Висновки і перспективи дослідження

В даній роботі представлено нестандартний протокол оцінки ефективності відомих і розроблюваних стеганоалгоритмів, в якому усунуто недоліки існуючих для даних цілей програм тестування. Тест-система, розроблена на основі даного протоколу, може бути використана для моніторингу ефективності алгоритмів, що використовуються для захисту авторського права, ідентифікації медіаконтенту цифровими "відбитками", контролю доступу до конфіденційної інформації тощо.

Список літератури

1. Internet-ресурс інформагентства Reuters (http://today.reuters.com/news/).
2. Internet-ресурс Цейтру дослідження проблем комп'ютерної злочинності — Computer Crime Research Center (http://www.crime-research.org/).
3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: "МК-Пресс", 2006. — 288 с.
4. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії. — Вінниця: ВДТУ, 2003. — 143 с.
5. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: "Солон-Пресс", 2002. — 272 с.
6. StirMark (http://www.petitcolas.net/fabien/watermarking/stirmark/index.html), UnZign (http://www.petitcolas.net/fabien/steganography/image_watermarking/unzign/).
7. Вентцель Е.С., Овчаров В.А. Теория вероятностей и её инженерные приложения. Изд. 3-е, перераб. и доп. Уч. пос. для ВУЗов. — М.: "Академия", 2003. — 464 с.
8. Б. Скляр, Цифровая связь: Теоретические основы и практическое применение. Изд. 2-е, исправл. — М.: "Вильямс", 2003. — 1104 с.

УДК 681.511.3

Кобозева А.А., Маракова И.И.

МЕТОД ОЦЕНКИ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ К ВОЗМУЩАЮЩИМ ПРЕОБРАЗОВАНИЯМ

По мере развития современного общества проблема защиты информации становится все более актуальной, что приводит к резкому повышению интереса к исследованиям в области компьютерной стеганографии [1]. Толчком для развития этих исследований в последнее время послужило появление новых областей применения. Дополнительная информация (ДИ) встраивается в основное сообщение (ОС), в качестве которого может использоваться видео, изображение, аудиозаписи и т.д., причем дополнительная информация может быть как секретной, так и несекретной. Без потери общности для конкретизации исследований далее в качестве ОС будем рассматривать изображение.

Целью исследования является установление таких свойств произвольного изображения, наличие которых явилось бы достаточным условием устойчивости предлагаемого алгоритма стеганографического преобразования этого изображения и декодирования скрытой в нем информации к различного рода искажениям, а также нечувствительности задачи о декодировании ДИ к возмущениям в исходных данных.

Дадим определения используемым понятиям.

Стеганографическим преобразованием будем называть процесс погружения ДИ в основное сообщение.

Задачу назовем нечувствительной к погрешностям в исходных данных (возмущениям), если малые изменения этих данных приводят к малой погрешности результата [2].

Произвольный численный алгоритм называется устойчивым, если от шага к шагу погрешность в этом алгоритме не возрастает или возрастает незначительно. Алгоритм пересылки и детектирования ДИ, применяемый в области компьютерной стеганографии, будем называть устойчивым, если он позволяет адресату детектировать полученную информацию с малой результирующей ошибкой.

Аналоговое описание наиболее приемлемо для человеческого восприятия изображения. Любое изображение в градациях серого можно рассматривать как некоторую вещественную функцию f двух вещественных переменных x и y, областью определения которой, не ограничивая общности рассуждений, можно считать $[0, 1] \times [0, 1]$ *c* $\mathbf{R}^2$:

$$f(x, y) : [0, 1] \times [0, 1] \rightarrow \mathbf{R}^+ . \qquad (1)$$

Если f (x, y) является основным сообщением или контейнером, используемым для встраивания в него некоторой дополнительной информации с целью ее скрытой передачи, также рассматриваемой в виде функции

$$z(x, y) : [0, 1] \times [0, 1] \rightarrow \mathbf{R}^+, \qquad (2)$$

тогда погружение ДИ в контейнер равносильно получению нового изображения, т.е. построению новой функции s(x, y) вида (1). Способы формирования стегосообщения могут быть различны. Так, например, аддитивный способ соответствует соотношению:

$$s(x, y) = f(x, y) + z(x,y).$$

Стеганографическое преобразование изображения можно иначе трактовать как возмущение исходных данных (контейнера f(x, y)), причем даже в случае отсутствия преобразований атакующим, канал связи внесет дополнительные искажения стегосообщения, т.е. погрешность еще более возрастет. Для оценки погрешности исходного сообщения на приемном конце нужно оценить степень возмущения решения задачи о детектировании погруженного дополнительного сообщения при малом возмущении ее входных данных.

