7. *G. Zacharia.* Collaborative reputation mechanisms for online communities. Massachusetts Institute of Technology, September 1999.

8. *Goguen J. A., Meseguer J.* Unwinding and Inference Control. 1984, Symposium on Security and Privacy, P. 75-85, IEEE, May 1984.

Поступила 19.10.2006 г.

УДК 004.056.5: 518: 512.624.3 **Кобозева А.А., Маракова И.И.**

МЕТОД ПОВЫШЕНИЯ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ К ВОЗМУЩАЮЩИМ ВОЗДЕЙСТВИЯМ

Введение

В настоящий момент во всем мире назрел вопрос разработки методов защиты информации, представленной в цифровом виде, среди которых важное место занимают стеганографические методы [1].

Несмотря на то, что стеганографирование может осуществляться различными способами, общей чертой этих способов является то, что секретное сообщение, или дополнительная информация (ДИ), погружается в некоторый объект, или основное сообщение (ОС), не привлекающий внимания, который затем открыто пересылается адресату. Одной из основных проблем при этом является проблема обеспечения устойчивости таких стеганографических сообщений к возмущающим воздействиям в канале связи.

Дополнительным толчком для развития исследований в области компьютерной стеганографии в последнее время послужило появление новых областей ее применения. В качестве ОС, или контейнера, может использоваться видео, изображение, аудиозаписи и т.д. Не ограничивая общность рассуждений, для простоты изложения далее в качестве контейнера рассматривается монохромное изображение.

В настоящей работе предлагается новый метод организации пересылки и декодирования ДИ, основанный на решении систем линейных алгебраических уравнений (СЛАУ), целью которого является обеспечение повышения устойчивости стегоалгоритмов к возмущающим воздействиям; обосновываются достаточные условия нечувствительности задачи о декодировании ДИ путем решения СЛАУ к погрешностям исходных данных. В качестве инструмента исследования используется теория относительных возмущений [2].

Число обусловленности задачи - мера ее чувствительности к возмущениям входных данных

Любое монохромное изображение можно рассматривать как функцию f двух переменных x и y, областью определения которой, не ограничивая общности рассуждений, можно считать $[0,1]\times[0,1]\subset R^2$:

$$f(x,y):[0,1]\times[0,1]\to R^+. \qquad (1)$$

Пусть $f(x,y)$ является основным сообщением, используемым для встраивания в него некоторой ДИ с целью ее скрытой передачи, также рассматриваемой в виде функции $z(x,y)$ вида (1), тогда погружение секретного сообщения в контейнер равносильно получению нового изображения, т.е. построению новой сложной функции $s(x,y)=F(f(x,y),z(x,y))$ вида (1). Функцию $s(x,y)$ в дальнейшем будем называть стегосообщением.

Способы формирования стегосообщения могут быть различны. Стеганографическое преобразование можно трактовать как возмущение (или погрешность) Δf исходных данных (контейнера $f(x,y)$). Очевидно, в общем случае

$$\Delta f = s(x,y) - f(x,y),$$

$$F(f(x,y), z(x,y)) = f(x,y) + \Delta f \text{ для } (x,y) \in [0,1]\times[0,1].$$

Если стегосообщение формируется аддитивным способом, то $\Delta f = z(x,y)$.

Везде далее будем обозначать область $\Pi = [0,1]\times[0,1]$.

При пересылке сформированного стегосообщения даже в случае отсутствия преобразований атакующим, канал связи внесет дополнительные искажения в стегосообщение, т.е. погрешность исходных данных возрастет. Для оценки погрешности секретного сообщения на приемном конце нужно оценить степень возмущения решения задачи о детектировании погруженного дополнительного сообщения при малом возмущении ее входных данных. Если задача окажется чувствительной [3], то приемлемую степень точности декодирования обеспечить будет просто невозможно.

