации, интерполяции (сглаживания) и экстраполяции (прогнозирования), а также разработка алгоритмов оптимального управления стохастическими системами. Основными критериями при выборе теоретического подхода моделирования сети являются следующие:

- модель должна быть пригодной для описания современных высокоскоростных коммерческих сетей;
- модель должна быть универсальной, т.е. адаптируемой к различным типам сетей или их фрагментам;
- точность соответствия реальным потокам данных должна быть не более 10% при приемлемой вычислительной громоздкости;
- модель должна быть пригодной для прогнозирования поведения сети при более интенсивном трафике;

- модель должна отображать маршруты трафика и их изменение.

Для того чтобы определить, какой из теоретико-вероятностных методов наиболее близок к поведению высокоскоростных телекоммуникационных систем, и необходимо выполнить их сравнительный анализ. Задача усложняется тем, что большинство авторов осуществляли оценку точности модели при использовании данных локальных сетей, что не гарантирует пригодность подхода для больших территориально-разнесенных систем. Другими словами, необходима дополнительная проверка предлагаемых подходов, основанная на данных измерения трафика реальных высокоскоростных сетей.

Цель статьи и постановка задач исследований

Целью работы является проведение сравнительного анализа теоретических подходов моделирования сетевого трафика для разработки основных этапов моделирования высокоскоростного трафика коммерческих сетей.

Для достижения цели необходимо решить следующие *задачи*:

1. Провести анализ теоретических подходов к моделированию трафика.
2. Показать принципы и основные этапы технологии моделирования высокоскоростного трафика коммерческих сетей.
3. Обосновать необходимость применения комбинированного подхода для статистического описания трафика современных сетей.

Анализ теоретических подходов моделирования трафика

Поскольку основной математической моделью процессов, описывающих трафик в телекоммуникационных системах, является случайный поток данных, вполне оправданны попытки создания теоретической модели трафика на основании статистической теории. Случайный поток в рассматриваемом практическом приложении обладает следующими основными свойствами:

- независимость вероятностных характеристик от времени (стационарность);
- зависимости вероятностей событий (случайные процессы с памятью);
- бесконечно малая вероятность более одного события за бесконечно малый интервал времени.

Поток как случайный процесс характеризуется своими статистическими свойствами. Чаще всего используются: плотность вероятности поступления данных за период, функция вероятности потока и автокорреляционная функция.

Классической моделью трафика в информационных сетях является Пуассоновский поток. Он характеризуется набором вероятностей $P(k)$ поступления k сообщений за временной интервал t:

$$P(k) = \frac{(\lambda t)^k}{k!} \cdot e^{-\lambda t} \qquad (1)$$

где: $k = 0,1,2,\ldots$ — число сообщений; λ — интенсивность потока.

Заметим, что интервал времени измерения количества сообщений t и интенсивность потока λ являются постоянными величинами.

Для семейства Пуассоновских распределений (1) большее значение λ соответствует более широкому и симметричному графику плотности и большему объему информационных потоков. Зная вероятность поступления данных за период, можно получить распределение интервала τ между соседними событиями:

$P(\tau) = \lambda \cdot e^{-\lambda t}$. Основным свойством пуассоновского потока, обусловливающим его широкое применение при моделировании, является аддитивность: результирующий поток суммы пуассоновских потоков тоже является пуассоновским с суммарной интенсивностью

$$\lambda_{\Sigma} = \sum_{n-1}^{N} \lambda_n .$$

Однако, применение статистики (1) с учетом многофункциональности современных сетей возможно исключительно для описания очередей пакетов. Динамические процессы, происходящие в современных сетях, имеют сложную природу и относятся к стохастическим процессам. Такие свойства трафика возникают из-за недетерминированности системы в целом. Другими словами, долгосрочное прогнозирование действий, осуществляемых обрабатывающими трафик алгоритмами, невозможно предсказать, как впрочем, и массу других воздействующих на трафик факторов. На практике трафик обрабатывается алгоритмами, используемыми в различных реализациях протоколов семейства TCP/IP: генерация трафика протоколами транспортного уровня, управление трафиком на промежуточных сетевых устройствах, динамическая маршрутизация и т.д. В результате, процессы в компьютерных сетях находятся под постоянным влиянием регулирующих и возбуждающих стохастических воздействий, обуславливающих сложные флюктуации исследуемых процессов. Другими словами, требуется модель, являющаяся случайным процессом, управляемым другим случайным процессом.

В научных исследованиях последних лет отдается предпочтение описанию статистических свойств сети на основе применения Марковских скрытых цепей управляемых пуассоновской статистикой для описания очередей потоков (рис. 1).

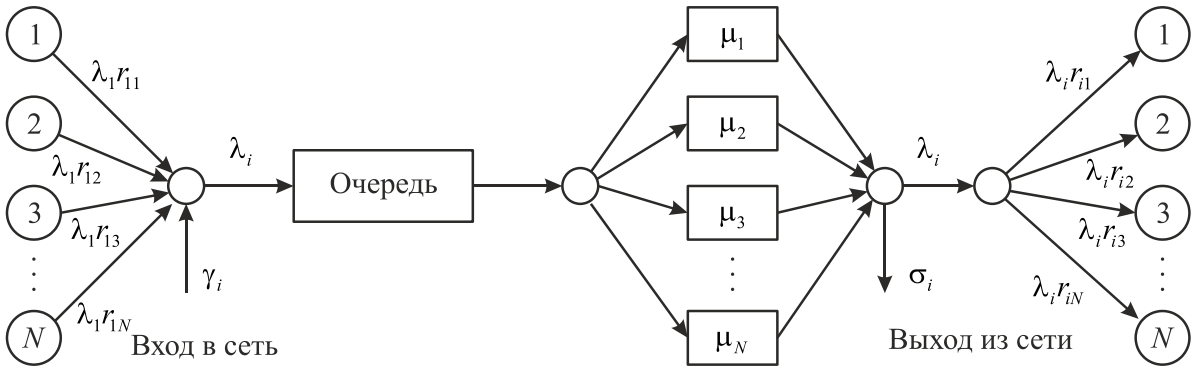


Рис. 1. Структура моделирования очередей трафика: r_{ij} — вероятность входа/выхода; λ_i — полная интенсивность потока; γ_i — параметр управления

Дискретный случайный Марковский поток характеризуется следующими свойствами

$$P(X_{n+1} = j \,|\, X_n = i_n, X_{n-1} = i_{n-1}, \ldots) = P(X_{n+1} = j \,|\, X_n = i_n)$$
$$P(X_{m+1} = j \,|\, X_n = i) = p_{ij} \qquad (2)$$

где: p_{ij} - вероятность перехода из состояния i в состояние j, $p_{ij} \geq 0$ для $\forall i, j$ и $\sum_j p_{ij} = 1$ для $\forall i$.

Процесс перехода некоторого дискретного случайного процесса из одного состояния в другое описывается матрицей переходов:

$$P = \begin{pmatrix} p_{00} & p_{01} & p_{02} & \cdots & p_{0j} & \cdots & p_{0N} \\ p_{10} & p_{11} & p_{12} & \cdots & p_{1j} & \cdots & p_{1N} \\ p_{20} & p_{21} & p_{22} & \cdots & p_{2j} & \cdots & p_{2N} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ p_{i0} & p_{i1} & p_{i2} & \cdots & p_{ij} & \cdots & p_{iN} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \ddots & \vdots \\ p_{N0} & p_{N2} & p_{N3} & \cdots & p_{Nj} & \cdots & p_{NN} \end{pmatrix}$$

Наиболее адекватно отобразить стохастические переходы сети из одного состояния в другое позволяет модель скрытых цепей Маркова (СМЦ) (рис. 2).

Для определения модели на основе СМЦ необходимо задать число возможных состояний N, объем символов используемого алфавита, M. Для некоторого конечного алфавита можно определить конечный набор вероятностей перехода $\Lambda = (a_{ij})$:

$$a_{ij} = P(s_{t+1} = j | s_t = i), 1 \leq i, j \leq N, \qquad (3)$$

где s_t — описывает текущее состояние.

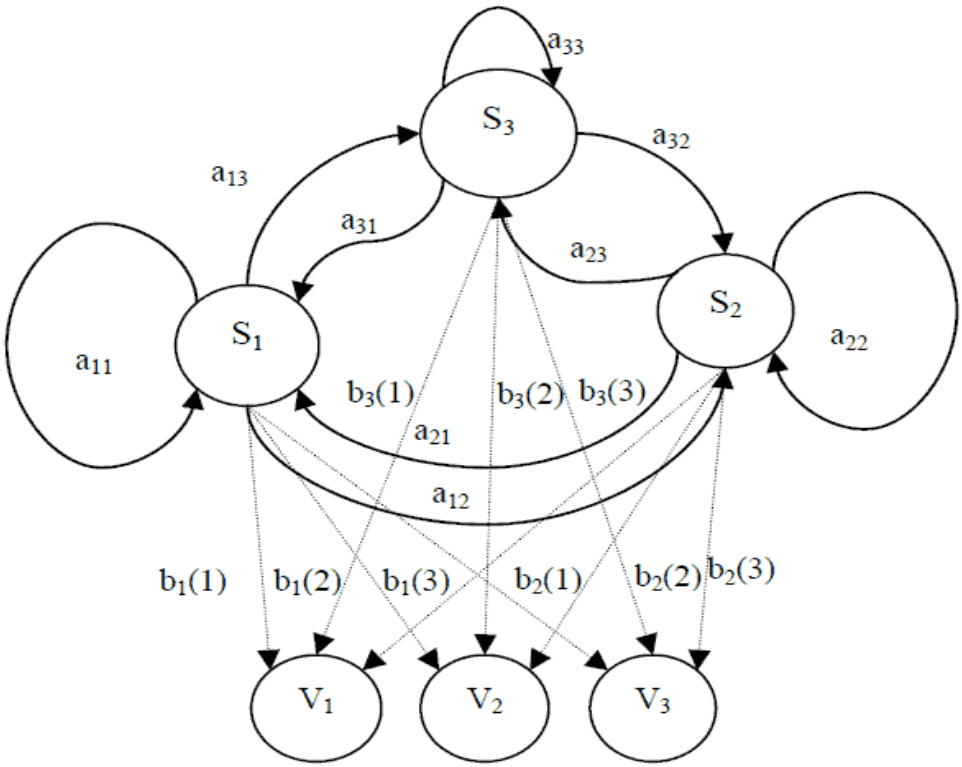


Рис. 2. Граф скрытой цепи Маркова

Для вероятностей перехода

$$\sum_{j=\&}^{N} a_{ij} = 1,\ a_{ij} \geq 0, 1 \leq i,\ j \leq N.$$

Функция вероятности возможных состояний $B = \{b_i(k)\}$

$$\begin{aligned} b_j(k) &= P(o_t = v_k | s_j = j), 1 \leq j \leq N, 1 \leq k \leq M, \\ b_j(k) &= P(o_t = v_k | q_t = j), 1 \leq j \leq N, 1 \leq k \leq M. \end{aligned} \tag{4}$$

где v_k — определяет k^{th} наблюдаемый символ алфавита, o_y - отображает текущее состояние.

Для описанной стохастической модели:

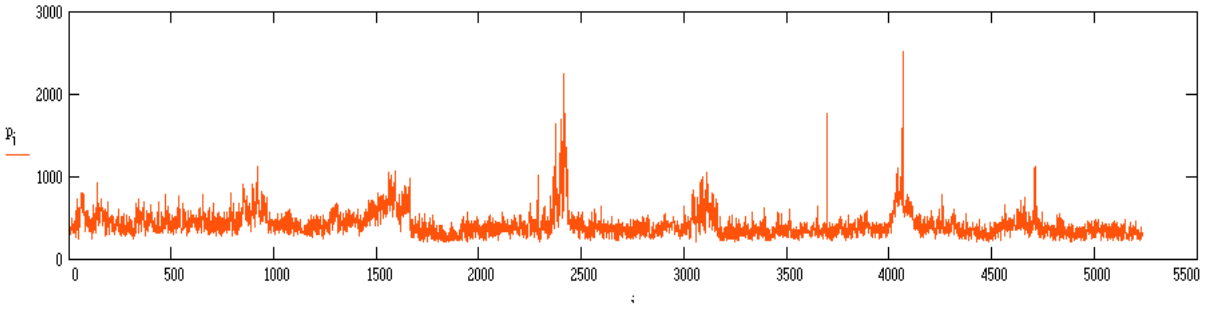
$$\begin{aligned} b_j(k) &\geq 0; 1 \leq j \leq N, 1 \leq k \leq M, \\ \sum_{k=1}^{M} b_j(k) &= 1, 1 \leq j \leq N. \end{aligned} \tag{5}$$

Если на основе, например, пуассоновской статистики определяется случайный процесс инициализации, $\pi = (\pi_i)$, где $\pi_i = P(s_1 = i)$, $1 \leq i \leq N$, то для определения СМЦ необходимо задание $\lambda = (\Lambda, B, \pi)$.

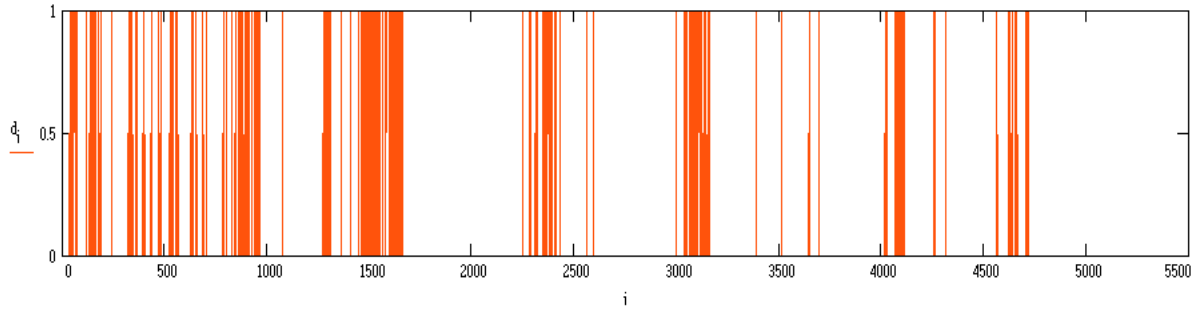
Таким образом, для рассматриваемого практического приложения при заданном λ и наблюдениях $Y = y_1, y_2, \ldots, y_T$, модель (1)–(5) позволяет оценить условную вероятность $P\{Y|\lambda\}$. Проблема моделирования будет заключаться в нахождении таких параметров модели $\{\Lambda, B, \pi\}$, которые позволят максимизировать вероятность $P\{Y|\lambda\}$.

