Поскольку, как правило, при использовании LSB-метода на практике ОПИ достаточно большой (50%–100%) [2], то полученные в ходе эксперимента результаты говорят о высокой эффективности разработанного стеганоаналитического алгоритма в условиях применения LSB-метода к КсП.

Заметим, что несколько бóльшая эффективность разработанного СА алгоритма в случае МАБ очевидно объясняется тем, что здесь сжатие осуществлялось непосредственно за счет обнуления наименьших СНЧ блоков матрицы ЦИ, которые затем и анализировались в процессе СА.

Заключение. На основе МПСА в работе разработан эффективный в условиях применения LSB-алгоритма СА алгоритм для КсП. Проделанный анализ и полученные результаты позволяют надеяться на успешную адаптацию данного алгоритма для детектирования работы стеганографических методов, отличных от LSB, на что и направлены в настоящий момент усилия автора.

Список литературы: **1.** *Хорошко В. А.* Методы и средства защиты информации / *В. А. Хорошко, А.А. Чекатков*. – К. : Юниор, 2003. – 501 с. **2.** *Грибунин В. Г.* Цифровая стеганография / *В. Г. Грибунин, И. Н. Оков, И. В. Туринцев*. – М. : Солон-Пресс, 2002. – 272 с. **3.** *G. Gul, F. Kurugollu*. SVD-Based Universal Spatial Domain Image Steganalysis / IEEE Transactions on Information Forensics and Security. – 2010. – Vol. 5, No. 2. – P. 349–353. **4.** *G. Gul, A. E. Dirik, I. Avcibas*. Steganalytic features for JPEG compression based perturbed quantization / IEEE Signal Process. Lett. – 2007. – Vol. 14, No. 3. – P. 205–208. **5.** *S. Lyu, H. Farid*. Detecting hidden messages using higher-order statistics and support vector machines / Lecture Notes in Computer Science. New York. – 2002.– Vol. 2578. – P. 340–354. ***6.*** *I. Avcibas, M. Kharrazi, N. Memon*, and etc. Image steganalysis with binary similarity measures / EURASIP J. Appl. Signal Process. – 2005. – Vol.7. – pp. 2749–2757. **7.** *Бобок И. И., Кобозева А. А.* Стеганоанализ как частный случай анализа информационной системы / Сучасна спеціальна техніка. – 2011. – № 2. – С. 21–34. **8.** *Бобок И. И., Кобозева А. А.* Общий стеганоаналитический подход, основанный на матричном анализе / Вісник Національного технічного ун-ту «ХПІ». Збірник наукових праць. Тематичний випуск «Системний аналіз, управління та інформаційні технології». – 2011. – № 35. – С. 12–20. **9.** *Кобозева А. А.* Анализ информационной безопасности / *А. А. Кобозева, В. А. Хорошко*. – К. : ГУИКТ, 2009. – 251 с. **10.** *Гонсалес Р.* Цифровая обработка изображений / *Р. Гонсалес, Р. Вудс*; пер. с англ. под ред. *П. А. Чочиа*. – М. : Техносфера, 2005. – 1072 с. **11.** *Кобозєва А. А.* Аналіз захищеності інформаційних систем / *А. А. Кобозєва, І. О. Мачалін, В. О. Хорошко*. – К. : ДУІКТ, 2010. – 316 с. ***12.*** *Кобозева А. А.* Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / Искусственный интеллект. – 2007. – № 4. – С. 531–538. **13.** *Деммель Дж.* Вычислительная линейная алгебра / *Дж. Деммель*; пер.с англ. *Х. Д. Икрамова*. – М. : Мир, 2001. – 430 с. **14.** *Каханер Д.* Численные методы и программное обеспечение / *Д. Каханер, К. Моулер, С. Нэш*; пер. с англ. *Х. Д. Икрамова*. – М. : Мир, 2001. – 575 с.

Надійшла до редколегії 26.12.2011

УДК 519.24

А. А. ПАВЛОВ, д-р техн. наук, проф., декан факультета информатики и вычислительной техники НТУУ «КПИ», Киев;

А. В. ЧЕХОВСКИЙ, студент НТУУ «КПИ», Киев

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ПОСТРОЕНИЯ МНОГОМЕРНОЙ ПОЛИНОМИАЛЬНОЙ РЕГРЕССИИ ПО ИЗБЫТОЧНОМУ ОПИСАНИЮ

У статті наводиться ефективний алгоритм відновлення багатовимірної поліноміальної регресії за надлишковим описом, що не приводить до послідовного накопичення помилок.