При численном решении любой задачи важным является то, как возмущения входных данных скажутся на возмущении результата. Пусть ξ - входные данные для некоторой задачи, результатом которой является $\phi(\xi)$; $\overline{\xi}$ - возмущенные входные данные, а решение задачи, полученное для этих входных данных – это $\phi(\overline{\xi})$. Числом обусловленности рассматриваемой задачи называется [4] величина, определяемая соотношением:

$$\overline{\lim_{\xi\to\overline{\xi}}} \frac{\textit{расстояние между } \phi(\xi) \textit{ и } \phi(\overline{\xi})}{\textit{расстояние между } \xi \textit{ и } \overline{\xi}} \qquad (2)$$

Расстояния, фигурирующие в формуле (2), определяются введением соответствующих метрик в пространствах входных данных и результатов. Очевидно, чем меньше число обусловленности, тем меньше возмущение результата зависит от возмущения входных данных, тем меньше чувствительность задачи, т.е. при малом числе обусловленности задача окажется нечувствительной к погрешностям исходных данных.

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 рассматриваемой задачи.

Пусть $s(x,y)$ – некоторая дифференцируемая функция вида (1), определяющая результирующее изображение после погружения ДИ, а через $a\lg or(x,y)$ будем обозначать непосредственно выбранный численный алгоритм для вычисления $s(x,y)$. Необходимо отметить, что результат $a\lg or(x,y)$ содержит вычислительную погрешность. Предположим, что $a\lg or(x,y)$ является обратно устойчивым алгоритмом для $s(x,y)$ [2], тогда возможно представление:

$$a\lg or(x,y) = s(x+\delta x, y+\delta y),$$

где $(\delta x, \delta y)$ - возмущение (x,y), а сама функция $s(x,y)$ в достаточно малой окрестности (x,y) удовлетворяет соотношению [5]:

$$s(x+\delta x, y+\delta y) = s(x,y) + \frac{\partial s(x,y)}{\partial x}\delta x + \frac{\partial s(x,y)}{\partial y}\delta y + \bar{o}\left(\sqrt{\delta x^2 + \delta y^2}\right), \text{ когда } \sqrt{\delta x^2 + \delta y^2} \to 0.$$

Тогда

$$|s(x+\delta x, y+\delta y) - s(x,y)| \approx \left|\frac{\partial s(x,y)}{\partial x}\delta x + \frac{\partial s(x,y)}{\partial y}\delta y\right| = |(grad\, s(x,y), (\delta x, \delta y))|, \quad (3)$$

где $grad\ s(x,y)$ - вектор-градиент функции $s(x,y)$ в точке (x,y). Используя в правой части (3) неравенство Коши – Буняковского, получим:

$$|(grad\, s(x,y), (\delta x, \delta y))| \le \|grad\ s(x,y)\| \, \|(\delta x, \delta y)\|.$$

Откуда

$$|s(x+\delta x, y+\delta y) - s(x,y)| \approx \|grad\ s(x,y)\| \, \|(\delta x, \delta y)\|$$

В качестве абсолютного числа обусловленности, как меры чувствительности задачи вычисления $s(x,y)$ к возмущениям исходных данных, здесь может рассматриваться $\|grad\ s(x,y)\|$. Тогда для погрешности становится возможной оценка:

$$|a\lg or(x,y) - s(x,y)| = |s(x+\delta x, y+\delta y) - s(x,y)| \approx \|grad\ s(x,y)\| \, \|(\delta x, \delta y)\| \quad (4)$$

Как видно из (4), абсолютная погрешность результата в каждой точке зависит от абсолютного числа обусловленности функции $s(x,y)$ в этой точке. При обратной устойчивости $a\lg or(x,y)$ 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 [2] $\|(\delta x, \delta y)\|$, результирующая погрешность может оказаться неприемлемо большой. Из всего вышесказанного вытекает справедливость следующего утверждения:

Утверждение. 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 $\|grad\ s(x,y)\|$, в любой точке (x,y) из области Π невелико.