Рассмотрим сначала вещественную дифференцируемую функцию g(x) вещественной переменной x. Пусть необходимо вычислить значение $g(x_0)$, но x_0 не может быть получено точно при наличии $x_0 + \delta x$ и границы для δx (δx - абсолютная погрешность исходных данных). Известно [3]:

$$g(x_0 + \delta x) = g(x_0) + g'(x_0)\,\delta x + \bar{o}(\delta x), \text{ когда } \delta x \rightarrow 0, \qquad (3)$$

тогда абсолютная погрешность

$$|g(x_0 + \delta x) - g(x_0)| \approx |g'(x_0)|\,|\delta x|. \qquad (4)$$

$|g'(x_0)|$ называется абсолютным числом обусловленности функции g в точке x_0 [4]. Число обусловленности часто называют мерой чувствительности задачи к погрешности в исходных данных. Как видно из (4), если число обусловленности велико, то погрешность может быть большой даже при малом возмущении исходного данного. Для относительной погрешности результата из (4) вытекает оценка:

$$\frac{|g(x_0+\delta x)-g(x_0)|}{|g(x_0)|} \approx \frac{|g'(x_0)|*|x_0|}{|g(x_0)|} * \frac{|\delta x|}{|x_0|} \qquad (5)$$

Множитель $|g'(x_0)|*|x_0|/|g(x_0)|$ называется относительным числом обусловленности.

Выражение для числа обусловленности варьируется для конкретной задачи, однако в любом случае число обусловленности дает возможность оценить погрешность результата в соответствии с погрешностью исходных данных и позволяет судить о чувствительности задачи.

Пусть $s(x, y)$ – некоторая функция вида (1), определяющая результирующее изображение после вписывания ДИ, а через $algor(x, y)$ будем обозначать непосредственно выбранный численный алгоритм для вычисления $s(x, y)$. Необходимо отметить, что результат $algor(x, y)$ содержит вычислительную погрешность. Предположим, что $algor(x, y)$ является обратно устойчивым алгоритмом для $s(x, y)$ [4], тогда возможно представление:

$$algor(x, y) = s(x + \delta x, y + \delta y),$$

а оценки, аналогичные (3) – (5), имеют вид:

$$s(x+\delta x, y+\delta y) = s(x, y) + \frac{\partial s(x,y)}{\partial x}\delta x + \frac{\partial s(x,y)}{\partial y}\delta y + \bar{\mathbf{o}}\left(\sqrt{\delta x^2+\delta y^2}\right),$$

когда $\sqrt{\delta x^2+\delta y^2} \to 0$,

$$|s(x+\delta x, y+\delta y) - s(x, y)| \approx \left|\frac{\partial s(x,y)}{\partial x}\delta x + \frac{\partial s(x,y)}{\partial y}\delta y\right| =$$

$$= |(\operatorname{grad} s(x, y), (\delta x, \delta y))|. \qquad (6)$$

Используя в правой части (6) неравенство Коши – Буняковского, получим:

$$|s(x+\delta x, y+\delta y) - s(x, y)| \le \|\operatorname{grad} s(x, y)\| * \|(\delta x, \delta y))\|$$

В качестве абсолютного числа обусловленности здесь может рассматриваться $\|\operatorname{grad} f(x, y)\|$. Тогда для погрешности становится возможной оценка:

$$|algor(x, y) - s(x, y)| = |s(x+\delta x, y+\delta y) - s(x, y)| \approx \|\operatorname{grad} s(x, y)\| * \|(\delta x, \delta y))\|. \qquad (7)$$

