УДК 004.056.5: 518: 512.624.3

ОЦЕНКА ЧУВСТВИТЕЛЬНОСТИ СТЕГОСООБЩЕНИЙ К ВОЗМУЩАЮЩИМ ВОЗДЕЙСТВИЯМ

А.А. КОБОЗЕВА, Е.В. НАРИМАНОВА

Разработана математическая база, и на ее основе создан метод оценки чувствительности стегосообщений к возмущающим воздействиям, независимо от используемого стеганографического алгоритма и области погружения секретной информации, позволяющий формализовать процесс решения задачи о выборе для заданого секретного сообщения такого контейнера, которому будет соответствовать наименее чувствительное к возмущающим воздействиям стегосообщение.

ВВЕДЕНИЕ

В настоящее время во всем мире возросла актуальность разработки новых и совершенствования существующих методов защиты информации, представленной в цифровом виде, среди которых важное место занимают методы криптографии и стеганографии.

Целью криптографии [1] является сокрытие содержимого секретных сообщений путем их шифрования. Однако бывают ситуации, когда применение криптографических методов не решает возникающих проблем. Например, шифрование документов во многих странах запрещено на законодательном уровне. К процедурам идентификации нередко предъявляется требование скрытности. Одним из выходов является использование методов компьютерной стеганографии [2,3]. Стеганографирование может осуществляться различными способами, общей чертой которых является то, что секретное сообщение (дополнительная информация (ДИ)) погружается в некоторый объект (основное сообщение (ОС)), не привлекающий внимания, и затем открыто пересылается по каналу связи адресату или хранится в таком виде. Итак, в стеганографии наличие скрытой связи остается незаметным. Однако не стоит рассматривать стеганографию и криптографию как альтернативу одна другой — это две стороны одной медали, и эффективность их только возрастает от совместного использования [4].

Процесс погружения ДИ в ОС (контейнер) будем называть *стегопреобразованием* ОС, а результат стегопреобразования — *стегосообщением.*

Одно из основных требований к любому стегосообщению с целью обеспечения эффективного декодирования секретной информации — его нечувствительность к возмущающим воздействиям [3, 5, 6]. Стегосообщение будем называть *чувствительным* [7], если даже незначительные возмущающие воздействия, которым оно подвергается, способны привести к большому росту количества ошибок при декодировании ДИ, и *нечувствительным* в противном случае.

© *А.А. Кобозева, Е.В. Нариманова*, 2008

Наибольшего развития достигло практическое приложение стеганографии, которое часто не имеет строгого теоретического обоснования. До сих пор в открытой печати не представлен общий математический подход, позволяющий оценивать чувствительность стегосообщения, а также проводить априорное сравнение различных стегосообщений с точки зрения их чувствительности к возмущающим воздействиям.

ПОСТАНОВКА ЗАДАЧИ

Цель настоящей работы — создание на основе матричного анализа [8,9] и теории возмущений [10,11] математической базы, дающей возможность оценить чувствительность стегосообщений к возмущающим воздействиям, который бы не зависел от используемого стеганографического алгоритма и области погружения ДИ, а также позволял проводить априорное сравнение чувствительностей различных стегосообщений. Этот метод даст возможность формализовать процесс решения чрезвычайно важной для стеганографии задачи о выборе для заданного секретного сообщения такого контейнера, которому будет соответствовать наименее чувствительное к возмущающим воздействиям стегосообщение.

СТЕГОПРЕОБРАЗОВАНИЕ КАК ВОЗМУЩЕНИЕ СПЕКТРА И СОБСТВЕННЫХ ВЕКТОРОВ МАТРИЦЫ ОСНОВНОГО СООБЩЕНИЯ

В качестве ОС рассмотрим изображение в градациях серого, матрицу которого обозначим F.

Погружение ДИ в ОС, независимо от способа и области этого погружения, можно представить как возмущение ΔF матрицы F. Тогда матрица стегосообщения $\overline{F}$ удовлетворяет соотношению

$$\overline{F} = F + \Delta F , \qquad (1)$$

где $\Delta F = f(F)$, т.е. ΔF является некоторой функцией матрицы контейнера F.

Из формулы (1), дающей матричное представление для стегопреобразования, вытекает

Утверждение 1. Произвольное стегопреобразование можно представить эквивалентным образом в виде аддитивного погружения некоторой информации в пространственной области.

Любые преобразования, которые производятся над стегосообщением, будем рассматривать как дополнительные возмущения матрицы ОС F. Очевидно, имеет место

Утверждение 2. Стегопреобразование исходного ОС, а также любые преобразования стегосообщения при его транспортировке или хранении, включая активные атакующие действия, представимы в виде элементарных матричных операций [9].