Очевидно, утверждение требует ограниченность $\|grad\ s(x,y)\|$ на всей области Π, причем мажорирующая константа для $\|grad\ s(x,y)\|$ не должна быть большой.

Сложность получения оценки значения $\|grad\ s(x,y)\|$ зависит от самой функции $s(x,y)$. Однако важную роль здесь играет тот факт, что функция $s(x,y)$ определена на компактном множестве [5]. Действительно, предположим, что $s(x,y) \in C^1(\Pi)$, т.е. все частные производные функции $s(x,y)$ непрерывны на Π, тогда по теореме Вейерштрасса [5] $s'_x(x,y)$, $s'_y(x,y)$ ограничены на этом компакте, а, значит, найдется такая постоянная величина $M \ge 0$, что для любой точки $(x,y) \in \Pi$ будет выполняться соотношение:

$\|grad\ s(x,y)\| \le M$. Если величина M является приемлемой для рассматриваемой задачи, то результирующая погрешность будет небольшой.

Все вышесказанное для оценки $\|grad\ s(x,y)\|$ будет верно и в том случае, если частные производные $s(x,y)$ будут просто ограничены в области Π.

Метод пересылки и декодирования ДИ

Компьютерное представление монохромного изображения – это двумерный массив неотрицательных целых чисел из ограниченного диапазона (256 градаций серого), каждый элемент которого отвечает пикселю изображения. Далее в качестве ОС будем рассматривать квадратную $n \times n$ матрицу F. Стеганографическое преобразование изображения будет иметь характер матричных операций [6].

В качестве ДИ выступает числовая последовательность, содержащая n элементов, принадлежащих множеству $\{-1, 1\}$. Последовательность может содержать и менее n элементов, тогда она дополняется незначащими элементами до нужной длины. Предполагается, что матрица F невырожденная, т.е. $\det F \neq 0$. Обозначим пересылаемое сообщение x. Вычислим произведение

$$b = F\,x,$$

представляющее из себя вектор длины n (заметим, что при предположении отсутствия ошибок машинной арифметики, вектор x является точным решение системы линейных алгебраических уравнений $F\,x = b$). Полученный вектор b кодируется или не кодируется и погружается в F вместо несущего нужную информацию x. Декодирование нужной информации адресатом будет включать в себя два этапа. Сначала при получении заполненного контейнера, подвергшегося возмущениям при пересылке, каким-либо известным устойчивым алгоритмом декодируется содержащийся в нем вектор b (получаем возмущенный вектор b_B), а выделение нужного информационного x будет происходить на втором этапе при решении неоднородной системы линейных алгебраических уравнений

$$F_B\, x_{np} = b_B\ . \tag{5}$$

Здесь $F_B = F + \delta F, b_B = b + \delta b$, где $\delta F, \delta b$ - возмущения входных данных: матрицы системы F и вектора правой части b соответственно. Нужно отметить, что, вообще говоря, источниками возмущения являются не только возможные атаки в канале связи при пересылке, но и работа алгоритма декодирования b. Ясно, что $x_{np} \neq x$.

Очевидно, идти по предлагаемому пути декодирования ДИ имеет смысл только в том случае, если такой способ декодирования, включающий дополнительный этап в виде решения СЛАУ, даст меньшую погрешность результирующего информационного вектора x, чем его непосредственная пересылка на месте вектора b при абсолютно аналогичных условиях. Ниже будут обоснованы достаточные условия, удовлетворение которым матрицы основного сообщения позволит утверждать, что предлагаемый метод, который в дальнейшем будем называть SISTEMA, действительно обеспечивает дополнительную «защиту» информационного вектора по сравнению с одноэтапным декодированием.