В статье приводится эффективный алгоритм восстановления многомерной полиномиальной регрессии по избыточному описанию не приводящий к последовательному накоплению ошибок.

The paper presents an efficient algorithm for reconstructing multivariate polynomial regression on excessive description that does not lead to a successive accumulation of errors.

В [1] приведен метод построения многомерной полиномиальной регрессии по избыточному описанию в условиях активного эксперимента. Метод реализует минимально необходимое число экспериментов (в схеме с фиксацией значений всех переменных кроме одной), но может приводить к существенному увеличению ошибок оценок неизвестных коэффициентов регрессии в результате решения последовательно конструируемых систем линейных равенств в следствие многократного использования в этих равенствах ранее найденных оценок коэффициентов регрессии. Этот эффект наиболее часто наблюдается в задачах большой размерности. Рассмотрим модификацию изложенного в [1] метода, которая исключает последовательное накопление ошибок оценок коэффициентов многомерной полиномиальной регрессии.

Возможность для одномерного случая практически гарантированно находить степень полинома линии регрессии, вычислять с допустимой вероятностью с заданной погрешностью коэффициенты этого полинома [1] позволяет предложить достаточно эффективную процедуру восстановления многомерной полиномиальной линии регрессии (при условии реализации активного эксперимента).

Пусть многомерная модель задается в виде

$$y(\bar{x}) = \sum_{\forall(i_1,\dots,i_t)\in K} \; \sum_{\forall(j_1,\dots,j_t)\in K(i_1,\dots,i_t)} b_{i_1,\dots,i_t}^{j_1,\dots,j_t} \left(x_{i_1}\right)^{j_1} \cdot \left(x_{i_2}\right)^{j_2} \dots \left(x_{i_t}\right)^{j_t} + E, \qquad (1)$$

где $\bar{x} = (x_1 \dots x_n)^{\mathrm{T}}$ – детерминированный вектор входных переменных;

$x_i - i$ -тая компонента вектора $\bar{x}$;

$b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ – неизвестные коэффициенты;

j_l – натуральные числа;

i_l – натуральные индексы из множества $\{1,\ldots,n\}$;

E – случайная величина с нулевым математическим ожиданием и ограниченной неизвестной дисперсией σ_E^2 (как и в одномерном случае может быть известна верхняя оценка σ_E^2).

Модель (1) является избыточной – возможно, некоторые из коэффициентов $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ равны нулю. Для удобства дальнейшего изложения линию регрессии модели (1) представим иначе:

$$\sum_{l=1}^{n} \sum_{\forall(i_1,\ldots,i_t)\in K_l} \sum_{\forall(j_1,\ldots,j_t)\in K_l(i_1,\ldots,i_t)} b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t} (x_{i_1})^{j_1} \cdot (x_{i_2})^{j_2} \ldots (x_{i_t})^{j_t}. \tag{2}$$

Составляющие

$$\sum_{\forall(i_1,\ldots,i_t)\in K_1} \sum_{\forall(j_1,\ldots,j_t)\in K_1(i_1,\ldots,i_t)} b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t} (x_{i_1})^{j_1} \cdot (x_{i_2})^{j_2} \ldots (x_{i_t})^{j_t} \tag{3}$$

содержат все слагаемые из (1), в каждую из которых входит компонента x_1.
Составляющие

$$\sum_{\forall(i_1,\ldots,i_t)\in K_1} \sum_{\forall(j_1,\ldots,j_t)\in K_1(i_1,\ldots,i_t)} b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t} (x_{i_1})^{j_1} \cdot (x_{i_2})^{j_2} \ldots (x_{i_t})^{j_t}, l=\overline{2,n}, \tag{4}$$

содержат все слагаемые из (1), в каждую из которых входит компонента x_l,

Рассмотрим составляющую (3). Обозначим через M_j^1, $j=\overline{1,n_1}$, количество слагаемых, каждая из которых содержит x_1 в j-й степени; $\mathrm{M}^1 = \max_j \mathrm{M}_j^1$, $j=\overline{1,n_1}$, n_1 – максимальная степень полинома от переменной x_1.