Поскольку математической моделью ОС является матрица, а все преобразования над ОС могут быть представлены в эквивалентном матричном виде, то в качестве набора параметров, однозначно определяющих и всесторонне характеризующих любое ОС, можно использовать множество сингулярных чисел и сингулярных векторов матрицы контейнера (или ее спектр) и множество собственных векторов (СВ) [11] определенного вида. Если бы матрица F ОС оказалась симметричной, то предпочтение безоговорочно следовало бы отдать второму набору параметров, так как

1) построение спектрального разложения симметричной матрицы имеет преимущества в вычислительном смысле по сравнению с построением сингулярного разложения для матрицы произвольной структуры той же размерности и того же уровня заполненности [11,12];

2) собственные значения (СЗ) симметричной матрицы являются хорошо обусловленными [13], т.е.

$$\max_{1\le j\le n}\left|\lambda_j(F)-\lambda_j(F+\Delta F)\right|\le\left\|\Delta F\right\|_2, \qquad (2)$$

где $\lambda_j(\bullet)$ — СЗ соответствующей матрицы; $\left\|\bullet\right\|_2$ — спектральная матричная норма (СМН) [11], т.е. задача вычисления СЗ симметричной матрицы не является чувствительной к возмущениям в исходных данных [11], чего нельзя утверждать в общем случае для несимметричных матриц.

Однако, как правило, матрица ОС не удовлетворяет свойству $F=F^T$. Поставим в соответствие F две симметричные матрицы A, B той же размерности по следующему правилу:

$$F=\begin{pmatrix} a_{11}\ a_{12}\ a_{13}\dots a_{1n}\\ a_{21}\ a_{22}\ a_{23}\dots a_{2n}\\ a_{31}\ a_{32}\ a_{33}\dots a_{3n}\\ \dots\dots\dots\dots\dots\\ a_{n1}\ a_{n2}\ a_{n3}\dots a_{nn}\end{pmatrix}\to A=\begin{pmatrix} a_{11}\ a_{12}\ a_{13}\dots a_{1n}\\ a_{12}\ a_{22}\ a_{23}\dots a_{2n}\\ a_{13}\ a_{23}\ a_{33}\dots a_{3n}\\ \dots\dots\dots\dots\dots\\ a_{1n}\ a_{2n}\ a_{3n}\dots a_{nn}\end{pmatrix}, B=\begin{pmatrix} a_{11}\ a_{21}\ a_{31}\dots a_{n1}\\ a_{21}\ a_{22}\ a_{32}\dots a_{n2}\\ a_{31}\ a_{32}\ a_{33}\dots a_{n3}\\ \dots\dots\dots\dots\dots\\ a_{n1}\ a_{n2}\ a_{n3}\dots a_{nn}\end{pmatrix}, \qquad (3)$$

которые будем рассматривать ниже как матрицы ОС. При встраивании ДИ в исходный контейнер, это стегопреобразование представляется в виде погружения в верхний (нижний) треугольник матрицы $A(B)$ с последующим симметричным отражением результата относительной главной диагонали $A(B)$. Пусть итогом такого погружения есть симметричные матрицы $\overline{A}$ и $\overline{B}$. При окончательном формировании матрицы стегосообщения используется верхний треугольник матрицы $\overline{A}$ и нижний треугольник матрицы $\overline{B}$. Применение такого подхода, дающего возможность рассматривать матрицу ОС как симметричную и поэтому использовать для ее описания спектр и соответствующие СВ, было предложено автором в работе [14].

Пусть E — матрица произвольного возмущения, которому подвергается ОС (стегосообщение). В общем случае $E\ne(E)^T$. Матрице E поставим в соответствие две симметричные матрицы той же размерности, используя правило (3) и рассматривая матрицу, отвечающую верхнему (нижнему) треугольнику E, как возмущающую для контейнера (стегосообщения), полученного на основе $A(B)$, что дает принципиальную возможность матрицу произвольного возмущения также рассматривать как симметричную.

Пусть A — произвольная симметричная $n \times n$-матрица, где $a_{ij} \in R$, $i, j = \overline{1, n}$ с СЗ $\lambda_i \in R$, $i = \overline{1, n}$, с ортонормированными СВ u_i, $i = \overline{1, n}$, т.е.

$$A = U \Lambda U^T \tag{4}$$

— спектральное разложение (СР) матрицы A [11] (здесь $\Lambda = \mathrm{diag}(\lambda_1, ..., \lambda_n)$, $U = [u_1, ..., u_n]$), которое в общем случае определяется неоднозначно. СР (4) назовем *нормальным*, если элементы матрицы Λ удовлетворяют соотношению $|\lambda_1| \geq ... \geq |\lambda_n|$, а СВ u_i, $i = \overline{1, n}$, *лексикографически положительны*, т.е. первая ненулевая компонента каждого вектора положительна.

Теорема 1. Пусть A — невырожденная симметричная $n \times n$-матрица, модули СЗ которой попарно различны. Тогда для нее существует *единственное* нормальное СР.

Доказательство следует из существования разложения (4) для произвольной симметричной матрицы A и лексикографической положительности СВ, которая в случае попарного различия СЗ A и обеспечит единственность нормального СР.

Далее будем считать, что все рассматриваемые ниже матрицы удовлетворяют условию теоремы 1.

Любое преобразование, в частности, стегопреобразование матрицы ОС, определенным образом возмутит ее спектр и (или) СВ, однозначно определяемые нормальным СР. В силу этого имеет место утверждение

Утверждение 3. Любое стегопреобразование эквивалентным образом представимо в виде возмущения спектра и (или) собственных векторов матрицы ОС, определяемых нормальным СР.