Оценки погрешности декодирования ДИ предлагаемым методом

Пусть $x_{np} = x + \delta x$, где $\|\delta x\| = \|x_{np} - x\|$ - **абсолютная погрешность** x_{np}. Тогда СЛАУ (5) представляется в виде:

$$\left(F+\delta F\right)\left(x+\delta x\right)=b+\delta b\ ,$$

откуда

$$\delta x=F^{-1}\left(\delta b-\delta F\ x_{пр}\right). \tag{6}$$

Учитывая элементарные свойства нормы и невырожденность матрицы F, из (6) получаем:

$$\left\|\delta x\right\|=\left\|F^{-1}\left(\delta b-\delta F\ x_{пр}\right)\right\|\le\left\|F^{-1}\right\|\left(\left\|\delta b\right\|+\left\|\delta F\right\|\left\|x_{пр}\right\|\right)=\left\|F^{-1}\right\|\left\|F\right\|\left(\frac{\left\|\delta b\right\|}{\left\|F\right\|}+\frac{\left\|\delta F\right\|\left\|x_{пр}\right\|}{\left\|F\right\|}\right).$$

Тогда

$$\frac{\left\|\delta x\right\|}{\left\|x_{пр}\right\|}\le\left\|F^{-1}\right\|\left\|F\right\|\left(\frac{\left\|\delta b\right\|}{\left\|F\right\|\left\|x_{пр}\right\|}+\frac{\left\|\delta F\right\|}{\left\|F\right\|}\right). \tag{7}$$

Здесь относительная погрешность результата сравнивается с относительным изменением входных данных через величину $cond\left(F\right)=\left\|F^{-1}\right\|\left\|F\right\|$, **число обусловленности** невырожденной матрицы F в задаче о решении СЛАУ, которое, как видно из (7), является мерой чувствительности задачи о решении системы к погрешности в исходных данных. Таким образом, если число обусловленности матрицы ОС мало (тогда матрица называется хорошо обусловленной), задача декодирования ДИ на втором этапе предложенного метода является нечувствительной к погрешностям в исходных данных, малые возмущения на входе не изменят заметно результат, т.е. $x_{пр}\approx x$, откуда очевидно вытекает, что в качестве контейнера для обеспечения этой нечувствительности нужно использовать изображение, матрица которого является хорошо обусловленной.

На практике оценка ошибки (7) часто оказывается чересчур «пессимистичной». Будем обозначать $\left|F\right|$ **матрицу, составленную из абсолютных значений элементов** F, а неравенства типа $\left|F\right|\le\left|G\right|$ **следует далее понимать как системы покомпонентных неравенств:** $\left|f_{ij}\right|\le\left|g_{ij}\right|$ **для всех** $i,j=1,\ldots,n$. Аналогичные обозначения будем использовать и для векторов. На практике часто можно добиться того, чтобы δF и δb удовлетворяли оценкам :

$$\left|\delta F\right|\le\varepsilon\left|F\right|,\quad\left|\delta b\right|\le\varepsilon\left|b\right|$$

где ε - некоторое малое число [2], [4]. Из (6) получаем:

$$\left|\delta x\right|=\left|F^{-1}\left(\delta b-\delta F\,x_{пр}\right)\right|\le\left|F^{-1}\right|\left(\left|\delta b\right|+\left|\delta F\right|\left|x_{пр}\right|\right)\le$$

$$\le\left|F^{-1}\right|\left(\varepsilon\left|b\right|+\varepsilon\left|F\right|\left|x_{пр}\right|\right)=\varepsilon\left(\left|F^{-1}\right|\right)\left(\left|b\right|+\left|F\right|\left|x_{пр}\right|\right). \tag{8}$$

Предположим, что используемая векторная норма обладает свойством:

$$\left\|\left|z\right|\right\|=\left\|z\right\|,$$

(такими будут, например, max-норма, евклидова норма), тогда из (8) получаем:

$$\|\delta x\| \le \varepsilon \left\| \left|F^{-1}\right| \left(|F| \left|x_{np}\right| + |b| \right) \right\|. \qquad (9)$$