Как видно из (7), абсолютная погрешность результата в каждой точке зависит от абсолютного числа обусловленности функции $s(x, y)$ в этой точке. При обратной устойчивости $algor(x, y)$ величина $\|(\delta x, \delta y))\|$ мала, тогда если абсолютное число обусловленности невелико (в этом случае функция называется хорошо обусловленной), то мала будет и погрешность. Если же число обусловленности большое (или бесконечно большое) (функция называется плохо обусловленной), то несмотря на малое значение обратной ошибки [4] $\|(\delta x, \delta y))\|$, результирующая погрешность может оказаться не-

приемлемо большой. Из всего вышесказанного представляется возможным сформулировать следующую теорему:

Т е о р е м а 1. Задача получения стеганографического преобразования изображения с использованием обратно устойчивого численного алгоритма является нечувствительной к погрешности исходных данных, если абсолютное число обусловленности функции $s(x, y)$, которое выражается как $\|\operatorname{grad} s(x, y)\|$, в любой точке (x, y) из области $[0, 1] \times [0, 1]$ невелико.

Иначе говоря, теорема 1 требует ограниченность $\|\operatorname{grad} s(x, y)\|$ на всей области $[0, 1] \times [0, 1]$, причем мажорирующая константа для $\|\operatorname{grad} s(x, y)\|$ не должна быть большой.

Сложность получения оценки значения $\|\operatorname{grad} s(x, y)\|$ зависит от самой функции $s(x, y)$. Однако важную роль здесь играет тот факт, что функция $s(x, y)$ определена на компактном множестве. Действительно, предположим, что $s(x, y) \in \mathbf{C}^1([0,1] \times [0,1])$, тогда по теореме Вейерштрасса [3] $s'_x(x, y)$, $s'_y(x, y)$ ограничены на этом компакте, т.е. найдется такая постоянная величина $M > 0$, что для любой точки $(x, y) \in [0,1]\times[0,1]$ будет выполняться соотношение:

$$\|\operatorname{grad} s(x, y)\| < M.$$

Если величина M является приемлемой в рассматриваемой задаче, то результирующая погрешность будет небольшой.

Все вышесказанное для оценки $\|\operatorname{grad} s(x, y)\|$ будет верно и в том случае, если частные производные $s(x, y)$ будут просто ограничены в области $[0,1]\times[0,1]$. Однако предложить общий путь для оценки числа обусловленности произвольной функции вида (1) помимо непосредственного вычисления $\|\operatorname{grad} s(x, y)\|$ невозможно.

Теорема 1 носит теоретический характер, показывая важность абсолютного числа обусловленности функции для нечувствительности задачи получения стеганографического преобразования, поскольку на практике при численной обработке мы имеем дело с цифровым изображением.

Получение цифрового изображения можно представить осуществляемым следующим образом. Непрерывная область $[0, 1] \times [0, 1]$ подвергается равномерной дискретизации прямыми $x = ih$, $y = jh$ (не ограничивая общности рассуждений, мы будем считать, что $i, j = 1, \ldots, n - 1$, $h = 1 / n$, где n – количество частичных сегментов, на которые разбиваются отрезки $[0, 1]$ по оси Ox и по оси Oy. Это количество выбирается одинаковым для обеих сторон исходного квадрата-изображения). Такая дискретизация приведет к появлению n^2 одинаковых квадратных подобластей со стороной, равной h. В каждой из полученных подобластей выбирается срединная точка (центр квадрата), координаты которой обозначим (x_i, y_j), $i, j = 1, \ldots, n$. Определим новую функцию $f_{пр}(x, y)$, значение которой в точках отдельной подобласти, являющейся окрестностью (x_i, y_j), считается постоянным и равным значению $[f(x_i, y_j)]$, $i, j = 1, \ldots, n$. Таким образом после описанной дискретизации изображения можно считать, что мы с некоторой погрешностью заменили исходную функцию $f(x, y)$ на интерполирующую ее функцию $f_{пр}(x, y)$, являющуюся интерполяционным сплайном нулевой степени. Значения $f_{пр}(x, y)$ могут быть только целыми. На практике для изображений в градациях серого используют:

$$f_{пр}(x, y): [0, 1] \times [0, 1] \rightarrow \{0, 1, 2, \ldots, 255\}.$$

Для представления полученного сплайна будем использовать квадратную матрицу F, размерность которой n x n. Элементы этой матрицы

$$F(i,j) = f_{пр}(x_i, y_j), i, j = 1, \ldots, n. \qquad (8)$$

Аналогичной дискретизации подвергается и функция (2) ДИ.