Стегопреобразование ОС, а также возмущающие воздействия, которым подвергается стегосообщение, должны обеспечивать надежность его восприятия, т.е. так возмутить матрицу ОС, чтобы зрительно это возмущение оказалось незаметным. Если E — это матрица возмущения ОС или стегосообщения, то, очевидно, любая ее норма $\|E\|$ не может быть бесконечно большой, так как в этом случае достоверным событием окажется нарушение надежности восприятия.

При $\|E\| \to 0$ вероятность обеспечения надежности восприятия будет стремиться к единице для каждого ОС [10]. Будем считать, что чем меньше норма матрицы возмущения, тем больше вероятность обеспечения надежности восприятия стегосообщения. Данная гипотеза подтверждается вычислительным экспериментом, но его описание выходит за рамки настоящей работы. Ниже рассматриваются такие возмущения, воздействующие на ОС и стегосообщение, которые обеспечивают надежность восприятия — *малые возмущающие воздействия*.

В силу соотношения (2) все СЗ симметричной матрицы ОС являются нечувствительными [11] к рассматриваемым возмущающим воздействиям, независимо от того, чувствительным или нечувствительным окажется полученное стегосообщение, что позволяет для оценки чувствительности стегосообщения анализировать лишь возмущения СВ при стегопреобразовании матрицы ОС. Поэтому и согласно утверждению 3 погруженную информацию будем представлять в виде совокупности возмущений СВ матрицы ОС. Для $n = 3$ геометрическая интерпретация погруженной ДИ дана на рис. 1.

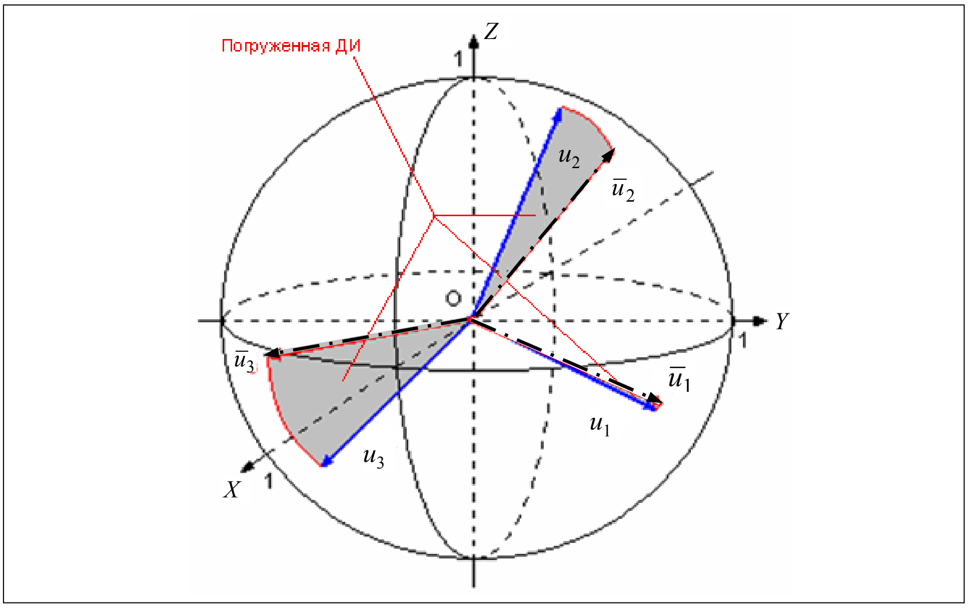

Рис. 1. Геометрическая интерпретация ДИ: ⟶ — СВ матрицы контейнера; —·—·— — возмущенные стегопреобразованием собственные векторы

СВЯЗЬ ЧУВСТВИТЕЛЬНОСТИ СТЕГОСООБЩЕНИЯ И ВОЗМУЩЕНИЙ СОБСТВЕННЫХ ВЕКТОРОВ МАТРИЦЫ КОНТЕЙНЕРА

Пусть A — произвольная симметричная матрица, удовлетворяющая условиям теоремы 1, рассматриваемая как матрица контейнера. Назовем *абсолютной отделенностью* СЗ λ_i матрицы A число, определяемое в соответствии с формулой

$$\mathrm{gap}_{\mathrm{abs}}(i, A) = \min_{i \neq j} \left| |\lambda_j| - |\lambda_i| \right|.$$

Теорема 2. Достаточным условием обеспечения малой чувствительности стегосообщения к возмущающим воздействиям является соответствие возмущенных при стегопреобразовании ОС собственных векторов собственным значениям матрицы стегосообщения, имеющим большие абсолютные отделенности.