Однако, несмотря на вычислительную сложность реализации данного подхода при моделировании даже локальных сетей проверка точности модели на данных реальных измерений высокоскоростных сетей дает большие расхождения, т.е. демонстрирует несостоятельность классических методов оценки вероятностно-временных характеристик сетей пакетной коммутации для больших территориально-разнесенных систем [2–4]. Усложнение модели посредством дополнения итерационных процедур для коррекции оценки параметров позволяет улучшить точность. Но открытыми остаются вопросы инициализации алгоритмов.

Основная проблема заключается в игнорировании стохастической динамики реальных сетей (рис. 3). Широкие перспективы применения адаптивных транспортных протоколов для мультимедиа приложений стимулируют разработку новой технологии моделирования трафика современных сетей.



а



б

Рис 3. Характер изменения задержек при передаче данных: а – абсолютные значения интервалов времени между отправкой пакета и получением подтверждения, мс; б – структура потока, превышающего пороговое значение 600 мс

С другой стороны, если протоколы маршрутизации используют только локальную информацию о связанности узлов пакетной коммутации, то для них индикатором разрыва соединения является увеличение объема выходной очереди и ее возможное переполнение, если время перекоммутации виртуального соединения превышает определенное пороговое значение. В силу случайного характера рассматриваемых событий их вероятностное моделирование должно отражать возможность появления подобных резких отклонений. Таким образом, возникает задача формализации основных свойств современного трафика.

Статистические свойства современного трафика

Многие особенности процессов в сети Интернет в настоящее время еще слабо изучены. На текущем этапе развития сети в связи с расширением мультисервисных услуг, происходит объединение разнородных потоков информации, например таких, как передача речи, данных, сигналов аналогового и цифрового телевидения, сигналов радиовещания. Основой для организации таких систем является пакетная коммутация. Однако такое объединение приводит не только к удобному использованию информационных потоков со стороны потребителя телекоммуникационных услуг, но и к некоторым техническим сложностям, например: недостаточно проработан вопрос о приоритетных потоках, необходимо учитывать пачечность трафика и т.д. Очевидно, что в агрегированном трафике современных сетей отчетливо выделяется случайная составляющая резких отклонений, корреляционная связанность которых сохраняется на весьма продолжительном интервале наблюдения. При этом статистические характеристики трафика обладают свойством временной масштабной инвариантности,

которое в современной научной литературе принято называть самоподобием [4]. Данное свойство является следствием протяженных статистических зависимостей, проявляющихся в степенном характере затухания автокорреляционных функций временных отсчетов. В зависимости от прогнозируемых изменений сетевых ресурсов можно регулировать сетевую производительность. Уменьшение объема буферной памяти относительно интенсивности потоков требует значительно более точного прогнозирования состояния сетевых ресурсов. В противном случае возникновение локальных перегрузок приводит к фактическому разрыву виртуальных соединений.

На транспортном уровне существенное влияние на характер сетевого трафика оказывает распределение времени подтверждения прихода пакетов. На рис. 4 показана зависимость логарифма экспериментально полученной функции распределения времен подтверждения передачи для трафика состоящего из 5000 пакетов.

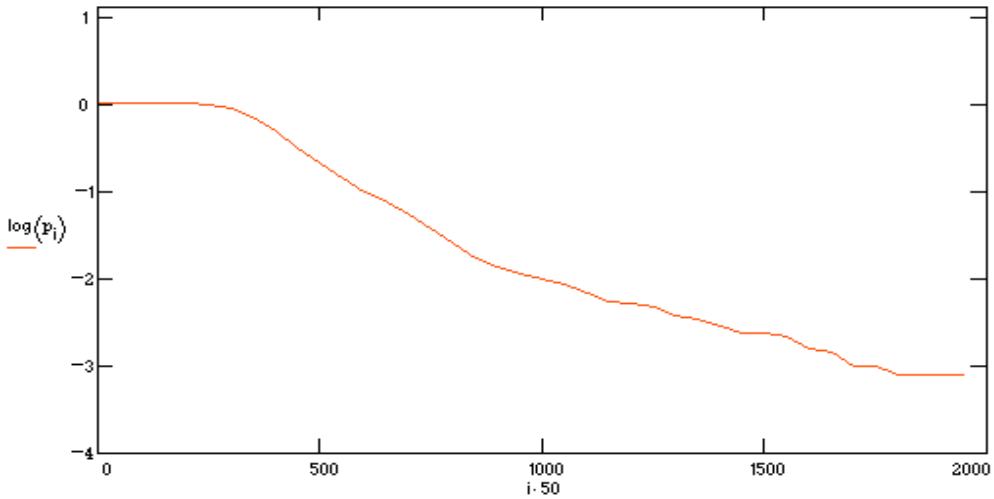


Рис. 4. Экспериментально полученное распределение времени прихода пакетов подтверждения

Фрактальные свойства нагрузки сети обусловили появление ряда моделей трафика на основе сильнокоррелированных самоподобных, или фрактальных стохастических процессов [4]. Такие функции распределения вероятности изучаются в теории статистики экстремальных значений, для применения которой необходимо выполнение следующих условий:

1. Наблюдаемый процесс обладает свойством цикличности, то есть определенной повторяемостью своего поведения через некоторый фиксированный интервал времени (интервал цикличности). Этот интервал задается, как правило, естественным путем, определяясь самой природой процесса, а не вводится искусственно.

2. Наибольший интерес с точки зрения исследователя (пользователя) представляют именно экстремальные значения, имеющие место в каждом цикле, поскольку они могут привести к серьезным последствиям, скачкообразно возрастающим потерям, к утрате ее работоспособности и неизбежным негативным последствиям различного рода.

Однако в рамках ограниченности измерений трудно говорить о самоподобии трафика современных коммерческих сетей в целом. Скорее данное свойство отображается для фрагмента сети и на заданном временном интервале. В общем случае интервал естественной цикличности может быть равен одним суткам, неделе, году.

Необходимо проанализировать и обосновать выбор аналитической зависимости функций распределения для описания наблюдаемых статистических закономерностей с учетом статистических свойств трафика сетей на основе собранных данных.

Функция распределения самоподобной случайной величины X характеризуется наличием тяжелого хвоста, если $P[X > x] \sim x^{-\alpha-1}$, $x \to \infty$, $0 \le \alpha < 2$, соответственно, плотность распределения вероятности $p(x) \sim ax^{-\alpha-1}$, $\alpha > 0$.

Не существует точных рекомендаций по выбору той или иной плотности вероятности со свойством самоподобия или в соответствие с другим определением — с тяжелым хвостом.

Наиболее распространенной является плотность распределения вероятности Парето

$$p(x) = \alpha k^{\alpha} x^{-\alpha-1}, \alpha < 2, k > 0, x \ge k, \tag{6}$$

и функция вероятности

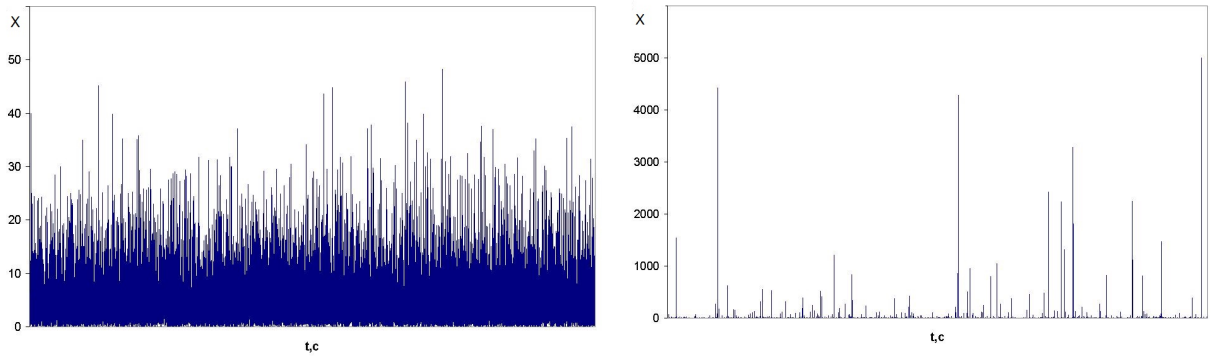
$$F(x) - P[X \le x] = 1 - (k/x)^{\alpha}. \tag{7}$$

При $\alpha \le 2$ случайный процесс (6), (7) характеризуется бесконечной дисперсией и при $\alpha \le 1$ - бесконечным средним.

Плотность распределения вероятности с тяжелым хвостом Вейбула является двухпараметрическим распределением

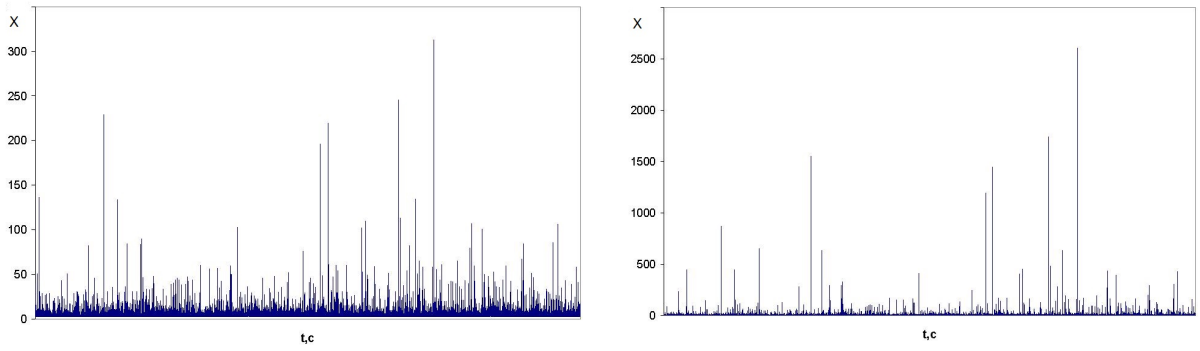
$$p(x) = \alpha\lambda^{-\alpha} x^{\alpha-1} e^{\left(\frac{x}{\lambda}\right)^{\alpha}}, \alpha, \lambda > 0, x \ge 0. \tag{8}$$

Для сравнения статистик (6) и (8) было выполнено моделирование случайных процессов (рис. 5, рис. 6).



а **б**

Рис. 5. Результаты имитационного моделирования потока с распределением Вейбулла: а - $\alpha = 2$, б - $\alpha = 1$



а **б**

Рис. 6. Результаты имитационного моделирования потока с распределением Парето: а - $\alpha = 1$; б - $\alpha = 0.1$

Наибольшую взрывоподобность проявляет поток с распределением Вейбулла. Для распределения Вейбулла оказалось достаточно сложно при небольшом среднем значении ($\mu = 5$) получить достоверные результаты для малого значения α. Это связано с тем, что значение коэффициента имеет величину такого порядка малости, что происходит влияние на процесс точности моделирования. Определенные вычислительные трудности характерны и для распределения Парето из-за большого значения дисперсии. Другими словами, для получения достоверных оценок требуется рассматривать большие объемы статистической информации. В результате эксперимента было установлено свойство масштабной инвариантности статистических характеристик. В отличие от процессов, не обладающих фрактальными свойствами, не происходит быстрого «сглаживания» процесса при усреднении по шкале времени — процесс сохраняет склонность к всплескам.

Важной задачей является определение, какая из моделей самоподобных случайных процессов приемлема для рассматриваемого приложения. Самоподобные процессы, в том числе описывающие явления в сетях передачи данных, обладают рядом свойств, существенно отличающих их от потоков, рассматриваемых в классической теории телетрафика.

Традиционно самоподобие в стохастическом процессе выявляется путем определения параметра Херста

$$H_{k,n} = \frac{1}{k} \sum_{i=n-k+1}^{n} \left(\log X_i - \log X_{i+1} \right). \qquad (9)$$

Тот факт, что $0.5 < H < 1$ считается достаточным основанием для признания процесса самоподобным (по крайней мере, асимптотически).

Имитационное моделирование и проверка условий (9) продемонстрировало неприемлемость использования логнормального распределения для рассматриваемого приложения. Данные реальных измерений трафика ОП пары фрагмента сети, соответствующей wi-fi технологии, наблюдались в течение месяца, затем был выполнен анализ статистических свойств полученного массива, был построен график хвоста эмпирической функции распределения $1 - F(x)$ в логарифмической шкале (рис. 7).