В дальнейшем, говоря об изображении, будем подразумевать матрицу вида (8), а стеганографическое преобразование изображения будет иметь характер матричных операций [5].

Для обоснования приводимого ниже предложения рассмотрим неоднородную систему линейных алгебраических уравнений (СЛАУ)

$$A x = b \qquad (9)$$

с невырожденной матрицей A и ненулевым вектором правой части. Предположим, что единственное решение этой системы получено некоторым численным методом , входными данными для которого является матрица A и вектор b, и равно $x_{пр}$. Очевидно, $A x_{пр} \neq b$, а $\|\delta x\| = \| x_{пр} - x \|$ является абсолютной погрешностью полученного решения. Мы можем рассматривать $x_{пр}$ как точное решение некоторой возмущенной СЛАУ

$$(A + \delta A) x_{пр} = b + \delta b, \qquad (10)$$

где δA и δb – возмущения исходных данных. Из (10) получаем:

$$\delta x = A^{-1} (\delta b - \delta A x_{пр}),$$

$$\| \delta x \| \leq \| A^{-1} \| (\| \delta b \| + \| \delta A \| \| x_{пр} \|). \qquad (11)$$

Поскольку $\det A \neq 0$, матрица A не может быть нулевой, значит любая норма этой матрицы отлична от нуля, вектор $x_{пр}$ - решение неоднородной системы, а потому $\| x_{пр} \| \neq 0$. Используя это, получаем из (11):

$$\frac{\| \delta x \|}{\| x_{пр} \|} \leq \| A^{-1} \| \| A \| \left(\frac{\| \delta b \|}{\| A \| \| x_{пр} \|} + \frac{\| \delta A \|}{\| A \|} \right) \qquad (12)$$

Здесь относительная погрешность результата сравнивается с относительным изменением входных данных через величину $\| A^{-1} \| \| A \|$, которая называется числом обусловленности невырожденной матрицы в задаче о решении СЛАУ и, как видно из (12), является мерой чувствительности задачи о решении системы к погрешности в исходных данных. Если число обусловленности матрицы системы мало, такая система является нечувствительной к малым погрешностям в исходных данных, т. е. малые возмущения на входе не изменят заметно результат.

Пусть F – матрица-изображение размерности n x n. Предположим, что это изображение используется как контейнер для пересылки ДИ. При пересылке заполненного контейнера по каналам связи он подвергается различным атакам, что приводит как к изменению самого контейнера, так и к изменению ДИ. Для нас результатом атак является возмущение исходных данных, т.е. изменение элементов матрицы-изображения. При этом важным является то, чтобы полученные возмущения не повлияли значитель-

но на результат детектирования ДИ адресатом. Именно в этом смысле рассматривается устойчивость алгоритма детектирования. Получим достаточные условия для выполнения данного требования.

Пусть контейнер F используется для пересылки ДИ – произвольной последовательности, содержащей n элементов (последовательность может содержать и менее n элементов. Тогда она дополняется незначащими элементами до нужной длины). Обозначим пересылаемое сообщение x. x – это вектор длины n. Вычислим произведение $b = Fx$, представляющее из себя тоже вектор длины n. Затем b кодируется и погружается в F вместо несущего нужную информацию x. Тогда декодирование нужной информации будет включать в себя два этапа. Сначала при получении заполненного контейнера стандартным устойчивым алгоритмом декодируется содержащийся в нем вектор b (получаем возмущенный вектор b_B), а получение нужного информационного x будет происходить на втором этапе при решении системы