Доказательство. При погружении ДИ в контейнер СВ матрицы A ОС возмутятся, отклонившись от первоначального положения на некоторые углы (рис.1), что происходит всегда, если только алгоритм погружения ДИ не базируется на непосредственной модификации лишь СЗ матрицы ОС, как, например, в работе [15]. Этот случай требует отдельного рассмотрения, которое не проводится в настоящей работе. Совокупность возмущений СВ является представлением для погруженной информации. Чувствительность полученного стегосообщения будет определяться чувствительностью возмущенных при стегопреобразовании СВ матрицы A. Как известно [11], СВ является *чувствительным*, если даже малое возмущающее воздействие может привести к значительному возмущению вектора, т.е. значительному углу его отклонения от первоначального положения. Очевидно, чтобы сохранить неизменной погруженную ДИ при возмущающем воздействии на стегосообщение, отклонения СВ, возникшие в результате стегопреобразования, должны остаться неизменными.

Пусть $\overline{A}$ — симметричная матрица стегосообщения, нормальное СР которой в соответствии с формулой (4) представляется в виде $\overline{A} = \overline{U}\overline{\Lambda}\overline{U}^T$; E — некоторое возмущение $\overline{A}$, $E = E^T$; $\overline{A} + E = \overline{\overline{U}}\overline{\overline{\Lambda}}\overline{\overline{U}}^T$ — нормальное СР $\overline{A} + E$; $\overline{u}_i$, $\overline{\overline{u}}_i$ — нормированные СВ $\overline{A}$ и $\overline{A} + E$ соответственно, отвечающие i-му СЗ, а θ_i — угол между ними. Легко показать [11], что

$$\sin\theta_i \le \frac{2\|E\|_2}{\operatorname{gap}_{\text{abs}}(i, \overline{A})}. \qquad (5)$$

В соответствии с (5) СВ, возмущенные при стегопреобразовании контейнера, а значит, и стегосообщение в целом, будут нечувствительными к возмущающим воздействиям, если соответствующие СЗ матрицы $\overline{A}$ имеют достаточно большие абсолютные отделенности, причем, чем больше $\operatorname{gap}_{\text{abs}}(i, \overline{A})$, тем менее чувствительным к возмущениям будет соответствующий СВ. Таким образом, абсолютная отделенность СЗ является мерой чувствительности СВ к возмущающим воздействиям, а абсолютные отделенности СЗ, соответствующих возмущенным при стегопреобразовании СВ, определяют чувствительность полученного стегосообщения. Стегосообщение будет наименее чувствительным к возмущающим воздействиям, если стегопреобразование возмутит СВ, соответствующие СЗ матрицы стегосообщения, которые имеют наибольшие абсолютные отделенности. Более того, как показывает вычислительный эксперимент, наибольшие абсолютные отделенности СЗ, присутствующих в спектре матрицы стегосообщения, таковы, что они обеспечивают *нечувствительность* стегосообщения в указанном случае (углы поворота соответствующих СВ составляют, как правило, доли секунды).

Следствие 1. Если возмущенные в результате стегопреобразования ОС СВ соответствуют СЗ матрицы стегосообщения с малыми абсолютными отделенностями, то полученное стегосообщение оказывается *чувствительным* к возмущающим воздействиям, что приводит к недостаточной эффективности декодирования ДИ.

Как следует из (2), абсолютные отделенности СЗ матриц $\overline{A}$ и A незначительно отличаются друг от друга. Откуда вытекает

Следствие 2. Достаточным условием обеспечения малой чувствительности стегосообщения к возмущениям является соответствие возмущенных при стегопреобразовании ОС СВ собственным значениям матрицы ОС, имеющим большие абсолютные отделенности.

Из всего сказанного следует вывод:

Чувствительность стегосообщения к возмущающим воздействиям определяется возмущениями СВ матрицы ОС при стегопреобразовании. Исходя из значений этих возмущений и абсолютных отделенностей соответствующих СЗ, можно сделать качественные априорные оценки чувствительности стегосообщения к возмущающим воздействиям.

Для получения количественной оценки чувствительности стегосообщения вернемся к соотношению (5). Заметим, что если правая часть (5) превзойдет единицу, т.е. $\|E\|_2 \ge \frac{\text{gap}_{\text{abs}}(i, \overline{A})}{2}$, то оценка возмущения СВ приобретет вид $\sin\theta_i \le 1$, превращаясь в тривиальную, и сделать заключение о реальной чувствительности такого вектора не представляется возможным.

Определение 1. Будем говорить, что СЗ λ_i имеет *достаточную (недостаточную) абсолютную отделенность по отношению к возмущению* E, если $\|E\|_2 < \frac{\text{gap}_{\text{abs}}(i, \overline{A})}{2}$ $\left(\|E\|_2 \ge \frac{\text{gap}_{\text{abs}}(i, \overline{A})}{2}\right)$.

Определение 2. Собственные векторы, отвечающие СЗ с достаточной (недостаточной) абсолютной отделенностью по отношению к возмущению E, назовем *защищенными (незащищенными) от рассматриваемого возмущения*.

Заметим, что только для защищенных СВ имеется потенциальная возможность численно оценить возмущение при помощи неравенства (5). СВ, отвечающие СЗ с большими (максимальными) абсолютными отделенностями, являются защищенными от любого из рассматриваемых возмущений.

Определение 3. ДИ, результатом погружения которой явилось возмущение защищенных СВ, будем называть *дополнительной информацией, защищенной от возмущения* E (ЗИ).