Если возмущению подверглась только матрица системы F, а вектор правой части остался неизменным ($\delta b = 0$), тогда из (8) вытекает оценка, подобная (9), имеющая вид:

$$\|\delta x\| \le \varepsilon \left\| \left|F^{-1}\right| |F| \right\| \left\|x_{np}\right\|.$$

Тогда для относительной погрешности полученного x_{np} имеем:

$$\frac{\|\delta x\|}{\left\|x_{np}\right\|} \le \varepsilon \left\| \left|F^{-1}\right| |F| \right\|. \qquad (10)$$

Величина $k(F) = \left\| \left|F^{-1}\right| |F| \right\|$ **называется относительным покомпонентным числом** обусловленности матрицы F или числом обусловленности Скила [4] и также, как и $cond(F)$, позволяет оценить относительную погрешность результата через относительную погрешность входных данных ε. Покажем, что $k(F)$ может использоваться для оценки погрешности результата через возмущения данных и в случае, если $\delta b \ne 0$. Действительно, из (9) получаем:

$$\|\delta x\| \le \varepsilon \left\| \left|F^{-1}\right| \left(|F| \left|x_{np}\right| + |b| \right) \right\| \le \varepsilon \left\| \left|F^{-1}\right| \left(|F| \left|x_{np}\right| + \left|F\left(x_{np} - \delta x\right)\right| \right) \right\| \le$$

$$\le \varepsilon \left(\left\| |F| \left|F^{-1}\right| \left(\left|x_{np}\right| + \left|x_{np}\right| + |\delta x| \right) \right\| \right) \le 3\varepsilon \left\| |F| \left|F^{-1}\right| \right\| \left\|x_{np}\right\|$$

Откуда

$$\frac{\|\delta x\|}{\left\|x_{np}\right\|} \le 3\varepsilon \left\| |F| \left|F^{-1}\right| \right\|. \qquad (11)$$

На практике оценка (10) может быть значительно меньше аналогичной оценки (7) [2], [4]. Это приводит к тому, что СЛАУ даже с большим $cond(F)$ может решаться с высокой точностью.

Из оценок (10) - (11) и предположения об устойчивости метода декодирования вектора b, сделанного выше, вытекает истинность следующей теоремы.

Теорема. Пусть матрица изображения, используемого в качестве ОС, имеет малое число обусловленности Скила. Тогда метод SISTEMA является устойчивым.

Практический метод обеспечения малого числа обусловленности Скила матрицы ОС

Оценка числа обусловленности Скила для матрицы изображения ОС является, очевидно, ключевым моментом в вопросе выбора подходящего для пересылки ДИ предложенным методом контейнера. Непосредственное вычисление числа обусловленности Скила для матриц большой размерности – процесс дорогостоящий. Конечно, если матрица F диагональная, то без каких-либо дополнительных исследований мы можем утверждать, что SISTEMA будет устойчив. Аналогичную картину можно ожидать и в случае, когда для элементов F выполняется условие [2]:

$$|f_{ii}| >> \sum_{j=1, j\neq i}^{n} |f_{ij}|, \; i = 1,...,n. \tag{12}$$

Но реальные изображения редко удовлетворяют свойству (12).

Ниже предлагается метод, позволяющий использовать практически любое изображение в качестве ОС в методе SISTEMA, независимо от его реального числа обусловленности. Не изменяя матрицу изображения явно, а лишь моделируя диагональное преобладание в ней виртуально, обеспечивается малость числа обусловленности Скила смоделированной по F матрицы.