$$F_B x = b_B . \qquad (13)$$

Здесь F_B и b_B - возмущенные входные данные. Источниками возмущения являются не только возможные атаки в канале связи при пересылке, но и работа алгоритма декодирования b. Поскольку F_B, вообще говоря, произвольная матрица, гарантировать устойчивость исключений при решении (13) без перестановок нельзя [2]. Поэтому предпочтительным здесь окажется устойчивый для невырожденной хорошо обусловленной матрицы метод Гаусса с выбором главного элемента. Предположим, что результирующие возмущения таковы, что значения

$$\| F_B - F \| / \| F \| , \quad \| b_B - b \| / \| b \| \qquad (14)$$

невелики. Нужно особо отметить, что последнее требование анализирует возмущение всей матрицы и всего вектора в целом. Даже большая погрешность, возникающая в отдельных пикселях заполненного контейнера при небольшом их количестве не отразится значительно на оценках для выражений (14), а значит, при хорошей обусловленности матрицы F, и на значении x.

Организованный предложенным образом алгоритм пересылки и получения ДИ назовем SISTEMA. Декодирование, осуществляемое в соответствии с алгоритмом SISTEMA, позволяет обеспечить дополнительную защиту информационного вектора x по сравнению с непосредственной пересылкой его в качестве ДИ.

Из всего вышесказанного вытекает следующая

Т е о р е м а 2 . Пусть матрица изображения, используемого в качестве ОС для пересылки ДИ, является хорошо обусловленной, а пересылка и декодирование ДИ производится в соответствии с алгоритмом SISTEMA. Тогда задача декодирования ЦВЗ является нечувствительной к погрешности исходных данных, а алгоритм SISTEMA устойчивым.

Одним из важных звеньев алгоритма SISTEMA является решения СЛАУ (13). Применение численного метода решения, даже устойчивого, к произвольной неоднородной системе с невырожденной матрицей в общем случае не гарантирует получение результата с малой погрешностью. Даже если вектор невязки для системы (9), определяемый соотношением $r = b - A x_{пр}$, мал , это еще не означает, что $x_{пр} \approx x$. Действительно, в соответствии с оценкой для относительной погрешности решения СЛАУ [2]

$$\| \delta x \| \qquad \| r \|$$

$$\frac{\|x\|}{} \leq \|A^{-1}\| \, \|A\| \, \frac{}{\|b\|}$$

очевидно, что малость вектора невязки гарантирует хорошую точность решения только в том случае, когда матрица системы хорошо обусловлена. Это еще раз подтверждает важность требования для обусловленности матрицы F системы (13) при использовании алгоритма SISTEMA.

При практическом использовании алгоритма SISTEMA в качестве контейнера достаточно будет использовать изображение, матрица которого является хорошо обусловленной, а значит актуальным становится вопрос оценки числа обусловленности матрицы F (cond F). Заметим, что вообще говоря, число обусловленности определяется не только для невырожденных матриц:

$$\text{cond } F = \begin{cases} \|F\| * \|F^{-1}\|, & \text{если } \det F \neq 0 \\ +\infty, & \text{если } \det F = 0. \end{cases}$$

Важно отметить, что число обусловленности матрицы обратно пропорционально связано с ее определителем : чем ближе определитель матрицы к нулю, тем больше число обусловленности. Таким образом, можно сказать, что cond F является мерой вырожденности матрицы F. Переходя к геометрическому смыслу вырожденности матрицы, получим, что cond F является мерой линейной независимости строк (или столбцов) матрицы F. Эти соображения позволят нам избежать оценки числа обусловленности матрицы за счет его непосредственного вычисления , требующего обращения F , а затем определения $\|F^{-1}\|$ (это стоила бы $2n^3$ операций. Для сравнения: гауссово исключение требует $2n^3 / 3$). Кроме того, нам вообще не нужно знать точное значение cond F , а нужна лишь его оценка. Существует множество более дешевых алгоритмов оценивания $\|F^{-1}\|$ [4], [6] , называемых оценщиками обусловленности и обладающими следующими свойствами : такой алгоритм использует $\underline{O}(n^2)$ операций, если имеются треугольные множители разложения матрицы F (F = L U) ; он дает оценку, почти всегда не превосходящую удесятиренного значения $\|F^{-1}\|$. Использование таких алгоритмов даст возможность удешевить процесс выбора подходящего контейнера при использовании алгоритма SISTEMA.