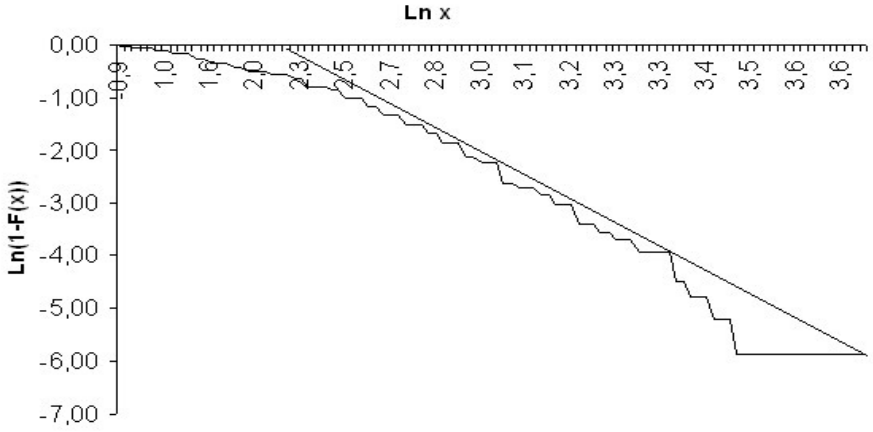


Рис. 7. График хвоста эмпирической функции распределения трафика локальной сети

Эксперимент продемонстрировал зависимость самоподобности от дня недели. Коэффициент самоподобности зависит от интенсивности трафика, а также от типа передаваемой информации. Аналогично параметр самоподобности меняется в течение суток, и это связано с особенностями поведения пользователей. Интенсивность трафика очень мала в интервале времени 02:00–08:00. В данном интервале времени параметр Хорста минимален. Рабочий день начинается в 08:00 и интенсивность трафика невелика, но, несмотря на это, параметр Хорста уже увеличивается. В интервале с 20:00 до 02:00, когда администраторы сети начинают тестировать написанный программный код в автоматическом режиме, интенсивность потока заявок к серверу вырастает очень значительно, и параметр Хорста также возрастает до значения 0.84 во все рабочие дни. Сетевой трафик в случае максимальной интенсивности (20:00–02:00) имеет более высокую степень самоподобности.

Однако данный подход применим для фрагмента сети и при ограничении временного интервала. Даже в этом случае для достижения приемлемой точности необходимо использовать комбинацию нескольких статистических составляющих, например фрактальный дробовой процесс.

Выводы

В результате проведенных исследований становятся ясным принципы и основные этапы технологии моделирования высокоскоростного трафика коммерческих сетей.

Важным выводом из проведенного анализа является необходимость применения комбинированного подхода для статистического описания трафика современных сетей.

Вероятностное распределение анализируемых сигналов, например, времени подтверждения, может иметь вид аддитивной смеси двух или более распределений с различными наборами параметров

$$P(x) = \sum_{j=1}^{m} p(x|j)p(j), \qquad (10)$$

где: $p(x|j)$ — плотность вероятности j-ой компоненты; $p(j)$ - весовой коэффициент учета j-ой компоненты в общей суперпозиции.

Открытым остается вопрос о том, какое семейство плотности вероятности нужно применять в качестве составляющих (10) для достижения наилучшей точности модели.

Очевидно, что ответ на этот вопрос зависит от того, можно ли получить данные только на основании изучения статистических свойств постоянно изменяющегося реального трафика коммерческих сетей.

Список литературы

1. Cao, J. Time-Varying Network Tomography: Router Link Data / J. Cao, D. Davis, S. Vander Wiel, B. Yu // Journal of the American Statistical Association. - vol. 95, no. 452, Dec. 2000.
2. Waldbusser, S. Remote Network Monitoring Management Information Base / S. Waldbusser // IETF RFC 2819, May 2002.
3. Van der Merwe. mmdump: A tool for monitoring Internet multimedia traffic / Van der Merwe, R. Caceres, Y. Chu, C. J. Sreenan // ACM Computer Communication Review, vol. 30, October 2000. - pp. 48-59.
4. Lakhina, A. Characterization of Network-Wide Anomalies in Traffic Flows (2004) / A. Lakhina, M. Crovella, C. Diot. May 19, 2004.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕОРЕТИЧНИХ ПІДХОДІВ МОДЕЛЮВАННЯ ТРАФІКА З ПОГЛЯДУ ВІДПОВІДНОСТІ МЕРЕЖАМ НОВОГО ПОКОЛІННЯ

О.А. Сиропятов, В.Я. Чечельницький

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: saa5511@ukr.net

У роботі проведено аналіз теоретичних підходів до моделювання трафіку. В результаті проведених досліджень показані принципи та основні етапи технології моделювання високошвидкісного трафіку комерційних мереж. Показано необхідність застосування комбінованого підходу для статистичного опису трафіку сучасних мереж. Імовірнісний розподіл аналізованих сигналів може мати вигляд адитивної суміші двох або більше розподілів з різними наборами параметрів.

Ключові слова: глобальні мережі, мережений трафік, моделювання трафіку, матриця трафіку

COMPARATIVE ANALYSIS OF THEORETICAL APPROACHES OF TRAFFIC SIMULATION IN TERMS OF CORRESPONDENCE TO NEW GENERATION NETWORKS

O.A. Siropyatov, V.J. Chechelnitsky

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: saa5511@ukr.net

An analysis of theoretical approaches to traffic simulation was performed in this work. Principles and main stages of high-speed traffic of commercial networks simulation were demonstrated as a result of investigations carried out. The need in applying combined approach for statistical description of modern networks traffic was demonstrated. Probabilistic distribution of analyzed signals can have the form of an additive mixture having two or more distributions with different sets of parameters.

Keywords: global networks, network traffic, traffic simulation, traffic matrix

UDC 004.94

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 68-76

MODELS OF DECISION-MAKING SUPPORT ON LOCAL ENERGY CONVERSION SYSTEMS

Dmitriy A. Bodarev, Alexander D. Bodarev, Sergey I. Grishin

Odessa National Maritime University,
34 Mechnikona str., Odessa, 65029, Ukraine: e-mail: grishin_si@ukr.net

We consider decision support models on local energy conversion systems in vagueness conditions. The problem of fuzzy multicriterial analysis of local energy conversion systems is considered as fuzzy non-linear programming problem of with a few incompatible criteria. We offer the sequence of decision-making steps in the fuzzy multicriterial analysis of the informal choice convolution scheme for transition from vectorial criterion to a scalar combination. We consider multi-agent model due to their ability to solve large-scale problems that are difficult to implement in single-agent approximation.

Keywords: fuzzy sets, energy conversion, decision support

Introduction

The modern scientific and technological decisions on creation of energetic complexes are characterized characterized by the transition from traditional energy development as a highly centralized system with a predominance of large generation sources to a variety of types and forms of energy development, including small distributed power engineering. Traditionally mathematical simulation of energy conversion systems is used for the solution of project tasks: load calculation, definition of transformers, transmission line route selection etc. [1]. Development of information technologies, in particular business intelligence tools, allows us to spread scope of mathematical simulation to other stages of life cycle of a power supply system [2].

The power supply system is a complex set of technical equipment. Therefore the stage of synthesis of the initial option of its structure requires decision-making in the conditions of uncertainty. The modern theory of making decision in the complicated systems allows us to describe uncertainty models by means of fuzzy set theory (FST).

Some uncertainty models aren't connected to the randomness concept, and reflect incompleteness of our knowledge of studied object and its interaction with surrounding environment. For example, the emergence of new working bodies for which the thermodynamic properties are unknown, complicates problem of estimating the energy efficiency of perspective local energy conversion systems, as obtaining information requires the long and expensive researches of thermophysical properties. Application of model of vagueness allows us to offer an effective way to the decision of this problem and to pass a traditional stage of determination of thermodynamic properties of not studied substances.

Comparison over of the uncertainty theories is presented in [3]. Fuzzy models are the system models, which are constructed, used and analysed with principles of FST and fuzzy logic. Fuzzy models provide an essential tool for research of both individual components and the whole system at various stages of its analysis in the case of qualitative elements domination over the quantitative.

Popular mathematical modeling packages (MATLAB, fuzzyTECH etc.), allow user to concentrate on application questions of fuzzy inference systems and to be released from

developing those systems. However, the use of such subject-oriented software requires analysts to involve in design that restricts FST application.

Data Mining is intended to improve power supply system structure using results of laboratory measurements, monitoring power system parameters, computer simulations. Effective means of solving complex Data Mining problems difficult to formalize are artificial neural networks (ANNs). Models using ANNs are universal and bind in unified manner target agent functions (thermodynamic, economic, eecological, social, etc.) with management variables. The disadvantage of neural network paradigm is the large volume of training sample.

Proceeding from explained, development of the software tools intended for mathematical simulation of energy conversion systems, remains the actual task

Objective and task

The *aim* is to create an information system to support decision-making (DSS) on local systems of electrical power supply of customers as a part of low or middle power energetic complexes.

To achieve this goal in the paper we solve such *problems*:

- formalization of the problem of fuzzy and multi-criteria selection of energy system;
- creation data warehouse for project and experimental data;
- construction of training samples for ANNs;
- providing of high-rate of convergence and reliability in the concordance of vagueness models of data and knowledge due to application of multiagent calculating models.

Formalization of the problem

Formulation of any problem of multi-choice contains three objects - a set of possible solutions, vector criterion and the preference relation of the decision maker.

Applying the Edgeworth-Pareto principle allows exclude obviously unacceptable solutions from the set of all possible. Informed choice of a Pareto-optimal solution is possible only if there is information, often in the form of coefficients of the relative importance of the criteria that are usually appointed by experts. Informed choice of a Pareto-optimal solution is possible only if there is information, often in the form of coefficients of the relative importance of the criteria that are usually appointed by experts.

The principle of hierarchy analysis [4], based on pairwise comparisons of objects of choice on different criteria with use of tenball scale and the subsequent ranking of a set of objects for all criteria and goals can be used to determine the relative importance of criteria. Mutual relations between criteria are taken into account by the constructing of hierarchy of criteria and application of pair comparisons for the exposure of importance of criteria and subcriteria. The method is simple and gives a good accordance to intuitional presentations.

The basic method of measuring of experts preferences, used in the method of hierarchy analysis, is pair comparisons. Each expert shall compare in pairs all objects by each criterion and give an assessment of preference on a tenball scale. The choice of this scale due to the following reasons: the higher the number of grades of the scale, the more accurate the expert assessment. It is extremely difficult to carry out simultaneous comparing more than nine objects. Therefore there are enough nine gradations for their distinguishing.

Results of an expert assessment of objects register in the form of the matrixes of pairwise comparisons. The principal eigenvector of the matrix is interpreted as a vector of priorities of the objects being compared.

R. Bellman and L. Zadeh offered a scheme [5], realizing the process of making decision in the conditions of vagueness, when aims and limitations of multicriterion task are set by

fuzzy sets. According to the principle of the Bellman-Zadeh diagram decision-making is meant as a choice of the object which is at the same time fitting both the indistinct purposes, and indistinct restrictions.

A model to support decision making based on fuzzy sets tools [2] is used in our DSS. Model takes into account the uncertainty of purpose, as a consequence of the incompleteness of our knowledge about the reaction of the environment on the functioning of local energy conversion systems. It is assumed that the target functions - exergetic efficiency and net income, along with environmental restrictions in the conditions of uncertainty of different nature can be represented by fuzzy sets. The global criterion of balance K is a vectorial criterion.

The problem of thermoeconomic optimization is considered as a problem of indistinct non-linear programming with n incompatible criteria (for example, economic and thermodynamic), m – management variables and k non-linear restrictions:

$$Optimize K\left[K_1(X), K_2(X), \ldots, K_n(X)\right], i = 1,2,\ldots,n$$

under conditions

$$C_i \equiv G_{Li} \le G_i(X) \le G_{Ui}, i = 1,2,\ldots,k,$$

$$X_{Li} \le Xx_i \le X_{Ui}, i = 1,2,\ldots,m,$$

where $K_i(X)$ represent the fuzzy local criteria of effectiveness; $X(X_1, X_2, \ldots, X_m)$ – vector of required management variables; G_{Li}, G_{Ui} - lower and upper limits of restrictions of $G_i(X)$, respectively; X_{Li} и X_{Ui} - lower and upper bounds for the required management variables.

Multicriteria approach is based on a combination of the formal and informal procedures of decision-making for finding of an alternative solution. The formal mathematical means for permission of a multicriteria problem are absent and additional exogenetic information is necessary. According to [3-5] the next sequence of decision-making steps in the fuzzy thermoeconomic analysis of the energytransforming systems is used.

- Determination of area of an optimality according to Pareto (or compromise areas) - XP, in which the coordinated solution of the conflict between criteria with opposite interests is reached;
- Submission criteria and constraints in the form of fuzzy sets to display of unstructured situations (so-called procedure of "fuzzying" of criteria);
- Informal choice of the diagram of a convolution for transition from vectorial criterion $K\left[K_1(X), K_2(X), \ldots, K_n(X)\right]$ to a scalar combination $K_1(X), K_2(X), \ldots, K_n(X)$;
- Estimation of final vector $X_{opt} \in X_P$, minimizing the fuzzy sources of uncertainty.

In the field of Pareto there is no single optimum decision, rather it is a set of alternative solutions. These decisions are optimum in a wider sense - there are no solutions of more significant if all aims are simultaneously attained. The optimality according to Pareto is considered as the tool for receiving alternatives, from which the designer can choose the final decision. Determination of area of Pareto is carried out by means of algorithm of normal boundaries [6].