Далее будем считать, что при увеличении величины угла отклонения СВ при стегопреобразовании увеличивается и количество ДИ, которая хранится в возмущении этого вектора. Собственные векторы «распределяют между собой» погруженную ДИ. Конечно, такое допущение будет не совсем оправданным, если алгоритм погружения связан с непосредственной модификацией СВ, например, с изменением знаков их определенных компонент, как, например, в работе [14]. Однако это лишь незначительно сужает область допущения и является предметом исследования другой работы автора.

Из сделанного выше допущения следует, что стегосообщение тем менее чувствительно, чем большему возмущению при стегопреобразовании подверглись СВ, отвечающие СЗ с максимальными абсолютными отделенностями, чем бóльшая «часть» ДИ является защищенной от возмущающих воздействий.

Количественной оценкой чувствительности стегосообщения будем считать объем защищенной в нем ДИ, определяемый с учетом возмущений защищенных СВ и абсолютных отделенностей соответствующих СЗ.

МЕТОД СРАВНИТЕЛЬНОЙ ОЦЕНКИ ЧУВСТВИТЕЛЬНОСТИ СТЕГОСООБЩЕНИЙ К ВОЗМУЩАЮЩИМ ВОЗДЕЙСТВИЯМ И ЕГО ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ В ЗАДАЧЕ О ВЫБОРЕ КОНТЕЙНЕРА

Предлагаемый метод демонстрируется при решении задачи о выборе ОС из имеющегося конечного множества контейнеров для заданного секретного сообщения с целью обеспечения наименьшей чувствительности получаемого стегосообщения. Метод основывается на исследовании возмущений СВ матриц ОС вследствие стегопреобразования на основании нормальных СР исходных матриц и матриц стегосообщений и базируется на теоретических заключениях, приведенных выше. Итогом работы метода является определение стегосообщения с наибольшим объемом ЗИ, являющегося наименее чувствительным к возмущающим воздействиям. Контейнер, отвечающий такому стегосообщению, — искомый.

При вычислении объема ЗИ учитываются возмущения СВ при стегопреобразовании и абсолютные отделенности соответствующих СЗ, рассматриваемые в качестве весовых коэффициентов.

Пусть $A_1, A_2,..., A_k$ — симметричные матрицы контейнеров размерности $n\times n$, из которых предстоит сделать выбор; $\overline{A}_1, \overline{A}_2,..., \overline{A}_k$ — соответствующие матрицы стегосообщений, полученные после погружения в $A_1, A_2,..., A_k$ одного и того же секретного сообщения с использованием одного стеганографического алгоритма.

Основные шаги метода.

Шаг 1. Построение нормальных СР. $A_j = U_j \Lambda_j U_j^T$, $\overline{A}_j = \overline{U}_j \overline{\Lambda}_j \overline{U}_j^T$, $j=\overline{1,k}$.

Шаг 2. Для $j = 1,2,...k$:

а) построение нормированного вектора VES_j абсолютных отделенностей СЗ стегосообщения $\overline{A}_j$, используемых в качестве весовых коэффициентов при определении объема ЗИ в $\overline{A}_j$

$$\overline{\mathrm{VES}_j}(i) = \mathrm{gap}_{\mathrm{abs}}(i,\overline{A}_j);\ \mathrm{VES}_j(i) = \frac{\overline{\mathrm{VES}_j}(i)}{\left\|\overline{\mathrm{VES}_j}\right\|},\ i=\overline{1,n};$$

б) построение нормированного вектора $\mathrm{OTKLONENIYE}_j$ возмущений СВ при стегопреобразовании ОС A_j

$\overline{\mathrm{OTKLONENIYE}}_j(i) = \sin\theta_i^{(j)}$, где $\theta_i^{(j)}$ — угол между $u_i(A_j)$ и $u_i(\overline{A}_j)$,

$$\mathrm{OTKLONENIYE}_j(i) = \frac{\overline{\mathrm{OTKLONENIYE}}_j(i)}{\left\|\overline{\mathrm{OTKLONENIYE}}_j\right\|},\ i=\overline{1,n};$$

в) построение вектора INF_j распределения ДИ по СВ стегосообщения

$$\overline{\mathrm{INF}}_j(i) = \mathrm{VES}_j(i) * \mathrm{OTKLONENIYE}_j(i),$$

$$\mathrm{INF}_j(i) = \frac{\overline{\mathrm{INF}}_j(i)}{\sum_{i=1}^{n} \overline{\mathrm{INF}}_j(i)} * 100\%, \quad i = \overline{1,n};$$

г) определение СЗ $\overline{\lambda}_{t_1}{}^{(j)}, \ldots, \overline{\lambda}_{t_p}{}^{(j)}$ стегосообщения $\overline{A}_j$ с достаточной абсолютной отделенностью по отношению к предполагаемому возмущению E с использованием вектора $\overline{\mathrm{VES}}_j$, определение защищенных СВ;

д) определение объема ЗИ в стегосообщении $\overline{A}_j$

$$\mathrm{OBYOM}(j) = \sum_{l=1}^{p} \mathrm{INF}_j(t_l).$$

Шаг 3. Определение стегосообщения с наибольшим объемом ЗИ

$$\mathrm{OBYOM}(m) = \max_{1 \le j \le k} \mathrm{OBYOM}(j),$$

A_m — искомый контейнер.