Другой путь для удешевления оценки cond F базируется на упомянутом выше свойстве числа обусловленности матрицы как меры линейной независимости ее строк (столбцов). Для некоторых изображений, например, представленных на рис.1, 2 , такая независимость является очевидной. Конечно, представленные изображения достаточно просты, а явно видимое распределение нулей в их матрицах говорит о линейной независимости строк (столбцов) без дополнительных исследований. Для произвольных монохромных изображений решение этого вопроса не будет столь простым, а очевидно потребует либо привлечение гистограммы и определенных оценок для геометрии контура, либо разбиение изображения на более «простые» подобласти, исследование каждой из которых позволит сделать вывод о числе обусловленности подматрицы исходной матрицы F, отвечающей этой подобласти. Под «простыми» подобластями понимаются такие, для матриц которых линейная независимость строк (столбцов) устанавливается без привлечения дополнительных исследований (например, как для изображений на рис. 1,2). Таким образом в исходном изображении (даже если его матрица является плохо обусловленной)

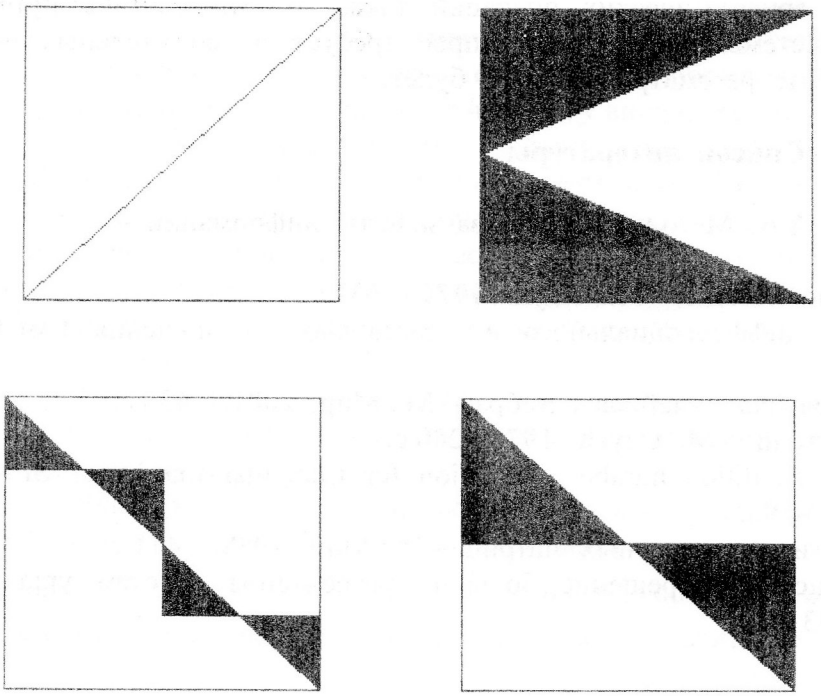

Рис. 1. Бинарные изображения с хорошо обусловленной матрицей.

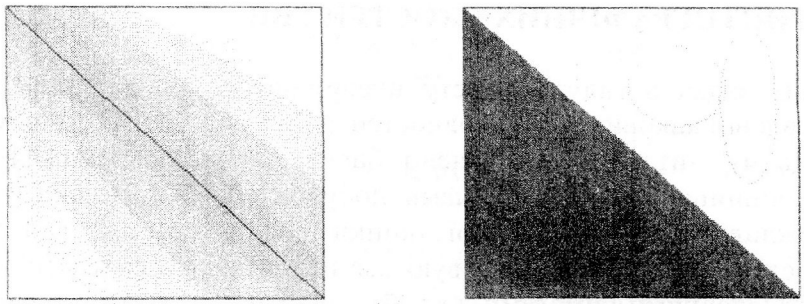

Рис. 2. Монохромные изображения с хорошо обусловленной матрицей

возможно выделить такие подизображения, которые будут иметь хорошо обусловленные подматрицы (это возможно практически всегда, если только начальное изображение не является однотонным или с сильно размытым, практически неопределяемым контуром. Но такое изображение само по себе неудобно использовать в качестве контейнера). В контейнере обнаруживаются подобласти, которые и будут использоваться для погружения в них ДИ. Преимущества такого пути заключается в уменьшении размерности возникающей задачи (размерность подматрицы меньше n).