The following step consists in determination of a final set of parameters of Pareto set, by means of additional external information and transformation of vectorial criterion in the scalar. This step represents a certain complexity in aspect of its formalization. In accordance with the recommendations of [7] obtained from the analysis of ways to convert the vector criterion in scalar we used the scheme [3]. A final decision was determined as a result of

intersection of all fuzzy criteria and restrictions displayed by their functions of accessory $\mu(X)$:

$$\mu_K(X) = \mu_{Kth}(X) \cap \mu_{Kec}(X) \cap \mu_{Gi}(X), i = 1,2,\ldots,k,\ X \in X_P .$$

Membership functions of objectives and constraints can be chosen in different ways depending on a problem context. One possible fuzzy convolution schemes is shown below:

- As an initial approximation choose a vector *X*. The maximum (minimum) values for each criterion of K_i are set as result of the solution of the scalar task of maximizing (minimization) for each of criteria. Results are designated as "ideal" points $\{X_j^0,\ j = 1,\ldots,m\}$.
- Matrix [T] where diagonal elements – "ideal" points, it is defined as follows:

$$[T] = \begin{bmatrix} K_{th}(X_1^0) & K_{th}(X_2^0) \\ K_{ec}(X_1^0) & K_{ec}(X_2^0) \end{bmatrix}$$

- The maximum and minimum boundaries of criteria are defined:

$$K_i^{\min} = \min_j K_j(X_j^0) = K_i(X_i^0),\ i = 1...n;$$
$$K_i^{\max} = \max_j K_j(X_j^0),\ \ i = 1...n.$$

- Membership functions for all fuzzy goals presented in the form:

$$\mu_{Ki}(X) = \begin{cases} 0, & if\ \ K_i(X) > K_i^{\max} \\ \dfrac{K_i^{\max} - K_i}{K_i^{\max} - K_i^{\min}} & if\ \ K_i^{\min} < K_i \le K_i^{\max}, \\ 1, & if\ \ K_i(X) \le K_i^{\min} \end{cases}$$

- Fuzzy constraints have the following structure:

$$C_j(X) \le C_j^{\max} + d_j,\quad j = 1, 2,...q$$

where d_j – real parameter which designates distance from admissible offset for boundary $C_j^{\max}$ of *j-th* restriction. The corresponding membership function is defined as follows:

$$\mu_{Cj}(X) = \begin{cases} 0, & if\ \ C_j(X) > C_j^{\max} \\ 1 - \dfrac{C_j(X) - C_i^{\max}}{d_j} & if\ \ C_j^{\max} < C_j(X) \le C_j^{\max} + d_j, \\ 1, & if\ \ C_j(X) \le C_j^{\max} \end{cases}$$

- The final decision is defined as the intersection of all indistinct criteria and constraints represented by their membership functions. This problem reduces to the standard nonlinear programming problem: find such values of *X* and λ, where, on maximizing λ, conditions will be satisfied:

$$\lambda \le \mu_{Ki}(X), \quad i = 1,2,...,n;$$
$$\lambda \le \mu_{Cj}(X), \quad j = 1,2,...,q$$

The decision of multicriterion problem exposes the value of operator of optimality *Optimize* and depends on experience of accepting decision person and his understanding of problem.

Data warehouse designing

Mining can not rely only on the data of their own corporation development. These data will be insufficiently. Tools, allowing us to integrate and store heterogeneous data from various sources are necessary.

As a model of design and experimental data warehouse it is common to use a multi-dimensional space with discrete number of values for each dimension. In the model we selected as measures are taken Time, capital costs, insurance costs, labor costs, ecology indicators are taken as dimensions in the model we selected. Target functions - exergetic efficiency and net profit are used as measures or facts. Time is a hierarchical dimension, measures and dimensions are stored in the data mart using the scheme snowflake.

The developed integration tools allow you to import data from available sources in a network.

Construction of training samples for ANNs

Using multi-layer neural networks as predictive models is caused by ability of ANNs to simulate arbitrary nonlinear continuous functions from training on a set of previously known data.

Neural network models appear to be most promising for modeling energy conversion systems, since they allow you to construct training sets for ANNs based on known models, that already have proved the adequacy, and, then, using the appropriate algorithms, to create neural networks, displaying efficiency criteria of local energy conversion systems, for the further acceptance of compromise decisions.

Procedure of identification of local energy conversion systems on the basis of neuronetwork model structures is multi-stage and includes the following main stages:

- construct the set of data that is used to train the data model;
- the choice of the model structure;
- model training;
- decision making on the adequacy of the model.

Standard training algorithm that implements classical scheme back error propagation is the gradient descent method. Program implementations of algorithms were borrowed by us from a neuronetwork packet of MATLAB [8]. The choice of a method of training isn't the universal and each new task requires its own rules for its decision.

The assessment of efficiency of cycles of energytransforming systems is carried out by methods of engineering thermodynamics. If thermodynamic properties of working environments are known, the calculation of the transformation coefficients (COP - Coefficient Of Performance) in direct and inverse cycles is carried out according to standard expressions. Energy efficiency of direct and inverse cycles is a functional of the parameters of equations of state working environments, for example, the critical parameters and a normal boiling point (input values). To define local energy conversion systems transformation coefficients for the new or low-studied working environment of calculation of thermodynamic properties, it is necessary to construct training set for known working bodies, for that the coefficient of

transformation or other technological indexes (output values) is known. After completing the construction of an artificial neural network, we will be able to predict the COP or other value for the new working body only by its input parameters.

Application of multiagent calculating models

To provide reasonable complexity of model training, in the paper, an approach that uses a class of computational models is considered - the so-called multi-agent models [9], for simulation of a set of the purposes of the local energy conversion system separate elements, which as a result of interaction create global properties of system, as a whole. The mathematical apparatus providing the solution of such tasks includes elements of game theory, complex systems theory, evolutionary programming and other sections of applied mathematics. The general structure of agent-based models based on the triple system "stimulus - response - consensus" and it is implemented in the form of interactive model. Interactive scheme carried out in stages. In the beginning a query follows from an arbitrary agent about possibility of achievement of its local aim. Other agents, depending on own purposes, create response of a network to this request. The dialogue established consensus between agents, providing stability of the system. Totality of such processes provides a transition from a microlevel (separate agents) to the macrolevel (system as whole). Thus, a simple behavior of isolated agents generates complicated behavior of the whole system.

Growing interest in the study of multi-agent systems is due such their intrinsic quality as ability to solve problems of big dimensionality, which are difficult for implementing in single agent approximation. High speed of convergence and reliability in coordination of different models of uncertainty of data and knowledge is thus provided. The most widely used agent-based models for concerted solutions under the coordination of the various points of view in dialog communicative processes [10]. Software of different architecture [11-13] are developed for information support the agent-based models in processes of coordination, communication and concordance. Software package RETSINA (Reusable Task Structure Based Intelligent Network Agents), proposed in [14], is among computing instruments of agent-based simulation of general purpose, constructed according to the scheme of the purpose of the agent as response to different incentives. The Multiagent Systems Engineering (MaSE) [15] is based on sequence of operations, starting from the initial specification of the system and to the adoption of solutions. At the analysis stage MaSE model uses the hierarchy of goals, while on design stage classes of agents both the appropriate class diagrams and communications are created. In [16] UML extension (AUML packet) is offered. Different aspects of simulation of the agents, including both class diagrams of agents, and charts of protocols are provided in AUML. Though these approaches, in principle, support cooperation of personal agents, collective interaction is insufficiently elaborated. Methodology Tropos [17] aims at making the analysis of exogenous requirements and constraints in the implementation of the decision-making sequence. Absence of support of protocols and simulation of dynamics of system is marked [18] as shortcomings of this approach. These disadvantages are avoided in the concept Prometheus [19], in which the software of engineering tasks and detail processes in the agent-based networks are supported. Here 3 phases are considered: 1) system specification; 2) agents network architecture design; 3) detailed and specified design of a network. DECAF (Distributed, Environment-Centered Agent Framework) system [20] is a tool for designing, development and implementation of agent-based objectives in a complex environment. Performed analysis of tools confirmed the possibility of real-world multi-agent systems development.

Conclusion

The developed system is tested on the problems of constructing the training samples from agent-based models for finite-time direct and reverse cycle power plants and training samples from agent-based models of the dynamics of energy efficiency of refrigeration systems.

It is expedient to apply in software implementations of DSS on local systems of electrical power supply of customers the perspective methods of simulation using fuzzy models, multi-dimensional data warehouse, neuronetwork model structures and multiagent calculating models.

References

1. Винославский, В.Н. Автоматизация проектирования систем электроснабжения. / В.Н. Винославский, В.И. Тарадай, У. Бутц, Д. Хайнце. - К: Выща школа. 1988.
2. Бодарев, Д.А. Информационные технологии принятия решений в моделях устойчивого развития локальных систем преобразования энергии / Д.А. Бодарев, В.Х. Кирилов // Электротехнические и компьютерные системы. - 2012. - № 8.
3. Ярушкина, Н.Г. Основы теории нечетких и гибридных систем. / Н.Г. Ярушкина. - М.: Финансы и статистика, 2008.
4. Saaty, T. L., The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. McGraw-Hill, 1980.
5. Bellman, R.E. Decision-making in a fuzzy environment. / R.E. Bellman, L.A. Zadeh // Management Science, 1970, 17, № 4, pp. 141–164.
6. Das, I. Normal Boundary Intersection: A New Method for Generating the Pareto Surface in Nonlinear Multi-criteria Optimization Problems. [Электронный ресурс] / I. Das, J. Dennis. Режим доступа: www.owlnet.rice.edu/~indra/ NBIhomepage. html
7. Mazur, V. Optimum Refrigerant Selection for Low Temperature Engineering. Low Temperature and Cryogenic refrigeration. / V. Mazur. // Kluwer Academic Publishers, 2003/ pp.101-118.
8. Дьяконов, В.П. MATLAB 6.5 SP1/7/7 SP1/7 SP2 + Simulink 5/6. Инструменты искусственного интеллекта и биоинформатики. / В.П. Дьяконов, В.В.Круглов. – М.: СОЛОН-ПРЕСС. 2006.
9. Bonabeau, E. Agent-based modeling: methods and techniques for simulating human systems. / E. Bonabeau. // In Proc. National Academy of Sciences 99(3), 2001. pp. 7280-7287.
10. Nwana, H. S. Software agents: An overview. / H. Nwana. // Knowledge Engineering Review, 11(3), 1996, pp. 1–40.
11. Xu, H. ADK: An agent development kit based on a formal design model for multi-agent systems. / H. Xu, S. Shatz. // Automated Software Engineering, 10(4), 2003, pp. 337–365.
12. Yim, H. S. Agent-based adaptive travel planning system in peak seasons. / H.S. Yim, H.J. Ahn, J.W. Kim, S.J. Park. // Expert Systems with Applications, 27(2), 2004, pp. 211–222.
13. Zambonelli, F. Developing multiagent systems: The Gaia methodology. / F. Zambonelli, N.R. Jennings, M. Wooldridge. // ACM Transactions on Software Engineering and Methodology (TOSEM), 12(3), 2003, pp. 317–370.
14. Sycara, K. The RETSINA MAS infrastructure. / K. Sycara, M. Paolucci, M. Van Velsen, J. Giampapa. // Autonomous Agents and Multi-Agent Systems, 7(1), 2003, pp. 29–48.
15. DeLoach, S. A. Multiagent systems engineering. / S.A. DeLoach, M.F. Wood, C.H. Sparkman. // International Journal of Software Engineering and Knowledge Engineering, 11(3), 2001, pp. 231–258.
16. Bauer, B. Agent UML: A formalism for specifying multiagent software systems. / B. Bauer, J.P. Muller, J. Odell. // International Journal of Software Engineering and Knowledge Engineering, 11(3), 2001, pp. 207–230.
17. Bresciani, P. Tropos: An agent-oriented software development methodology. / P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, J. Mylopoulos. // Autonomous Agents and Multi-Agent Systems, 8(3), 2004, pp. 203–236.
18. Dam, K. H. Comparing agent-oriented methodologies. / K.H. Dam, M. Winikoff. // 5th International Bi-conference Workshop on Agent-Oriented Information Systems (AOIS'03), July 2003, Melbourne, Australia, pp. 79–94.

19. Padgham, L. Prometheus: A methodology for eveloping intelligent agents. / L. Padgham, M. Winikoff. // Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, July 15–19, 2002, Bologna, Italy .
20. Graham, J. DECAF — a flexible multi agent system architecture. / J. Graham, K. Decker, M. Mersic. // Autonomous Agents and Multi-Agent Systems, 7(1), 2003, pp. 7–27.

МОДЕЛІ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПО ЛОКАЛЬНИХ СИСТЕМАХ ПЕРЕТВОРЕННЯ ЕНЕРГІЇ

Д.О. Бодарев, О.Д. Бодарев, С.І. Гришин

Одеський національний морский університет,
вул. Мечнікова, 34, Одеса, 65029, Україна: e-mail: grishin_si@ukr.net

Розглянуто моделі підтримки прийняття рішень в умовах невизначеності у локальних системах перетворення енергії. Задачу нечіткого багатокритеріального аналізу локальних систем перетворення енергії розглянуто як задачу нечіткого нелінійного програмування з кількома несумісними критеріями. Запропонована послідовність кроків ухвалення рішення в нечіткому багатокритерійному аналізі неформального вибору схеми згортки для переходу від векторного критерію до скалярної комбінації. Розглядаються мультиагентні моделі завдяки їх здатності вирішувати задачі великої розмірності, які важко реалізувати в одноагентному наближенні.
Ключові слова: нечіткі множини, перетворення енергії, підтримка прийняття рішень

МОДЕЛИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ЛОКАЛЬНЫМ СИСТЕМАМ ПРЕОБРАЗОВАНИЯ ЭНЕРГИИ

Д.А. Бодарев, А.Д. Бодарев, С.И. Гришин

Одесский национальный морской университет,
ул. Мечникова, 34, Одесса, 65029, Украина: e-mail: grishin_si@ukr.net

Рассмотрены модели поддержки принятия решений в условиях неопределенности в локальных системах преобразования энергии. Задача нечеткого многокритериального анализа локальных систем преобразования энергии рассмотрена как задача нечеткого нелинейного программирования с несколькими несовместимыми критериями. Предложена последовательность шагов принятия решения в нечетком многокритериальном анализе неформального выбора схемы свертки для перехода от векторного критерия к скалярной комбинации. Рассматриваются мультиагентные модели благодаря их способности решать задачи большой размерности, которые трудно реализовать в одноагентном приближении
Ключевые слова: нечеткие множества, преобразования энергии, поддержка принятия решений

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 76-84

МЕТОД ЛОКАЛИЗАЦИИ И ИДЕНТИФИКАЦИИ ОРИГИНАЛЬНОЙ И КЛОНИРОВАННОЙ ОБЛАСТЕЙ ИЗОБРАЖЕНИЯ

Е. Ю. Лебедева

Одесский национальный политехнический университет,
просп. Шевченко, 1, 65044, Украина; e-mail: whiteswanhelena@gmail.com

В работе разработан теоретически обоснованный метод локализации и идентификации оригинальной и клонированной областей изображения. По результатам экспериментов и наблюдений выявлены качественные отличия оригинальной области от клонированной. Разработан математический базис для формального выявления предложенных качественных отличий.