Замечание 1. Общее количество арифметических операций, необходимое для выбора наименее чувствительного к возмущающим воздействиям контейнера предложенным методом, будет определяться как $k\underline{O}(n^3)$, где k — количество контейнеров, из которых делается выбор; $\underline{O}(n^3)$ — количество операций для построения нормального СР матрицы размерности $n \times n$.

Замечание 2. Пусть имеется некоторое ОС, которое предварительно подвергается стандартному разбиению на блоки фиксированной малой размерности [16]. Предложенный метод может быть применен к множеству блоков контейнера, что даст возможность для данного ОС выбрать блоки, малочувствительные к возмущающим воздействиям, и погружение ДИ производить именно в них. Заметим, что количество арифметических операций для исследования каждого блока будет определяться некоторой константой, не зависящей от размерности матрицы ОС. Тогда общее количество арифметических операций для обработки всего ОС определится количеством блоков, т.е. как $\underline{O}(n^2)$, где n — размерность матрицы ОС.

РЕЗУЛЬТАТЫ ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА

Как известно, в реальных наборах операций большинство задач вычислительной математики, в том числе и задача построения спектрального разложения матрицы, являются задачами неограниченной вычислительной сложности, т.е. решаются приближенно [17]. Качество такого решения характеризуется погрешностью, составной частью которой является вычислительная погрешность. При реализации на ЭВМ любого алгоритма на его окончательный результат будет оказывать влияние (существенное или нет) наличие ошибок округления. Этот факт не учитывался выше в предлагаемом методе оценки чувствительности стегосообщений к возмущающим воздействиям, основные вычислительные затраты которого связаны с получением нормального СР матриц. Для оценки суммарного влияния ошибок округления при вычислении нормального СР на итоговые результаты работы предложенного метода используем подход, называемый обратным анализом ошибок [18]. При таком подходе СЗ и СВ, полученные при численной реализации нормального СР матрицы A, несущие в себе погрешность округлений, будем рассматривать как полученные точно, но для $A+H$ (задача с возмущенными входными данными [18]) — для некоторой матрицы H. Как известно [13], норма H удовлетворяет соотношению

$$\|H\|_2 \le f(n)\,\varepsilon\|A\|_2, \tag{6}$$

где n — размерность матрицы A; $f(n)$ — функция размерности матрицы, зависящая от деталей выбранного вычислительного метода; ε — единичная ошибка округления (roundoff error). Как следует из [13], в любом случае оценку (6) можно заменить на

$$\|H\|_2 < n\,\varepsilon\|A\|_2. \tag{7}$$

Из (7) следует, что H можно рассматривать как малое возмущение исходной матрицы A, $\|H\|_2$ мала даже при достаточно большом n (в вычислительном эксперименте, проводимом в среде MATLAB 7, где $\varepsilon \approx 2{,}22e-16$, результаты которого приведены ниже, $\|H\|_2 << 1$). Это означает, что в соответствии с (2) полученный спектр лишь очень незначительно будет отличаться от точных СЗ матрицы A, в силу чего качественная картина для абсолютных отделенностей СЗ, а потому и чувствительностей соответствующих СВ, не пострадает. Однако отреагируют СВ на возмущающее воздействие H в соответствии с соотношением (5) по-разному: более всего от точных СВ матрицы A могут отличаться полученные в результате вычислений СВ, соответствующие СЗ с малыми абсолютными отделенностями. Возмущения даже чувствительных СВ будут незначительными в силу малости $\|H\|_2$, хотя и внесут свой вклад в окончательный результат работы алгоритма, предложенного выше: в элементах вектора $\mathrm{OTKLONENIYE}_j$ возмущений СВ при стегопреобразовании ОС A_j, получаемом на шаге 2,б, составной частью, очевидно, будут и ошибки округлений. Ошибки округлений, «растворяясь» в итоговом возмущении СВ при стегопреобразовании, конечно, «портят» качественную картину анализа чувствительности стегосообщения, однако портят ее очень незначительно, подтверждением чему являются результаты вычислительного эксперимента, приведенные ниже. Таким образом, для тех контейнеров, размерность и норма матрицы которых обеспечивают малость правой части (7), погрешностями округлений в предлагаемом методе оценки чувствительности стегосообщений к возмущающим воздействиям можно пренебречь, что мы и сделаем ниже.

Реализация предложенного метода оценки чувствительности стегосообщений проводилась для решения задачи о выборе ОС, порождающего для заданной ДИ стегосообщение, наименее чувствительное к возмущающим воздействиям.

Для наглядности и простоты анализа получаемых результатов продемонстрируем сначала работу метода на множестве, содержащем лишь три контейнера малой размерности: главные подматрицы матриц изображений CAMERAMAN.TIF, CELL.TIF, MOON.TIF размерности 15×15. Секретное сообщение формировалось случайным образом и погружалось в ОС при помощи LSB-алгоритма [19]. После этого на стегосообщения накладывался одинаковый аддитивный гауссовский шум с нулевым математическим ожиданием и различной дисперсией.