Фиксируем M^1 наборов значений компонент $x_2^s,\ldots,x_n^s$, $s=\overline{1,\mathrm{M}^1}$. На числа x_i^s, $i=\overline{2,n}$, $s=\overline{1,\mathrm{M}^1}$, накладывается единственное условие – определенные ниже квадратные матрицы должны быть невырожденными.

Реализуем M^1 экспериментов, в каждом из которых (s-м, $s=\overline{1,\mathrm{M}^1}$) переменные $x_2,\ldots,x_n$ принимают фиксированные значения $x_i^s\left(i=\overline{2,n}\right)$, а переменная x_1 изменяется как при построении одномерной полиномиальной регрессии. При фиксированных значениях переменных $x_2,\ldots,x_n$ в s-м эксперименте ($s=\overline{1,\mathrm{M}^1}$) многомерная линия регрессии превращается в полином от переменной x_1 степени n_1.

Для каждого s-го эксперимента ($s=\overline{1,\mathrm{M}^1}$) находим значения дисперсий $D\hat{\theta}_j^s$, $j=\overline{1,n_1}$, и эти числа ранжируем по возрастанию их значений при фиксированном j. Получим n_1 проранжированных последовательностей оценок коэффициентов $\theta_j^{s_1},\ldots,\theta_j^{s_{M^1}}\left(j=\overline{1,n_1}\right)$.

Эти результаты позволяют сформировать n_1 систем линейных уравнений, решениями которых являются значения всех коэффициентов $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ в выражении (3).

Действительно, в каждом из s экспериментов неизвестные коэффициенты $\hat{\theta}_j^s\left(j=\overline{1,n_1}\right)$ одномерной полиномиальной регрессии степени n_1 от переменной x_1 определяются следующим образом: необходимо из всех членов выражения (содержащих переменную x_1 в степени j) вынести x_1^j. Полученное выражение для θ_j^s содержит только M_j^1 неизвестных коэффициентов вида $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$, так как в каждом s-м эксперименте при изменении значений переменной x_1 переменные x_i, $i=\overline{2,n}$ принимают одно и то же фиксированное значение x_i^s, $i=\overline{2,n}$. Таким образом, для построения системы линейных уравнений для нахождения M_1^1 коэффициентов вида $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ надо использовать M_1^1 чисел $\hat{\theta}_1^{s_1},\ldots,\hat{\theta}_1^{s_{M_1^1}}$ (они имеют наименьшую дисперсию).

Для определения верхних статистических оценок точности нахождения M_1^1 коэффициента вида $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$, полученную систему линейных уравнений условно запишем так:

$$A\begin{pmatrix} x_1 \\ \vdots \\ x_{\mathrm{M}_1^1} \end{pmatrix}\begin{pmatrix} \hat{\theta}_1^{s_1} \\ \vdots \\ \hat{\theta}_1^{s_{M_1^1}} \end{pmatrix}, \tag{5}$$

где x_i, $i=\overline{1,\mathrm{M}_1^1}$ – переменные (соответствующие M_1^1 переменным вида $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$).

Пусть оценки $\widehat{\theta}_1^{s_l}, l=\overline{1,\mathrm{M}_1^1}$, с заданной статистически значимой вероятностью p оценивают $\theta_1^{s_l}$ с погрешностью, по модулю не превышающей чисел $\Delta_1^{s_l}, l=\overline{1,\mathrm{M}_1^1}$. Тогда с вероятностью p максимальная погрешность нахождения точных значений M_1^1 соответствующих коэффициентов вида $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ имеет вид

$$\max_{j=1,\mathrm{M}_1^1}\left\{\max\left(\sum_l{}^{(+)}a_{jl}^{-1}\Delta_1^{s_l},\sum_l{}^{(-)}\left|a_{jl}^{-1}\right|\Delta_1^{s_l}\right)\right\}, \tag{6}$$

где $\sum_l{}^{(+)}a_{jl}^{-1}\Delta_1^{s_l}$ берется по всем $l=\overline{1,\mathrm{M}_1^1}$, для которых $a_{jl}^{-1}\ge 0$; $\sum_l{}^{(-)}a_{jl}^{-1}\Delta_1^{s_l}$ берется по всем $l=\overline{1,\mathrm{M}_1^1}$, для которых $a_{jl}^{-1}<0$; a_{jl}^{-1} – jl-й элемент матрицы A^{-1}.