Ключевые слова: фальсификация изображения, выявление фальсификации, клонирование, локализация области.

Введение

Развитие технологий компьютерной, фото и видео техники позволяет быстрее создавать и обрабатывать большие объемы информации. Простота использования программного обеспечения, например, графических редакторов, и рост их возможностей создают благоприятную основу для развития и широкого использования цифровой фальсификации. Объектами фальсификации выступают цифровые изображения (ЦИ) и цифровое видео (ЦВ). Самым простым и доступным способом создания фальсификации ЦИ с помощью графических редакторов является клонирование. ЦИ могут использоваться как материал для журналов, как доказательство в суде, в медицинских целях и т.п. Поэтому проверка предоставляемых ЦИ на наличия фальсификаций является актуальной задачей. При этом также важно знать в случае обнаружении фальсификации, какая область является оригинальной, а какая – клонированной.

Постановка задачи и цель исследования

В работе рассматриваются фальсификации, созданные путем клонирования одной или нескольких частей того же изображения, так как этот вид фальсификации является самым легко реализуемым и широко распространённым. Для создания такого рода фальсификаций используются такие графические редакторы как Adobe Photoshop, GIMP и другие. Для создания фальсификации путем клонирования в этих графических редакторах можно воспользоваться такими инструментами как Прямоугольное выделение, Лассо, Штамп и т.п. Для лучшего визуального внедрения клонированных областей можно воспользоваться такими инструментами, как Размытие, Яркость и контраст, Микширование каналов и т.п. Данные инструменты позволяют создавать фальсификации, незаметные человеческому глазу.

Целью является разработка метода локализации и идентификации оригинальной и клонированной областей фальсифицированного ЦИ.

Для достижения поставленной цели необходимо решить следующие *задачи*:

- Найти качественные отличия оригинальной области от клонированной.
- Разработать математический базис для формального выявления этих качественных отличий.
- Определить количественные значения параметров, позволяющие отделить клонированную область от оригинальной.
- Разработать метод локализации и идентификации оригинальной и клонированной областей.

Качественные отличия оригинальной области от клонированной

Инструменты выделения в графических редакторах позволяют создавать клонированные области любого размера и формы. Чтобы клонированные области были не заметны человеческому глазу и наилучшим образом внедрились в ЦИ, их дополнительно обрабатывают. Одним из средств такой обработки является инструмент Размытие (Blur). Инструмент Размытие (Blur) уменьшает контраст между точками ЦИ. Его используют, чтобы смягчить границы между фрагментами изображения (рис. 1).

а

б

Рис.1. Применение инструмента Размытие: а – клонированная область без обработки; б – клонированная область после обработки инструментом Размытие

Таким образом, применение инструмента Размытие сгладит край клонированной области, и сделает его визуально менее заметным. Будем считать, что клонированная область отличается от оригинальной, применением к ее границе инструмента Размытия.

Математический базис для формального выявления качественных отличий

Состояние любой информационной системы, например, ЦИ, формально описывается совокупностью однозначно определенных ее параметров, таких как сингулярные числа (СНЧ) и сингулярные вектора (СНВ) соответствующей матрицы (матриц) [1].

Пусть имеется ЦИ в цветовой модели RGB. Преобразуем ЦИ из RGB в модель YUV. Модель YUV (1) основана на разложении изображения на три составляющие: Y – самая значимая составляющая, определяющая яркость точки изображения; U, V – две цветовые составляющие (их называют цветоразностями, т.к. $U = G - R$, $V = G - B$):

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.522 & 0.311 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

Пусть имеем блок ЦИ с матрицей яркости Y. Получим новый блок Y' путем размытия блока Y. Используемый вид размытия незначительно изменит Y, т.е. матрицы Y и Y' будут близкими по значениям.

Для матриц Y и Y' вычислим нормальные сингулярные разложения

$$Y = U\Sigma V^T \text{ и } Y' = U'\Sigma' V'^T,$$

где матрицы $U = (u_1,...,u_n)$, $\Sigma = diag(\sigma_1,...,\sigma_n)$, $V = (v_1,...,v_n)$; $u_i, v_i, i = \overline{1,n}$, - столбцы матриц U, V - левые и правые лексикографически положительные ортонормированные СНВ Y, $\sigma_1 \geq ... \geq \sigma_n \geq 0$ - СНЧ Y. Матрицы $U' = (u'_1,...,u'_n)$, $\Sigma' = diag(\sigma'_1,...,\sigma'_n)$, $V' = (v'_1,...,v'_n)$, $u'_i, v'_i, i = \overline{1,n}$, - столбцы матриц U', V' - левые и правые лексикографически положительные ортонормированные СНВ Y', $\sigma'_1 \geq ... \geq \sigma'_n \geq 0$ - СНЧ Y'.

Схожесть блоков Y и Y' влечет за собой схожесть значений их СНЧ. Операция размытия затрагивает в большей степени высокие и средние частотные составляющие сигнала-изображения. Поэтому для определения значения параметров близости Y и Y' будем использовать $\Sigma = diag(\sigma_1,...,\sigma_n)$ и $\Sigma' = diag(\sigma'_1,...,\sigma'_n)$, кроме первых (максимальных).

Для СНЧ Y и Y' построим линейную аппроксимацию вида $y = ax + b$ и $y' = a'x + b'$ соответственно. Схожесть блоков Y и Y' влечет за собой близкое расположение прямых $y = ax + b$ и $y' = a'x + b'$. В качестве параметра близости кривых будем использовать следующие коэффициенты: $coef_1 = \frac{a}{a'}$ и $coef_2 = \frac{b}{b'}$

Для оригинального блока Y и размытого Y' выполняются неравенства (2):

$$\begin{cases} P_1 < coef_1 < P_2 \\ P_1 < coef_2 < P_2 \end{cases}, \quad (2)$$

где P_1 и P_2 - пороговые значения, устанавливаемые экспериментально, для чего был проведен вычислительный эксперимент, в процессе которого использовались блоки размерности 8×8, которые размывались в программе Adobe Photoshop инструментом Размытие (Blur) с радиусом в половину блока. В ходе этого эксперимента были определены числовые значения для параметров P_1 и P_2: $P_1 = 1.0$; $P_2 \approx 1.099$

Метод локализации и идентификации оригинальной и клонированной областей

На основе полученных выше результатов предлагаем метод локализации и идентификации оригинальной и клонированной областей. Метод разделен на следующие этапы:

1. Обнаружение клонированных областей ЦИ;
2. Локализация клонированных областей ЦИ и идентификация оригинальной и клонированной областей;
3. Формирование результирующих изображений с обнаруженными и идентифицированными областями.

Исследуемые изображения хранятся в формате RGB. На первом этапе для ускорения процесса обнаружения клонированных областей преобразуем ЦИ из RGB в YUV, и будем использовать только первую компоненту - Y.

Для запоминания местоположения блока будем использовать систему координат, предложенную на рис.2. Под координатами блока будем понимать координаты верхнего левого угла блока.

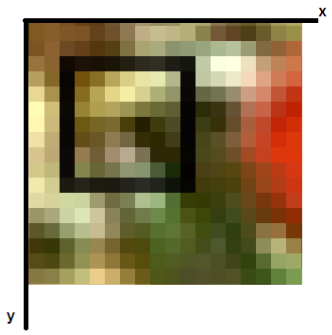


Рис.2. Система координат ЦИ

Рассмотрим основные шаги первого этапа [2, 3]:

1. Разбить матрицу яркости Y ЦИ на множество пересекающихся блоков размерами $p\times p$ пикселей: $C=\{c_1,c_2,\ldots,c_s\}$, таких что: $\bigcup_{i=1}^{s} c_i = Y$ (здесь каждый последующий блок c_i отличается от предыдущего c_{i-1} сдвигом на 1 пиксель вправо, влево, вниз или вверх).

2. Каждый блок c_i, $i=1,\ldots,s$ рассмотрим в паре со всеми c_j, $j=1,\ldots,s$, $j\neq i$, соответственно. Для каждой пары:

2.1. Вычислим коэффициент корреляции $cor = correlation(c_i, c_j)$

2.2. Если $cor = 1$, то запоминаем координаты блоков, для которых выполняется это условие: $xy_к =< i, j >$, где $XY = \{xy_1, xy_2, \ldots, xy_k, \ldots\}$.

Таким образом, после окончания первого этапа в XY сохраняются координаты обнаруженных блоков, соответствующих оригинальной и клонированной областям ЦИ.

Следующим этапом объединим обнаруженные блоки в объекты и идентифицируем объекты как оригинальный и клонированный. Локализация осуществляется посредством использования координат XY обнаруженных блоков. В данной работе рассмотрим метод разделения блоков на два объекта.

Под центром объекта будем понимать координаты, соответствующие центру области, занимаемой объектом. В процессе локализации блоков, значения координат центра будем пересчитывать. Пересчет осуществляется по координатам уже локализованных блоков.

1. Пусть центр первого объекта - координаты первого обнаруженного блока $center_1 = (center_1^x, center_1^y) =< x_1, y_1 >$, а центр второго объекта - координаты второго обнаруженного блока $center_2 = (center_2^x, center_2^y) =< x_2, y_2 >$, где x_1, y_1 и x_2, y_2 - элементы из XY.

2. Для каждой пары координат $xy_i =< x_i, y_i >$ и $xy_j =< x_j, y_j >$ из $XY = \{xy_1, xy_2, \ldots, xy_i, xy_j, \ldots, x_m y_m\}$ выполняем следующие шаги:

2.1 Вычисляем расстояние от центра объектов до текущих пар координат

$$d_{1i} = \sqrt{(center_1^x - x_i)^2 + (center_1^y - y_i)^2} \text{ и } d_{2i} = \sqrt{(center_2^x - x_i)^2 + (center_2^y - y_i)^2},$$

$$d_{1j} = \sqrt{(center_1^x - x_j)^2 + (center_1^y - y_j)^2} \text{ и } d_{2j} = \sqrt{(center_2^x - x_j)^2 + (center_2^y - y_j)^2}.$$

2.2 Если $d_{1i} \le d_{2i}$, то координаты $< x_i, y_i >$ относим к первому объекту $first_q =< x_i, y_i >$. В противном случае – ко второму объекту $second_z =< x_i, y_i >$, где $F = \{first_1, \ldots first_q, \ldots\}$ и $S = \{second_1, \ldots second_z, \ldots\}$.

Если $d_{1j} \le d_{2j}$, то координаты $< x_j, y_j >$ относим к первому объекту $first_q =< x_j, y_j >$. В противном случае – ко второму объекту $second_z =< x_j, y_j >$, $second_z =< x_i, y_i >$, где $F = \{first_1, \ldots first_q, \ldots\}$ и $S = \{second_1, \ldots second_z, \ldots\}$.

2.3 Проверяем, была ли использована операция размытие к блокам с координатами соответствующим четырем направлениям (вверх, вправо, вниз, влево) относительно $< x_i, y_i >$ и $< x_j, y_j >$:

- для направления вверх получаем матрицы цветов R, G, B блоков с координатами $< x_i, y_i - 1 >$ и $< x_j, y_j - 1 >$;
- для направления направо получаем матрицы цветов R, G, B блоков с координатами $< x_i + 1, y_i >$ и $< x_j + 1, y_j >$;
- для направления вниз получаем матрицы цветов R, G, B блоков с координатами $< x_i, y_i + 1 >$ и $< x_j, y_j + 1 >$;
- для направления влево получаем матрицы цветов R, G, B блоков с координатами $< x_i - 1, y_i >$ и $< x_j - 1, y_j >$;

2.4 Для блоков каждого направления выполняем следующие шаги:

2.4.1 Пусть имеем матрицы цветов R, G, B для блоков текущего направления $c_i^{(R)}, c_i^{(G)}, c_i^{(B)}$ и $c_j^{(R)}, c_j^{(G)}, c_j^{(B)}$, где $c_i^{(R)} \in R$, $c_j^{(R)} \in R$, $c_i^{(G)} \in G$, $c_j^{(G)} \in G$, $c_i^{(B)} \in B$, $c_j^{(B)} \in B$.