Как видно из результатов эксперимента, приведенных в табл.1, где спектральная норма матрицы возмущения характеризует накладываемый на стегосообщение шум, количество возникающих при декодировании ДИ ошибок определяется объемом ЗИ: чем больше этот объем, тем менее чувствительным является стегосообщение, тем меньше количество ошибок при декодировании, что полностью соответствует полученным теоретическим заключениям.

Таблица 1. Результаты исследования различных стегосообщений для данного секретного сообщения

Изображение	Норма матрицы возмущения							
	1		1,8019		2,9754		4,8775	
	Объем ЗИ, %	Кол-во ошибок при декоди-ровании	Объем ЗИ, %	Кол-во ошибок при декоди-ровании	Объем ЗИ, %	Кол-во ошибок при декодир овании	Объем ЗИ, %	Кол-во ошибок при декоди-ровании
CAMERAMAN	2,8	4	0,005	14	0,005	28	0,005	98
CELL	31	2	31	11	4,1	22	3,22	79
MOON	12,1	2	0,2	14	0,2	28	0,2	100

Как видно из табл. 1, на основе изображения CELL получается наименее чувствительное к возмущающим воздействиям стегосообщение во всех случаях возмущающих матриц, что определяет наибольшую эффективность декодирования. Контейнер же CAMERAMAN во всех рассмотренных случаях дает наихудший результат. Практически так же ведет себя и MOON (в табл. 1 для каждого варианта возмущающей матрицы информация о наилучшем и наихудшем в смысле чувствительности стегосообщении окрашена в серый и темно-серый цвета соответственно).

Важную роль в обеспечении такой «стабильности» играют абсолютные отделенности СЗ стегосообщений (табл.2). Для матрицы стегосообщения, сформированного на основе главной подматрицы изображения CELL, наибольшее количество СЗ имеет сравнительно большие абсолютные отделенности (достаточные по отношению к любому из рассмотренных возмущений) в отличие от стегосообщений, сформированных на основе изображений CAMERAMAN, MOON, что не может гарантировать достаточного объема ЗИ и, как следствие, достаточной эффективности декодирования в таких стегосообщениях.

Таблица 2. Абсолютные отделенности в порядке убывания модулей собственных значений матриц стегосообщений для различных ОС

CAMERAMAN	2353.9	2.5	1.6	1.6	1.1	0.3	0.3	0.5	0.5	0.1	0.1	0.4	0.7	0.7	0.7
CELL	1978.5	21.1	21.1	9.5	9.5	15.6	7.5	5.2	1.4	1.4	0.2	0.2	1.1	1.0	1.0
MOON	55.2721	0.5548	0.5548	2.607	0.5192	0.3011	0.3011	1.2542	0.8904	0.8904	1.3887	0.4425	0.4425	0.4771	0.4771

Для обобщения изложенных результатов вычислительный эксперимент проводился со 100 изображениями в градациях серого одинаковой размерности (100×100), различных по контрастности, текстуре, жанру (пейзажи, портреты, натюрморты и т.д.), по объему ЗИ. Для стегопреобразования были взяты произвольно два стеганографических алгоритма, осуществляющих погружение и декодирование ДИ в различных областях: метод квантования изображений (пространственная область) и метод относительной замены величин коэффициентов ДКП (частотная область) [3]. Случайным образом генерировалось бинарное секретное сообщение, одинаковое для всех контейнеров, после погружения которого на каждое стегосообщение накладывался один и тот же аддитивный гауссовский шум, после чего производилось декодирование ДИ из возмущенных стегосообщений. Результаты проведенных экспериментов показаны на рис. 2 и 3 (кривая скользящего усреднения для большей наглядности строится с использованием пяти значений).

Рис. 2. Метод квантования изображения

Заметим, что имеющиеся различия в объеме восстановленной информации для стегосообщений с близкими значениями объемов ЗИ связаны с наличием в стегосообщениях СВ, возмущенных в процессе стегопреобразования, но незащищенных от применяемого возмущающего воздействия. Как было показано, поведение незащищенных СВ является неконтролируемым.

Однако, несмотря на это, из сопоставления всей совокупности полученных результатов для всех рассмотренных стегосообщений непосредственно следует, что *наибольшая эффективность декодирования, независимо от специфики стеганографического алгоритма, отвечает наименее чувствительным стегосообщениям, т.е. стегосообщениям с наибольшим объемом ЗИ*, что было теоретически обосновано выше. Такие результаты дают возможность использовать предложенный метод для обоснованного выбора контейнера, обеспечивающего наибольшую эффективность декодирования ДИ при имеющейся возможности предварительной оценки ожидаемого возмущающего воздействия на стегосообщение.