Как указывалось выше, предполагается, что $x_i^s, i=\overline{2,n}, s=\overline{1,\mathrm{M}_1^1}$ выбраны так, что матрица A^{-1} существует.

Для каждой переменной $x_l, l=\overline{2,n}$ нахождение коэффициентов $b_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ в выражениях (4) реализуется точно так же, как это описано для переменной x_1.

Недостаток модифицированной схемы заключается в увеличении необходимого числа экспериментов, повторной оценке коэффициентов слагаемых, присутствующих в выражениях (4), которые были найдены на предыдущих этапах.

Преимущество заключается в отсутствии последовательного накопления ошибок и появлении косвенного критерия эффективного восстановления многомерной регрессии: практическое совпадение оценок повторяющихся коэффициентов многомерной регрессии в результате решения разных систем линейных равенств.

Изложенные выше методики требуют избыточное число экспериментов для практически точного нахождения коэффициентов в слагаемых полинома вида $a_i x_{i_1} x_{i_2} \ldots x_{i_k}$. Так при фиксации значений всех переменных кроме одной получаем слагаемое первой степени относительно скалярной переменной. В этом случае удобен следующий прием:

кладем $x_{i_1}=x_{i_2}\ldots x_{i_{k-1}}=x$, а значения x_{i_k} фиксируются; либо $x_{i_1}=x_{i_2}\ldots=x_{i_k}=x$. Тогда в одномерных регрессиях соответствующие члены имеют вид $Q_{ke}a_i x^{k-1}$, (Q_{ke} фиксированные числа), либо $a_i x^k$. В этом случае одно и тоже количество экспериментов приводит на порядки более точному нахождению коэффициентов при x^{k-1} либо x^k в одномерных регрессиях и

следовательно решение соответствующих систем линейных равенств приводит к качественно более точным оценкам коэффициентов a_i. Представление независимых переменных $x_i, i=\overline{1,n}$ в одном из двух приведенных выше видов определяется структурой избыточного полиномиального описания многомерной регрессии и как следствие требованиями к системам линейных равенств для оценки неизвестных коэффициентов линии регрессии. Из анализа решения конкретных примеров следует что приведенный прием может приводить к построении существенно меньшего количества одномерных регрессий.

Список литературы: **1.** *Згуровский М. З.* Принятие решений в сетевых системах с ограниченными ресурсами: Монография / *М. З. Згуровский, А. А. Павлов* // К. : Наукова думка, 2010. – 574 с.

Надійшла до редколегії 01.02.2012

УДК 519.2

В. А. ШЕХОВЦОВ, канд. техн. наук, НТУ «ХПИ»;
М. Д. ГОДЛЕВСКИЙ, д-р. техн. наук, НТУ «ХПИ»;
И. Л. БРАГИНСКИЙ, аспирант, НТУ «ХПИ»

ВЕРБАЛЬНОЕ ОПИСАНИЕ ТЕХНОЛОГИИ УЛУЧШЕНИЯ КАЧЕСТВА ПРОЦЕССА РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Модель зрілости програмного забезпечення є одним із основних понять, які пов‘язані з покращенням процесу розробки програмного забезпечення. Вона реалізована як опис просування організації до бажаного рівня реалізації процесу розробки, заданий як сукупність послідовних етапів (які треба виконати) або рівнів (яких треба досягти). У цій роботі розглянуто питання вербального опису основних понять моделей зрілості програмного забезпечення, спираючись на інформацію, що доступна із практики.

Модель зрелости программного обеспечения является одним из основных понятий, связанных с улучшением процесса разработки программного обеспечения. Она представляет собой описание продвижения организации к желаемому уровню реализации процесса разработки, заданное в виде нескольких последовательных этапов (которые нужно выполнить) или уровней (которых нужно достичь). В данной работе рассмотрен вопрос вербального описания основных понятий моделей зрелости программного обеспечения, опираясь на информацию, доступную из практики.

Software maturity model is a main concept, related to software process improvement. It is a description of the ideal movement of the organization (or its branch) towards the desired level of implementation of the software process, defined as the sequence of consequent stages (which must be implemented) or levels (which must be reached), together with the means of assessment of the completeness of the implementation of the described stages or compliance to the described levels. In this paper, we