Для блоков $c_i^{(R)}, c_i^{(G)}, c_i^{(B)}$ и $c_j^{(R)}, c_j^{(G)}, c_j^{(B)}$ вычисляем нормальное сингулярное разложение

$$c_i^{(R)} = U_i^{(R)}\Sigma_i^{(R)}\left(V_i^{(R)}\right)^T,\ c_j^{(R)} = U_j^{(R)}\Sigma_j^{(R)}\left(V_j^{(R)}\right)^T,$$

$$c_i^{(G)} = U_i^{(G)}\Sigma_i^{(G)}\left(V_i^{(G)}\right)^T,\ c_j^{(G)} = U_j^{(G)}\Sigma_j^{(G)}\left(V_j^{(G)}\right)^T,$$

$$c_i^{(B)} = U_i^{(B)}\Sigma_i^{(B)}\left(V_i^{(B)}\right)^T,\ c_j^{(B)} = U_j^{(B)}\Sigma_j^{(B)}\left(V_j^{(B)}\right)^T,$$

где

$$\Sigma_i^{(R)} = diag\left(\sigma_1^{(R)}, \sigma_2^{(R)}, ..., \sigma_p^{(R)}\right),\ \Sigma_j^{(R)} = diag\left(\overline{\sigma}_1^{(R)}, \overline{\sigma}_2^{(R)}, ..., \overline{\sigma}_p^{(R)}\right),$$

$$\Sigma_i^{(G)} = diag\left(\sigma_1^{(G)}, \sigma_2^{(G)}, ..., \sigma_p^{(G)}\right),\ \Sigma_j^{(G)} = diag\left(\overline{\sigma}_1^{(G)}, \overline{\sigma}_2^{(G)}, ..., \overline{\sigma}_p^{(G)}\right),$$

$$\Sigma_i^{(B)} = diag\left(\sigma_1^{(B)}, \sigma_2^{(B)}, ..., \sigma_p^{(B)}\right),\ \Sigma_j^{(B)} = diag\left(\overline{\sigma}_1^{(B)}, \overline{\sigma}_2^{(B)}, ..., \overline{\sigma}_p^{(B)}\right).$$

2.4.2 Получаем линейную аппроксимацию по полученным сингулярным числам (кроме первого) и вычисляем коэффициенты:

$$coef_1^{(R)} = \begin{cases} \dfrac{a^{(R)}}{\overline{a}^{(R)}}, a^{(R)} > \overline{a}^{(R)} \\ \dfrac{\overline{a}^{(R)}}{a^{(R)}}, \overline{a}^{(R)} > a^{(R)} \end{cases} \text{ и } coef_2^{(R)} = \begin{cases} \dfrac{b^{(R)}}{\overline{b}^{(R)}}, a^{(R)} > \overline{a}^{(R)} \\ \dfrac{\overline{b}^{(R)}}{b^{(R)}}, \overline{a}^{(R)} > a^{(R)} \end{cases},$$

$$coef_1^{(G)} = \begin{cases} \dfrac{a^{(G)}}{\overline{a}^{(G)}}, a^{(G)} > \overline{a}^{(G)} \\ \dfrac{\overline{a}^{(G)}}{a^{(G)}}, \overline{a}^{(G)} > a^{(G)} \end{cases} \text{ и } coef_2^{(G)} = \begin{cases} \dfrac{b^{(G)}}{\overline{b}^{(G)}}, a^{(G)} > \overline{a}^{(G)} \\ \dfrac{\overline{b}^{(G)}}{b^{(G)}}, \overline{a}^{(G)} > a^{(G)} \end{cases},$$

$$coef_1^{(B)} = \begin{cases} \dfrac{a^{(B)}}{\overline{a}^{(B)}}, a^{(B)} > \overline{a}^{(B)} \\ \dfrac{\overline{a}^{(B)}}{a^{(B)}}, \overline{a}^{(B)} > a^{(B)} \end{cases} \text{ и } coef_2^{(B)} = \begin{cases} \dfrac{b^{(B)}}{\overline{b}^{(B)}}, a^{(B)} > \overline{a}^{(B)} \\ \dfrac{\overline{b}^{(B)}}{b^{(B)}}, \overline{a}^{(B)} > a^{(B)} \end{cases}.$$

2.4.3 Если $P_1 \le coef_1^{(R)} \le P_2$ & $P_1 \le coef_2^{(R)} \le P_2$ & $P_1 \le coef_1^{(G)} \le P_2$ & $P_1 \le coef_2^{(G)} \le P_2$ & $P_1 \le coef_1^{(B)} \le P_2$ & $P_1 \le coef_2^{(B)} \le P_2$, то

- Если координаты $< x_i, y_i >$ были отнесены к первому объекту, то

$$fbw_r = \begin{cases} 1, (a^{(R)} \ge \overline{a}^{(R)}) \,\&\, (a^{(G)} \ge \overline{a}^{(G)}) \,\&\, (a^{(B)} \ge \overline{a}^{(B)}) \\ 0, (\overline{a}^{(R)} > a^{(R)}) \,\&\, (\overline{a}^{(G)} > a^{(G)}) \,\&\, (\overline{a}^{(B)} > a^{(B)}) \end{cases} \text{ и}$$

$$sbw_r = \begin{cases} 0, (a^{(R)} \ge \overline{a}^{(R)}) \,\&\, (a^{(G)} \ge \overline{a}^{(G)}) \,\&\, (a^{(B)} \ge \overline{a}^{(B)}) \\ 1, (\overline{a}^{(R)} > a^{(R)}) \,\&\, (\overline{a}^{(G)} > a^{(G)}) \,\&\, (\overline{a}^{(B)} > a^{(B)}) \end{cases}.$$

- Если координаты $< x_i, y_i >$ были отнесены ко второму объекту, то

$$sbw_r = \begin{cases} 1, (a^{(R)} \geq \overline{a}^{(R)}) \,\&\, (a^{(G)} \geq \overline{a}^{(G)}) \,\&\, (a^{(B)} \geq \overline{a}^{(B)}) \\ 0, (\overline{a}^{(R)} > a^{(R)}) \,\&\, (\overline{a}^{(G)} > a^{(G)}) \,\&\, (\overline{a}^{(B)} > a^{(B)}) \end{cases} \text{ и}$$

$$fbw_r = \begin{cases} 0, (a^{(R)} \geq \overline{a}^{(R)}) \,\&\, (a^{(G)} \geq \overline{a}^{(G)}) \,\&\, (a^{(B)} \geq \overline{a}^{(B)}) \\ 1, (\overline{a}^{(R)} > a^{(R)}) \,\&\, (\overline{a}^{(G)} > a^{(G)}) \,\&\, (\overline{a}^{(B)} > a^{(B)}) \end{cases},$$

где $FBW = \{fbw_1, \ldots fbw_r, \ldots\}$, $SBW = \{sbw_1, \ldots sbw_r, \ldots\}$.

2.5 Пересчитываем новые центры объектов, используя существующие и добавленные блоки.

Имеем

$$F = \{first_1, \ldots first_q\}, \text{ где } first_{ii} = (first^{\,x}_{ii}, first^{\,y}_{ii}) \text{ и}$$

$$S = \{second_1, \ldots second_z\}, \text{ где } second_{jj} = (second^{\,x}_{jj}, second^{\,y}_{jj}).$$

Тогда новые центры

$$center_1 = (center_1^x, center_1^y),$$

$$\text{где } center_1^x = \frac{1}{q}\sum_{ii=1}^{q} first^{\,x}_{ii} \text{ и } center_1^y = \frac{1}{q}\sum_{ii=1}^{q} first^{\,y}_{ii},$$

$$center_2 = (center_2^x, center_2^y),$$

$$\text{где } center_2^x = \frac{1}{z}\sum_{jj=1}^{z} second^{\,x}_{jj} \text{ и } center_2^y = \frac{1}{z}\sum_{jj=1}^{z} second^{\,y}_{jj}.$$

3. Вычисляем количество нулей и единиц в $FBW = \{fbw_1, \ldots fbw_t\}$, $SBW = \{sbw_1, \ldots sbw_p\}$.

Пусть в FBW количество единиц $f^{(1)}$, а нулей $f^{(0)}$.

Пусть в SBW количество единиц $s^{(1)}$, а нулей $s^{(0)}$.

4. Если $f^{(1)} > f^{(0)}$, то блоки с координатами из F будем показывать белым цветом (оригинал), иначе, если $f^{(1)} < f^{(0)}$, то блоки с координатами из F будем показывать чёрным цветом (клон).

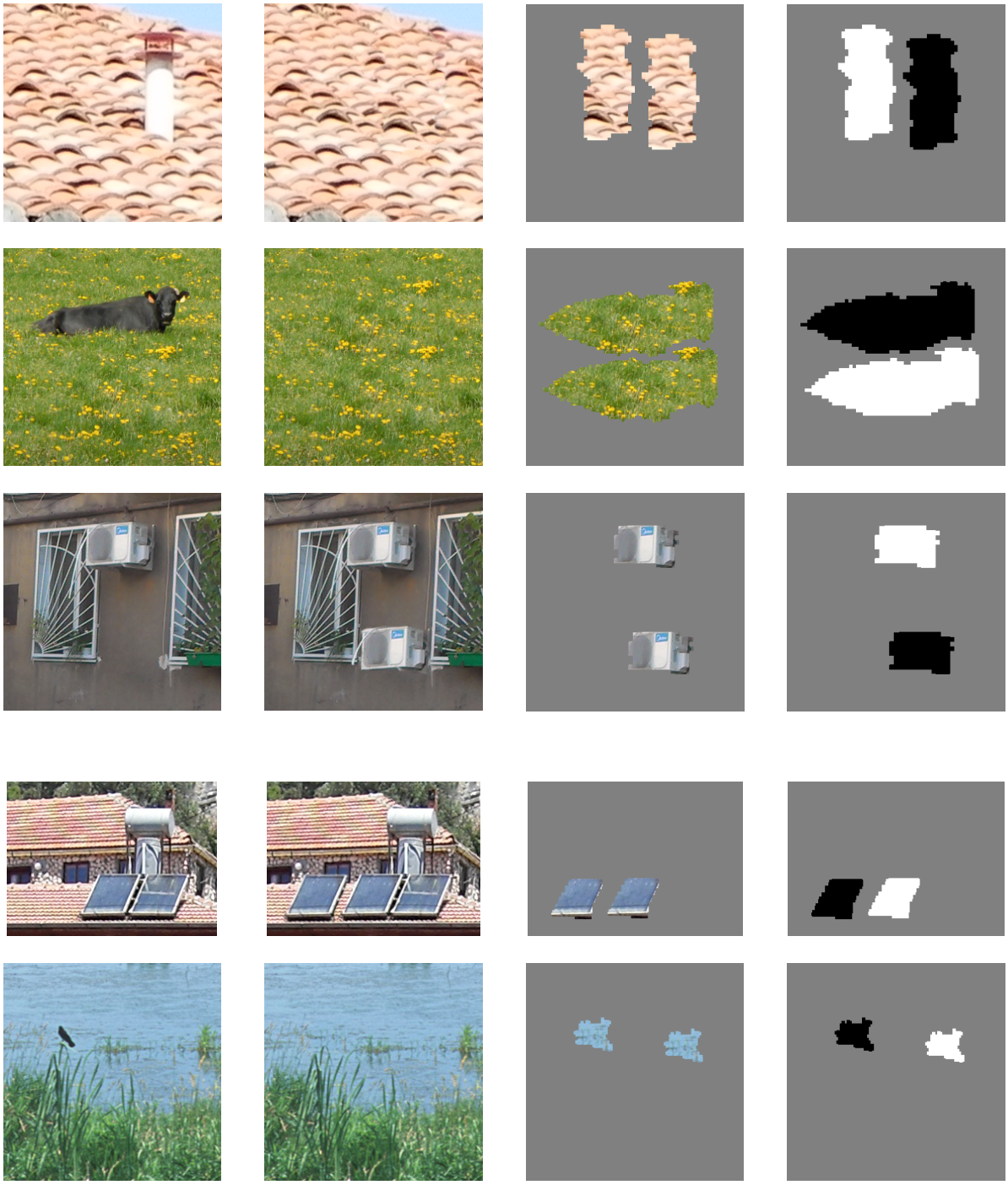
Если $s^{(1)} > s^{(0)}$, то блоки с координатами из S будем показывать белым цветом (оригинал), иначе, если $s^{(1)} < s^{(0)}$, то блоки с координатами из S будем показывать чёрным цветом (клон).

Если $f^{(1)} = f^{(0)}$ и $s^{(1)} = s^{(0)}$, то имеем неопределенность идентификации.

Результаты исследований

В исследованиях использовались ЦИ, полученные различными цифровыми аппаратами. Создание клонированных областей осуществлялась в программе Adobe Photoshop CS6. Фальсифицированные ЦИ не сжимались. На рисунке 3 показаны

некоторые из результатов исследований; оригинальная область обозначена белым цветом, фальсифицированная – чёрным.



а **б** **в** **г**

Рис. 3. Результаты исследований: а – оригинальные ЦИ, б – фальсифицированные, в – результат выявления клонированных областей, г – результат идентификации оригинала и клона

Выводы

В работе впервые разработан теоретически обоснованный метод локализации и идентификации оригинальной и клонированной областей изображения. В ходе работы разработан математический базис для метода выявления качественных отличий оригинальной области от клонированной. Метод, построенный на основе разработанного базиса, является эффективным не только при выявлении, но и идентификации клонированных областей, что подтверждено результатами представительного вычислительного эксперимента.

Список литературы

1. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А.Хорошко. — К.: ГУИКТ, 2009. — 251 с..
2. Лебедева, Е.Ю. Обнаружение клонированных участков изображений в задачах выявления фальсификации / Е.Ю. Лебедева // XII міжнародна науково–практична конференція «Современные информационные и электронные технологии». — 2011. С. 175.
3. Лебедева, Е.Ю. Исследование метрик используемых при обнаружении клонированных участков изображений в задачах выявления фальсификации / Е.Ю. Лебедева, Ю.Ф. Лебедев // Вісник національного технічного університету «ХПІ». —2011. — №35. — С.25 – 31.

МЕТОД ЛОКАЛІЗАЦІЇ Й ІДЕНТИФІКАЦІЇ ОРИГІНАЛЬНОЇ Й КЛОНОВАНОЇ ОБЛАСТЕЙ ЗОБРАЖЕННЯ

О. Ю. Лєбєдєва

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: whiteswanhelena@gmail.com

У роботі розроблений теоретично обґрунтований метод локалізації й ідентифікації оригінальної й клонованої областей зображення. За результатами експериментів і спостережень виявлені якісні відмінності оригінальної області від клонованої. Розроблений математичний базис для формального виявлення запропонованих якісних відмінностей.
Ключові слова: фальсифікація зображення, виявлення фальсифікації, клонування, локалізація області.