Пусть D - диагональная матрица размерности $n \times n$, элементы которой определяются по формулам:

$$d_{ii} = m \sum_{j=1}^{n} |f_{ij}|, \quad i = \overline{1, n}. \tag{13}$$

Здесь f_{ij}, $i, j = \overline{1,n}$, - **элементы матрицы** F исходного изображения, m - натуральное число, выбор которого должен обеспечить для матрицы $F + D$ наличие свойст, близких к (12). Однако, значение m не может быть слишком большим, т.к. вектор b для используемой СЛАУ будем вычислять в соответствии с выражением:

$$b = (F + D)\, x .$$

Реально матрица F не меняется, т.е. исходное основное сообщение не «портится», а виртуально построенная для нее матрица $F + D$ очевидно имеет диагональное преобладание. Алгоритм (13) построения матрицы D известен декодеру. Получая стегосообщение, для которого ОС - это матрица F_B, на втором этапе декодирования для получения нужной информации x решается СЛАУ

$$\left(F_B + D'\right)x_{np} = b_B , \tag{14}$$

где D' - диагональная матрица, которая формируется декодером по полученной возмущенной матрице F_B:

$$d'_{ii} = m \sum_{j=1}^{n} |f_{B\,ij}|, \quad i = \overline{1, n},$$

где $f_{B\,ij}$ - элементы матрицы F_B. Очевидно, $\det\left(F_B + D'\right) \neq 0$.

Свойства матрицы системы (14) близки к свойствам (12), а потому матрица $F_B + D'$ не может иметь большое число обусловленности Скила, что дает возможность ожидать, что решение СЛАУ (14) $x_{np} \approx x$, δx достаточно мало. Таким образом, практический метод введения виртуальной диагонали в матрицу реального изображения обеспечивает хорошую обусловленность Скила матрицы СЛАУ для декодирования ДИ и устойчивость SISTEMA практически для любого ОС в предположении устойчивости алгоритма декодирования b.

Заключение

Предложенный новый подход к организации пересылки и декодирования ДИ обеспечивает повышение устойчивости пересылаемой информации к различным возмущениям при малом числе обусловленности Скила матрицы ОС по сравнению с тем, если бы пересылка необходимой информации производилась непосредственно, что подтверждается проведенным вычислительным экспериментом, результаты которого в настоящий момент готовятся к печати. Моделирование виртуального диагонального преобладания для матрицы ОС обеспечивает устойчивость при решении рассмотренной выше СЛАУ, что позволяет использовать в качестве контейнера в предложенном методе SISTEMA произвольное изображение, никак не изменяя его явно.

Открытым пока является вопрос организации непосредственного решения СЛАУ. Использование стандартных методов является здесь нежелательным в силу большой размерности матрицы изображения и специфики ее вида.

Список литературы

1. *В.А. Хорошко, А.А. Чекатков.* Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с.

2. *Дж. Деммель.* Вычислительная линейная алгебра. – М. Мир, 2001. – 430 с.

3. *Бахвалов Н.С., Жидков Н.П., Кобельков Г.М.* Численные методы.- М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.

4. *R.D. Skeel.* «Scaling for numerical stability in Gaussian elimination». Journal of the ACM, 26: 494-526, 1979.

5. *Фихтенгольц Г.М.* Курс дифференциального и интегрального исчисления. Т.1.- М.: Наука, 1969. – 608 с.

6. *Ф.Р.Гантмахер.* Теория матриц.- М.: Наука, 1988. – 552 с.

Поступила 23.11.2006 г.

УДК 681.3.064 **Куржеевский И.В., Лакаева Е.А.**

АЛГОРИТМ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ ВСТРАИВАЕМЫХ В ИЗОБРАЖЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Надежная защита информации от несанкционированного доступа является более чем актуальной. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии. Слово стеганография в переводе с греческого буквально означает тайнопись.

Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде, а также средств реализации этих методов. К ней можно отнести огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные (скрытые) каналы, средства связи с плавающими частотами, голография.

В настоящее время развитие средств вычислительной техники дало толчок развитию компьютерной стеганографии. Сообщения встраивают в цифровые данные, как правило, имеющие аналоговую природу – речь, аудиозаписи, изображения, видео и даже текстовые файлы и исполняемые файлы программ.

Можно выделить две причины популярности исследований в области компьютерной стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытие факта передачи информации), вторая – еще более многочисленные исследования в области так называемых