Уменьшение размерности задачи важно не только с точки зрения оценки числа обусловленности. Вторым этапом в декодировании является решение СЛАУ вида (13). Поскольку матрица решаемой системы (или матрицы решаемых систем меньшей размерности в случае разбиения области на подобласти) является хорошо обусловленной, то любой устойчивый прямой численный метод решения СЛАУ гарантированно даст результат с приемлемой погрешностью. Количество арифметических операций, требуемых для этого, определяется как $\underline{O}(n^3)$. Очевидно, разбиение исходной задачи на подзадачи меньшей размерности даст возможность сократить требуемое для решения СЛАУ время.

Уменьшение количества арифметических операций также можно достичь путем переупорядочения исходной системы [7, 8]. Этот вопрос требует дополнительных исследований и в настоящей работе рассматриваться не будет.

Список литературы

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с.
2. Бахвалов Н.С. Численные методы. – М.: Наука, 1975. – 632 с.
3. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. Том 1.- М.: Наука, 1969. – 608 с.
4. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. – 430 с.
5. Ланкастер П. Теория матриц. – М.: Наука, 1978.- 280 с.
6. N.J.Higham. A survey of condition number estimation for triangular matrices.// SIAM Rev., № 29, 1987.- P. 575-596.
7. Писсанецки С. Технология разреженных матриц. – М.: Мир, 1988. – 411 с.
8. Джордж А., Лю Дж. Численное решение больших разреженных систем уравнений. – М.: Мир, 1984.- 333 с.

УДК 691.321

Л.В.Ковальчук, В.Т.Бездітний

ПЕРЕВІРКА НЕЗАЛЕЖНОСТІ СТАТИСТИЧНИХ ТЕСТІВ, ПРИЗНАЧЕНИХ ДЛЯ ОЦІНКИ КРИПТОГРАФІЧНИХ ЯКОСТЕЙ ГВП.

Однією з найактуальніших задач в галузі захисту інформації є задача створення генератора випадкових (або псевдовипадкових) послідовностей (ГВП або ГПВП), що має певні криптографічні якості. Цьому питанню присвячено багато робіт, зокрема, [1-5]. Незалежно від того, за якими принципами та алгоритмами побудовано ГВЧ, оцінка його криптографічних якостей неможлива без статистичної оцінки послідовностей, що він виробляє. Для оцінки якостей послідовностей використовуються певні набори статистичних тестів (див., наприклад, [1, 6-9]). Основними вимогами до набору тестів є достатність цього набору та незалежність його складових. Питання достатності набору тестів тісно пов'язане як з умовами застосування набору, так і з можливою сферою застосування генератора і у даній роботі не розглядається. Задача перевірки незалежності статистичних тестів є актуальною не тільки при оцінці якостей генератора, але й при вирішенні багатьох інших прикладних криптографічних задач, які пов'язані з аналізом та синтезом криптографічних систем. В першу чергу це задачі оцінки *одноразових блокнотів*[1], *криптографічних алгоритмів*[2] та інших параметрів криптосистем.

Необхідність перевірки незалежності статистичних тестів, що використовуються при розв'язанні зазначених задач, полягає у наступному.

По-перше, це необхідність мінімізації кількості статистичних тестів. Набір тестів повинен бути "оптимальним" у тому розумінні, що він повинен містити суттєві тести і не містити тестів, які б повторювали інші. Наприклад, якщо відомо, що послідовність, яка пройшла тест А, з великою ймовірністю пройде тест В, то тест В можна виключити з набору для зменшення часу тестування

По друге, це необхідність оцінки загальної помилки першого роду при виборі набору тестів, яка можлива лише за умови незалежності тестів.

---

[1] В даному випадку, оцінка стійкості криптографічних перетворень зводиться до аналізу процедури генерації ключів, а фактично - фізичних датчиків випадкових чисел.

[2] Оцінці підлягають статистичні властивості виходу криптографічних перетворень, а саме функції виходу автоматної моделі криптоалгоритму.