LOCALIZATION AND IDENTIFICATION METHOD OF ORIGINAL AND CLONED IMAGE AREAS

H. J. Lebedeva

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: whiteswanhelena@gmail.com

A scientifically grounded method to localize and identify both original and cloned image areas was proposed. Qualitative differences between original area and cloned area were found based on the results of experiments and observations. The mathematical basis for formal identification of proposed qualitative differences was developed.
Keywords: image falsification, identification of falsification, cloning, area localization

УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 85-92

ЧИСЕЛЬНИЙ МЕТОД РЕАЛІЗАЦІЇ МАТЕМАТИЧНИХ МОДЕЛЕЙ ПРОЦЕСІВ ПЕРВИННОЇ ПЕРЕРОБКИ СИРИХ ВУГЛЕВОДНІВ

Ю. В. Григоренко

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: ygrygorenko@lukoil.com

Виконано узагальнення математичного опису процесів первинної переробки сирих вуглеводнів (ППСВ) у вигляді нелінійних нестаціонарних диференційних рівнянь у часткових похідних, що дає змогу застосувати принцип типізації при подальшому математичному моделюванні зазначених процесів. Запропоновано та обґрунтовано ефективний чисельний метод реалізації математичних моделей (ММ) процесів ППСВ, заснований на ітераційній процедурі розв'язання нелінійних нестаціонарних дискретних ММ досліджуваних процесів.

Ключові слова: математична модель, ітераційний процес, різницева схема, параметрична нелінійність, збіжність ітераційної процедури, стисліть відображення

Вступ

Розв'язок задачі математичного моделювання, в тому числі при дослідженні процесів переробки сирих вуглеводнів, в значній мірі визначається обраною ММ. Адекватно обрана ММ забезпечує достовірність результатів математичного моделювання. Крім того, на результати математичного моделювання (зокрема, його точність) впливають чисельні методи, якими реалізується обрана ММ. Тому сукупний вибір ММ та чисельного методу є важливим етапом математичного моделювання, що визначає ефективність процесу дослідження.

В роботі [1] запропоновано ММ процесів (та апаратів) ППСВ у вигляді диференційних рівнянь (систем диференційних рівнянь) у часткових похідних (ДРЧП), отриманих на основі фундаментальних законів матеріального балансу та збереження (енергії, імпульсу, тощо). Адекватність запропонованої сукупності ММ визначається тим, що вони найбільш повно відбивають характер фізико-хімічних явищ, притаманних досліджуваному класу процесів. Особливістю запропонованих ММ є те, що вони мають нелінійний та нестаціонарний характер, що визначається відповідною варіативністю параметрів сирих вуглеводнів. Наприклад, густина сирої нафти в значній мірі залежить від температури, що призводить до нелінійності ММ, а зміна в часі функції стану сировини в ході технологічного процесу (наприклад, тієї ж температури сирої нафти), зумовлює не стаціонарність ММ.

Постановка задачі та мети дослідження

Однак слід зазначити, що існуючі чисельні методи [2, 3] не забезпечують у повній мірі ефективну реалізацію нелінійних нестаціонарних ММ процесів ППСВ.

Метою запропонованої роботи є розробка ефективного чисельного методу реалізації ММ процесів ППСВ, який передбачає застосування принципу типізації ММ.

Основна частина

Запропоновані в роботі [1] ММ можна представити у вигляді узагальненої моделі, а саме:

$$\frac{\partial\overline{\Phi}_i\left(r_j,z,t\right)}{\partial t}=$$

$$=f_i\left[\overline{\Phi}_i\left(r_j,z,t\right),\frac{\partial\overline{\Phi}_i\left(r_j,z,t\right)}{\partial z},\frac{\partial^2\overline{\Phi}_i\left(r_j,z,t\right)}{\partial r_j^2},\frac{\partial\overline{\Phi}_i\left(r_j,z,t\right)}{\partial r_j},\overline{U}_g\left(r_j,z,t\right)\right]+D_i\left(\overline{\Phi}_i,r_j,z,t\right), \tag{1}$$

$$\forall i=1,...,k;\ \forall j=1,...,N;\ \forall\left(r_j,z\right)\in\Omega;\ \forall t\in\left(0,t_k\right),$$

$$\overline{\Phi}=\left[\Phi_1,\Phi_2,...,\Phi_k\right]^T\ \ (T\ \text{— знак транспонування})$$

з урахуванням початкових

$$\overline{\Phi}_i\left(r_j,z,0\right)=\overline{\Phi}_{i_0}\left(r_j,z\right),\ \forall i=1,...,k;\ \forall j=1,...,N;\ \ \forall\left(r_j,z\right)\in\Omega \tag{2}$$

та граничних умов наступних типів:

- граничних умов першого роду, ГУ-1 (типу Діріхле)

$$\overline{\Phi}_i\left(r_j,z,t\right)\Big|_{\substack{r_i=0\\r_i=r_{i\max}\\z=0\\z=z_{\max}}}=\varphi_i\left[P_i\left(r_j,z,t\right)\right],\ \forall i=1,...,k;\ \forall j=1,...,N;\ \ \forall\left(r_j,z\right)\in\Omega \tag{3}$$

- граничних умов третього роду, ГУ-3

$$\left.\frac{\partial\overline{\Phi}_i\left(r_j,z,t\right)}{\partial r_i}\right|_{\substack{r_i=0\\r_i=r_{i\max}}}=\lambda_i\left[\overline{\Phi}\left(r_j,z,t\right),P_i\left(r_j,z,t\right)\right], \tag{4}$$

$$\forall i=1,...,k;\ \forall j=1,...,N;\ \ \forall\left(r_j,z\right)\in\Omega,$$

де $\overline{\Phi}_i\left(r_j,z,t\right)$ — безперервні функції стану, що залежать від часової $t\in\left(0,t_k\right)$ та просторових $\forall\left(r_j,z\right)\in\Omega$ координат (координати r_j,z змінюються у відкритій (циліндричній) множині $\Omega\in R^{M_k}$ із гладкою границею $\partial\Omega$; R^{M_k} — евклідовий простір дійсних чисел розмірності M_k); функції стану $\overline{\Phi}_i\left(r_j,z,t\right)$ визначаються розв'язком системи (1) — (4), що (за визначенням) існує і є єдиним; $\overline{U}_g\left(r_j,z,t\right),\ g=1,...,k^*$ — функції розподіленого управління, що належать гільбертовому простору $\overline{U}_{g_o}$ на R^{M_k}.

Змінні стану $\overline{\Phi}_i\left(r_j,z,t\right)$ та управління $\overline{U}_g\left(r_j,z,t\right)$ визначено у відкритих гільбертових просторах із границями відповідно $\Omega_{\Phi_i},\Omega_{U_r}\ \forall i=1,...,k;\ \forall r=1,...,k^*$.

Функції $f_i[\cdot]$ та $y_i[\cdot]$ — безперервні лінійні або нелінійні функції; $D_i\left(\overline{\Phi}_i,r_j,z,t\right)=D_i\left\{r_i,z,t,\Phi_1\left(r_j,z,t\right),\Phi_2\left(r_j,z,t\right),...,\Phi_k\left(r_j,z,t\right)\right\}$ — лінійні або нелінійні функції, що характеризують дію зовнішніх збуджуючих впливів; $P_i\left(r_j,z,t\right),\ \forall i=1,...,k;\ \forall j=1,...,N;\ \forall\left(r_j,z\right)\in\Omega$ — задані функції на границі $\partial\Omega$ області, які можуть виступати в якості граничних управляючих впливів; $\lambda_i,\ \forall i=1,...,k$ —

параметр, який характеризує енергетичні властивості елементів об'єкта (технологічного апарата); N — число поверхонь теплообміну (зокрема, ректифікаційних тарілок).

Змінні стану $\overline{\Phi}_i\left(r_j,z,t\right)$ та управління $\overline{U}_g\left(r_j,z,t\right)$ можуть визначати різні фізичні (зокрема, температуру, витрату), або геометричні (наприклад, рівень) величини, а також відхилення цих величин від стаціонарних значень; параметри λ_i визначають відповідно: коефіцієнт теплопровідності, коефіцієнт теплопередачі, тощо.

Таким чином, застосування ММ у вигляді (1) — (4) дасть змогу у подальшому втілити принцип типізації — тобто орієнтації на певний клас ММ — при розробці чисельного метода реалізації ММ часткових випадків процесів (апаратів) ППСВ.

Представимо (з метою конкретності подальших математичних викладок) узагальнену ММ (1) — (4) в наступному вигляді:

$$\frac{\partial\overline{\Phi}_i\left(r_j,z,t\right)}{\partial t}=\sum_{i=1}^{3}A_i\left(\overline{\Phi}_i,r_j,z,t\right)\frac{\partial^2\overline{\Phi}_i\left(r_j,z,t\right)}{\partial r_j^2}+\sum_{i=1}^{3}B_i\left(\overline{\Phi}_i,r_j,z,t\right)\frac{\partial\overline{\Phi}_i\left(r_j,z,t\right)}{\partial r_j}+$$

$$+\sum_{i=1}^{3}B_i\left(\overline{\Phi}_i,r_j,z,t\right)\frac{\partial\overline{\Phi}_i\left(r_j,z,t\right)}{\partial z}+C_i\left(\overline{\Phi}_i,r_j,z,t\right)\overline{\Phi}_i\left(r_j,z,t\right)+ \tag{5}$$

$$+D_i\left(\overline{\Phi}_i,r_j,z,t\right)U_i\left(r_j,z,t\right)+E_i\left(\overline{\Phi}_i,r_j,z,t\right)F_i\left(r_j,z,t\right),\ \forall j=\overline{1,N};$$

$$\overline{g}=\{r_1,r_2,r_3,z\},\ \overline{g}\in\Omega\subset R^3;\ \overline{\Phi}_i=\left[\Phi_{1_i},\Phi_{2_i},...,\Phi_{k_i}\right],\ t\in\left(0,t_k\right),\ Q=\Omega\times\left(0,t_k\right);$$

$$\overline{U}\left(r_j,z,t\right)=\left[U_1,U_2,...,U_{k_1}\right]^T,\ \overline{F}\left(r_j,z,t\right)=\left[F_1,F_2,..,F_k\right]^T,\ k_1\le k; \tag{6}$$

$$\Phi_i\left(0,\overline{g}\right)=\Phi_{0_i}\left(\overline{g}\right),\ \overline{g}\in\Omega;$$

$$\lambda_j\left(0,0,t\right)\frac{\partial\Phi_i\left(0,0,t\right)}{\partial r_j}+K_j\left(t\right)\Phi_i\left(0,0,t\right)=\Psi_j\left(t\right),\ \forall j=\overline{1,N} \tag{7}$$

Перетворення початкової диференційної задачі (5) — (7) в різницеву може бути виконано за допомогою різноманітних різницевих схем [4, 5], що зумовлює також отримання цілої низки апроксимуючих дискретних ММ з різними якісними характеристиками. Аналіз вказаної літератури показує, що з точки зору структурної повноти розгляду можливих варіантів різницевих схем, для ДРЧП гіперболічного та гіперболо-параболічного типу доцільно використовувати шеститочковий шаблон [4]. Він дозволяє побудувати схеми двошарові за часом та тришарові за простором, тобто дає змогу розв'язувати задачі: стаціонарні та нестаціонарні, а також одно- (лінійні), дво- (пласкі) та тривимірні (об'ємні).

Введемо наступні сітки:

$$\overline{\omega}_{\Delta g}=\{\overline{g}_n=l\,\Delta\overline{g},\ l=0,1,...,L\};\ \omega_{\Delta t}=\{t_m=m\,\Delta t,\ m=0,1,...,M\};$$

$$\overline{\omega}_{\Delta g\Delta t}=\overline{\omega}_{\Delta g}\times\omega_{\Delta t}=\{(l\,\Delta g,m\,\Delta t),\ l=0,1,...,L,\ m=0,1,...,M\},$$

з кроками по просторових координатах $\Delta\overline{g}=\left\{\Delta r_j,\Delta z\right\}$; $\Delta r_j=r_{\max}/L_r$; $j=\overline{1,N}$; $\Delta z=z_{\max}/L_z$ (для рівномірних сіток $\Delta r=\Delta z$) та по часовій координаті $\Delta t=t_k/M$.

Позначимо через Φ_l^m значення сіткової функції у вузлі $(\bar{g}_l, t_m)$, визначеної на $\bar{\omega}_{\Delta\bar{g}\Delta t}$. Тоді, заміняючи безперервні похідні в рівняннях системи (5) на відповідні різницеві похідні, одержимо:

$$\Phi_{l_i}^{m+1} - \Phi_{l_i}^m = \frac{A_i\{\cdot\}}{\Delta r_j^{\,2}}\left[\sigma\left(\Phi_{(l+1)_i}^{m+1} - 2\Phi_{l_i}^{m+1} + \Phi_{(l-1)_i}^{m+1} + (1-\sigma)\left(\Phi_{(l+1)_i}^{m} - 2\Phi_{l_i}^{m} + \Phi_{(l-1)_i}^{m}\right)\right)\right] +$$

$$+ \frac{B_i\{\cdot\}}{(\Delta r_j + \Delta z)}\left[\Phi_{(l-1)_i}^{m+1} - 4\Phi_{l_i}^{m+1} + 3\Phi_{(l+1)_i}^{m+1} + \Phi_{l_i+1}^{m} - \Phi_{(l-1)_i}^{m}\right] + C_i\{\cdot\}\Phi_{l_i}^m + D_i\{\cdot\}U_{l_i}^m + E_i\{\cdot\}F_{l_i}^m \qquad (8)$$

$$j = \overline{1, N}$$

де $i = 1, 2, ..., k$; σ — довільний речовинний параметр $(0 \le \sigma \le 1)$. Як різницевий аналог граничних умов (7) використаємо наступні вирази:

$$\lambda_j^m \frac{\Phi_{l_i}^m - \Phi_{l_i-1}^m}{\Delta r_j} - K_j^m \Phi_{n_i}^m = \Psi_j^m;\ r_j = 0,\ t \ge 0,\ i = 1, 2, ..., k;\ j = \overline{1, N}. \qquad (9)$$

Початкові умови мають вигляд:

$$\Phi_i(0, l) = \Phi_i^0(l). \qquad (10)$$

Схема (8) описує однопараметричне (відносно σ) сімейство різницевих схем і, у відповідності до загально прийнятої термінології [5], носить назву схеми з вагами. Від вибору параметра σ залежить стійкість та точність схеми (8) [4, 5].