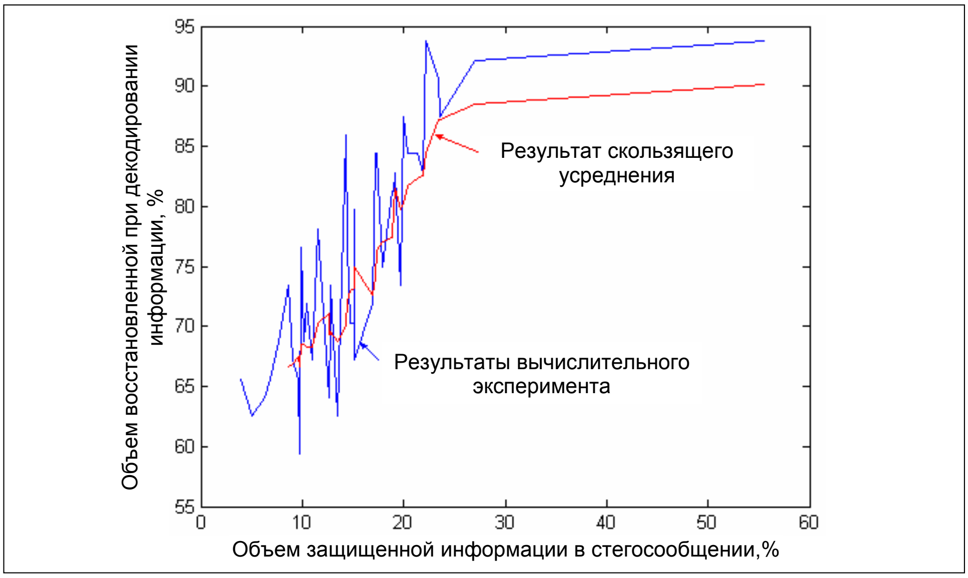

Рис. 3. Метод относительной замены величин коэффициентов ДКП

ВЫВОДЫ

1. Разработана математическая база для построения метода оценки чувствительности стегосообщения к возмущающим воздействиям на основе матричного анализа и теории возмущений.

2. Предложен метод, позволяющий проводить сравнение чувствительностей различных стегосообщений к возмущающим воздействиям, независимо от особенностей формирующего их стегоалгоритма, основанный на анализе спектральных разложений матриц стегосообщений.

3. На основании предложенного метода решается задача о выборе контейнера из имеющегося конечного множества контейнеров для заданного секретного сообщения, обеспечивающего наименьшую чувствительность получаемого на его основе стегосообщения к возмущающим воздействиям и, как следствие, наибольшую эффективность процесса декодирования ДИ.

4. Нерешенной остается проблема оценки возмущений незащищенных СВ, что в настоящий момент является приоритетной областью исследований авторов.

ЛИТЕРАТУРА

1. *Фергюсон Н., Шнайер Б.* Практическая криптография. — М.: Издательский дом «Вильямс», 2005. — 424 с.
2. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. — Киев: Юниор, 2003. — 501 с.
3. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. — Киев: МК –Пресс, 2006. — 288 с.
4. *Задірака В.К., Олексюк О.С., Недашковський М.О.* Методи захисту банківської інформації. — Київ: Вища шк., 1999. — 261 с.
5. *Кобозева А.А.,Маракова И.И., Скопа А.А.* Стеганографический метод обеспечения информационной безопасности морской связи // Зб. наук. праць НУК. — 2006. — № 3(408). — С.155–161.
6. *Кобозева А.А., Маракова И.И.* Метод повышения устойчивости стеганографических методов к возмущающим воздействиям // Наук.-техн. журн. «Захист інформації». — 2007. — №1(32). — С. 53–60.
7. *Каханер Д., Моулер К., Нэш С.* Численные методы и программное обеспечение. — М.: Мир, 2001. — 575 с.
8. *Хорн Р., Джонсон Ч.* Матричный анализ. — М.: Мир,1989. — 656 с.
9. *Гантмахер Ф.Р.* Теория матриц. — М.: Наука, 1988. — 552 с.
10. *Маслов В.П.* Асимптотические методы и теория возмущений. — М.: Наука, 1988. — 312 с.
11. *Деммель Дж.* Вычислительная линейная алгебра. — М.: Мир, 2001. — 430 с.
12. *Бахвалов Н.С., Жидков Н.П., Кобельков Г.М.* Численные методы. — М.: БИНОМ. Лаборатория знаний, 2006. — 636 с.
13. *Парлетт Б.* Симметричная проблема собственных значений. Численные методы. — М.: Мир, 1983. — 384 с.
14. *Кобозева А.А.* Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах // Вісн. Східноукр. національн. ун-ту ім. В.Даля. — 2006. — №9(103). — С. 74–82.
15. *Кобозева А.А.* Стеганографический метод, основанный на преобразовании спектра симметричной матрицы // Праці УНДІРТ. — 2006. — № 4 (48). — С. 44–52.
16. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. — М.: Техносфера, 2005. — 1072 с.
17. *Т-ефективні* алгоритми наближеного розв'язання задач обчислювальної та прикладної математики / В.К. Задірака т. ін. — Київ, 2003. — 261 с.
18. *Воеводин В.В.* Вычислительные основы линейной алгебры. — М.: Наука, 1977. — 304 с.
19. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с.

Поступила 22.05.2007