Розглянемо схеми, які відповідають частковим значенням σ. При $\sigma = 0$ та заміні часткових похідних першого порядку по простору на центральну різницю, тобто

$$\frac{\partial \Phi_i(r_j, z, t)}{\partial r_j} = \frac{\Phi_{(l+1)_i}^m - \Phi_{(l-1)_i}^m}{2\Delta r_j},\ j = \overline{1, N};$$

$$\frac{\partial \Phi_i(r_j, z, t)}{\partial z} = \frac{\Phi_{(l+1)_i}^m - \Phi_{(l-1)_i}^m}{2\Delta z};$$

отримуємо чотириточкову схему (вироджений випадок для шеститочкового шаблону):

$$\frac{\Phi_{l_i}^{m+1} - \Phi_{l_i}^m}{\Delta t} = A_i\{\cdot\}\frac{\Phi_{(l+1)_i}^m - 2\Phi_{l_i}^m + \Phi_{(l-1)_i}^m}{\Delta r_j^2} + B_i\{\cdot\}\frac{\Phi_{(l+1)_i}^m - \Phi_{(l-1)_i}^m}{(r_j + \Delta z)} +$$

$$+ C\{\cdot\}\Phi_{l_i}^m + D_i\{\cdot\}U_l^m + E_i\{\cdot\}F_{l_i}^m,\ i = 1, 2, ..., k;\ j = \overline{1, N}. \qquad (11)$$

Дана схема є явною. Значення сіткової функції Φ_l^{m+1} в кожній точці шару $t = (m+1)\Delta t$ (нового шару) виражається через відомі значення $\Phi_{(l+1)_i}^m, \Phi_{l_i}^m, \Phi_{(l-1)_i}^m$ на шарі $t = m\Delta t$ (старому шарі). Оскільки при $t = 0$ задана початкова умова (10), то схема (11) дозволяє послідовно визначити значення сіткової функції на будь-якому часовому шарі. Якщо $\sigma \ne 0$, то схема (8) буде містити як явні, так і неявні члени (так звана явно-неявна

схема). При $\sigma = 1$ та заміні часткової похідної першого порядку по простору наступним виразом

$$\frac{\partial \Phi_i(r_j, z, t)}{\partial r_j} = \frac{\Phi^{m+1}_{(l+1)_i} - \Phi^{m+1}_{(l-1)}}{2\Delta r_j},\ j = \overline{1, N}; \quad \frac{\partial \Phi_i(r_j, z, t)}{\partial z} = \frac{\Phi^{m+1}_{(l+1)_i} - \Phi^{m+1}_{(l-1)_i}}{2\Delta z}$$

отримаємо чисто неявну схему:

$$\frac{\Phi^{m+1}_{l_i} - \Phi^{m}_{l_i}}{\Delta t} = A_i\{\cdot\}\frac{\Phi^{m+1}_{(l+1)_i} - 2\Phi^{m+1}_{l_i} + \Phi^{m+1}_{(l-1)_i}}{\Delta r_j^2} + B_i\{\cdot\}\frac{\Phi^{m+1}_{(l+1)_i} - \Phi^{m+1}_{(l-1)_i}}{(\Delta r_{j+}\Delta z)} + \\ + C_i\{\cdot\}\Phi^m_l + D_i\{\cdot\}U^m_l + E_i\{\cdot\}F^m_{l_i},\ i = 1,2,...,k;\ j = \overline{1, N}. \tag{12}$$

Рівняння (10) може бути використане у всій просторовій області $0 < r_j < r_{\max};\ j = \overline{1, N},\ 0 < z < z_{\max}$, за винятком граничних точок: $r_j = 0$, $r_j = z_{\max}$ та $z = 0$, $z = z_{\max}$. Для зазначених точок сіткова функція визначається із граничних умов (9).

Для випадку $\sigma = 0.5$ одержимо шеститочкову симетричну щодо явних членів схему:

$$\frac{\Phi^{m+1}_{l_i} - \Phi^{m}_{l_i}}{\Delta t} = A_i\{\cdot\}\left[\frac{\Phi^{m+1}_{(l+1)_i} - 2\Phi^{m+1}_{l_i} + \Phi^{m+1}_{(l-1)_i}}{2\Delta r_j^2} + \frac{\Phi^{m}_{(l+1)_i} - 2\Phi^{m}_{l_i} + \Phi^{m}_{(l-1)_i}}{2\Delta r_j^2}\right] + \\ + \frac{B_i\{\cdot\}}{2(\Delta r_j + \Delta z)}\left[\Phi^{m+1}_{(l-1)_i} - 4\Phi^{m+1}_{l_i} + 3\Phi^{m+1}_{(l+1)_i} + \Phi^{m}_{(l+1)_i} - \Phi^{m}_{(l-1)_i}\right] + \\ + C_i\{\cdot\}\Phi^m_{l_i} + D_i\{\cdot\}U^m_{l_i} + E_i\{\cdot\}F^m_{l_i},\ i = 1,2,...,k;\ j = \overline{1, N}. \tag{13}$$

Схема (13) відома в літературі [4, 5] як схема Кранка-Ніколсона. Для неї справедливо зауваження, зроблене для схеми (12).

Таким чином схеми (11), (12) та (13) являють собою кінцевовимірні (дискретні) аналоги (дискретні ММ) узагальненої математичної моделі основних технологічних апаратів процесів ППСВ і вони суть складають основу програмно-алгоритмічних інструментальних засобів математичного моделювання зазначених процесів.

Спираючись на роботи [4, 5] легко показати, що явна схема (11) стійка лише за умови $\left[\Delta t/(\Delta r_j\ \Delta z)\right] \le 1/2$, $j = \overline{1, N}$ яка зв'язує кроки $\Delta r_j, \Delta z;\ j = \overline{1, N}$ та Δt. При цьому схеми (12) і (13), для яких $\sigma \ge 0.5$, стійкі для будь-яких значень $\Delta r_j, \Delta z;\ j = \overline{1, N}$ та Δt. Крім того, виконавши розкладання в ряд Тейлора для задачі (8) одержимо, що при $\sigma = 0$ схема апроксимує вихідну задачу з точністю $e = 0[(\Delta t)] + 0[(\Delta z)^2]$, а при $\sigma \ge 0.5$ похибка відповідно складає $e = 0[(\Delta t)^2] + 0[(\Delta z)^2]$.

Різницеві схеми (11), (12) та (13) отримано з припущення про нелінійний та нестаціонарний характер матриць коефіцієнтів A_i — E_i узагальненої ММ виду (1) — (4). Таке припущення досить суттєво і виникає з тієї обставини, що в технологічному циклі за досить нетривалий час (навіть у межах однієї зміни) у сирих вуглеводнів, які надходять на переробку, можуть значно змінюватися такі фізико-хімічні параметри як густина, газованість, температура, тощо. Це викликано тим, що сирі вуглеводні можуть подаватися на переробку, наприклад, безпосередньо із залізничних цистерн або зі

сховищ і, таким чином, перехід між сировиною з різними параметрами (наприклад, так звані «легкі» та «важкі» нафти), в свою чергу, може здійснюватися за короткий (в технологічному розумінні) час. Покажемо можливість врахування параметричної нелінійності різницевих схем (11), (12) та (13). Для конкретності подальших розмірковувань розглянемо схему (13).

Використовуючи матричну форму запису, представимо рівняння схеми (13) у наступному вигляді:

$$\left[\Phi_{l_i}^{m+1}-\Phi_{l_i}^{m}\right]=\Delta t\left[\left(A_i+\frac{B_i}{2\left(\Delta r_j+\Delta z\right)}\right)\nabla^2\Phi_{l_i}\right]^{m+1}+$$
$$+\Delta t\left[\left(A_i+\frac{B_i}{2\left(\Delta r_j+\Delta z\right)}+C_i\right)\nabla\Phi_{l_i}\right]^{m}=\left[D_iU^m+E_iF^m\right]. \tag{14}$$

Виходячи з посилання про те, що відображення $G:\phi\to\phi$ (де ϕ — банановий простір, а відображення g задає перетворення за схемою (13)) — стисле, можна стверджувати, що для будь-яких $\Phi_{l_i}^1$, $\Phi_{l_i}^2\in\phi$ виконується нерівність [6]

$$\left\|G\left(\Phi_{l_i}^1\right)-G\left(\Phi_{l_i}^2\right)\right\|\le q\left\|\Phi_{l_i}^1-\Phi_{l_i}^0\right\|;\ q\le 1. \tag{15}$$

Далі скористаємося методом простої ітерації [4 — 6]. При цьому, якщо відображення $G:\phi\to\phi$ — стисле, то (14) має єдиний розв'язок $\Phi_{l_i}^*$:

$$\left\|\Phi_{l_i}^*-\Phi_{l_i}^{\nu}\right\|\le\frac{q^{\nu}}{1-q}\left\|\Phi_{l_i}^1-\Phi_{l_i}^0\right\|, \tag{16}$$

де ν — номер ітерації.

Тоді можна стверджувати, що у досить малій околиці розв'язку $\Phi_{l_i}^*$ рівняння (14) для наближень методом простої ітерації має вигляд

$$\Phi_{l_i}^{\nu+1}-\Phi_{l_i}^{\nu}=T\left(\Phi_{l_i}^{\nu}\right)-G\left(\Phi_{l_i}^*\right). \tag{17}$$

Вважаючи, що характер нелінійності однаковий для всіх вузлів області дискретизації Ω, ітераційний процес (17) завершується за умови виконання критерію

$$\max_{L_r,L_z}\left|\frac{\Phi_{l_i}^{\nu+1}-\Phi_{l_i}^{\nu}}{\Phi_{l_i}^{\nu+1}}\right|\le\delta_{l_i}, \tag{18}$$

де δ_{l_i} — задана точність розв'язку.

Відмінність запропонованого методу полягає в тому, що застосування при чисельній реалізації узагальненої ММ (вирази виду (1) — (4)) схеми Кранка — Ніколсона (вираз (13)) забезпечує на першому кроці розв'язання першу ітерацію ітераційного процесу (вираз (17)).

Конструктивність та ефективність запропонованого методу підтверджено розв'язанням прикладних задач з моделювання процесу електро-(термо)знесолення та зневоднення сирої нафти. Зокрема, моделювався динамічний стан термодегідраторів,

призначених для відокремлення сирої нафти від мінеральних солей та пластової води. Пласка нелінійна та нестаціонарна задача для дискретної області у 192 вузли (сітка розміром 16×12) і часу моделювання 6.5год. (з кроком дискретизації $\Delta t = 90$с) потребувала на розв'язання 218с машинного часу (застосовувався процесор з тактовою частотою 1.5ГГц). Збіжність ітераційного процесу (17) досягалась не більше, ніж за 7 ітерацій і не залежала від зміни вихідних даних, які визначали значення коефіцієнтів узагальненої ММ виду (1) — (4).

Висновок

Таким чином, розроблено метод реалізації узагальненої ММ процесів ППСВ, який зводиться до дискретизації неперервної узагальненої ММ за схемою з вагами та подальшого розв'язання отриманої системи нелінійних дискретних рівнянь за процедурою простої ітерації.

Список літератури

1. Polozhaenko, S. Research of solvability of task of authentication of water-oil mixtures on the parameters of tuning of mathematical model / Polozhaenko S. A., Grigorenko Yu. V. // Інформатика та математичні методи в моделюванні. — 2012. — Т. 2. — №3. — С. 199 — 210.
2. Рей, У. Методы управления технологическими процессами. — М.: Мир, 1983. — 367 с.
3. Мацевитый, Ю. М. Моделирование нелинейных процессов в распределенных системах / Ю. М. Мацевитый, В. Е. Прокофьев. — К.: Наукова думка, 1985. — 302 с.
4. Самарский, А. А. Введение в теорию разностных схем. — М. Наука, 1971. — 552 с.
5. Самарский, А. А. Методы решения сеточных уравнений / А. А. Самарский, Е. С. Николаев. — М.: Наука, 1988. — 591 с.
6. Краскевич, В. Е. Численные методы в инженерных расчетах / В. Е. Краскевич, Л. Х. Зеленский, В. И. Гречко. — К.: Вища школа, 1986. — 263 с.

ЧИСЛЕННЫЙ МЕТОД РЕАЛИЗАЦИИ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ПРОЦЕССОВ ПЕРВИЧНОЙ ПЕРЕРАБОТКИ СЫРЫХ УГЛЕВОДОРОДОВ

Ю. В. Григоренко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: ygrygorenko@lukoil.com

Выполнено обобщение математического описания процессов первичной переработки сырых углеводородов (ППСУ) в виде нелинейных нестационарных дифференциальных уравнений в частных производных, что дает возможность применить принцип типизации при последующем математическом моделировании указанных процессов. Предложен и обоснован эффективный численный метод реализации математических моделей (ММ) процессов ППСУ, основанный на итерационной процедуре решения нелинейных нестационарных дискретных ММ исследуемых процессов.

Ключевые слова: математическая модель, итерационный процесс, разностная схема, параметрическая нелинейность, сходимость итерационной процедуры, сжатость отображения

NUMERICAL METHOD OF IMPLEMENTING MATHEMATICAL MODELS FOR THE PRIMARY PROCESSING OF RAW HYDROCARBONS

Yu. V. Grigorenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: ygrygorenko@lukoil.com

Generalization of the mathematical description of primary processing of raw hydrocarbons (PRH) in the form of nonstationary and nonlinear partial differential equations, which gives the opportunity to apply the principle of typification subsequent mathematical modeling of these processes. Proposed and justified efficient numerical method of realization of the mathematical model (MM) of processes of PRHs, based on the iterative procedure of solving nonlinear unsteady discrete MM investigated processes.

Keywords: mathematical model, iterative process, difference scheme, parametric non-linearity, the convergence of the iterative procedure, compactness display

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 4, номер 1, 2014. Одеса – 93 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 4, номер 1, 2014. Одесса – 93 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 4, No. 1, 2014. Odesa – 93 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №4 від 24.12.2013)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com