УДК 004.056.5:518:512.624.3

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 3, pp. 254-267

ТЕОРИЯ ВОЗМУЩЕНИЙ КАК ОСНОВА ОБЩЕГО ПОДХОДА К ОЦЕНКЕ ЧУВСТВИТЕЛЬНОСТИ СТЕГАНОСООБЩЕНИЙ

А.А. Кобозева, Е.В. Нариманова

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

Разработан общий математический подход к оценке чувствительности стеганосообщений к возмущающим воздействиям, не зависящий от используемого стеганографического алгоритма, области погружения секретной информации, области анализа стеганосообщения – пространственной или частотной. Основными математическими инструментами являются матричный анализ и теория относительных возмущений. Предлагается способ оценки защищенности секретной информации, внедренной в контейнер, в качестве которого рассматривается цифровое изображение. Разработан способ количественной оценки чувствительности стеганосообщения к возмущающим воздействиям, который используется для решения задачи о выборе контейнера из конечного множества контейнеров для заданного секретного сообщения. Получаемое решение обеспечивает наименьшую чувствительность стеганосообщения к возмущающим воздействиям, т.е. наибольшую эффективность процесса декодирования дополнительной информации, оцениваемую при помощи объема восстановленной информации. Приведены результаты вычислительного эксперимента.

Ключевые слова: стеганосообщение, возмущающее воздействие, чувствительность, матрица, собственное число, собственный вектор

Введение

Жизнедеятельность общества немыслима без накопления, хранения, изменения, передачи информации. Специфика сегодняшнего дня заключается в том, что информация характеризуется не только как ресурс, но и как объект труда. В настоящее время в число защищаемых помимо военных, государственных и ведомственных, включены также секреты промышленные, коммерческие и даже личные. Информация все больше становиться товаром, причем одним из самых дорогих. Трудно переоценить важность и актуальность вопросов, связанных с ее защитой [1-3].

Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений информационной безопасности сформировали современные методы стеганографии [4-13].

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. Особенностью стеганографического подхода является то, что он не предусматривает оглашения факта существования защищаемой информации. Это обстоятельство позволяет в рамках традиционно существующих информационных потоков или информационной среды решать важные задачи защиты информации ряда прикладных областей, как, например, в [4, 14, 15].

Стеганографирование может осуществляться различными способами, однако 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 по каналу связи адресату или хранится в таком виде. Процесс погружения ДИ в ОС, или контейнер, будем называть стеганопреобразованием (СП), а результат стегопреобразования – стеганосообщением (СС).

Постановка задачи и цель исследования

Хотя практические приложения стеганографии в настоящий момент достигли значительного развития, используемые стеганографические методы часто не имеют под собой строгого теоретического обоснования [6, 8-10, 12]. Это затрудняет выделение ограничений для области применимости тех или иных стеганографических алгоритмов (СА), не дает возможности разработки универсальных в некотором смысле стеганографических методов и общих подходов решения актуальных задач стеганографии, в частности, задачи обеспечения одного из основных требований, предъявляемых к любому СА, – требования нечувствительности получаемого СС к возмущающим воздействиям, которое равносильно требованию устойчивости СА к преднамеренным (непреднамеренным) атакам [4, 16, 17]. До настоящего момента активно культивировалась и продолжает культивироваться ошибочная, по мнению авторов, идея о том, что результат СП при помощи СА, работающих в частотной области, менее чувствителен к большинству возмущающих воздействий, чем результат пространственного СП [4-6].

Таким образом, задача создания единого подхода к качественной и количественной оценке чувствительности СС, основы решения которой были заложены авторами настоящей работы в [18], остается актуальной задачей стеганографии.

Целью работы является разработка общего математического подхода к оценке чувствительности СС к возмущающим воздействиям, не зависящего от используемого стеганоалгоритма и области погружения ДИ, который позволит:

- оценивать (сравнивать) устойчивость существующих СА;
- делать выбор контейнера, обеспечивающего для заданного секретного сообщения наименее чувствительное стеганосообщение;
- теоретически обоснованно модифицировать существующие и разрабатывать новые устойчивые к атакам СА, независимо от используемой ими области ОС для СП (пространственной, частотной).

Для достижения поставленной цели в работе решаются следующие *задачи*:

- универсальной (не зависящей от конкретики используемого СА) формализации процесса СП;
- выбора формальных параметров, определяющих СС (ОС), характеризующих его чувствительность к возмущающим воздействиям;
- получения достаточных условий нечувствительности СС к возмущающим воздействиям.

Основными математическими инструментами выступают матричный анализ и теория относительных возмущений. Использование теории возмущений дает принципиальную возможность для определения степени зависимости состояния произвольного ОС (СС) от произвольного возмущающего воздействия; позволяет производить априорную оценку основных свойств СС (ОС); абстрагируясь от конкретики СП, дает возможность анализировать результат этого возмущающего воздействия.

Формализация процесса стеганопреобразования

В качестве контейнера в силу широкого распространения в настоящее время цифровых сигналов часто используются цифровые изображения (ЦИ), аудио (ЦА) и видео (ЦВ). Произвольное ЦИ и ЦВ, рассматриваемое как последовательность видеокадров, естественным образом представимы в виде матрицы (совокупности матриц). Хотя общеиспользуемой математической формализацией ЦА является вектор, элементарно осуществляется переход к его двумерному матричному представлению [19], что позволяет в качестве математической модели любого из указанных цифровых сигналов использовать матрицу (конечное множество матриц). Таким образом, не ограничивая общности рассуждений, для определенности и простоты изложения везде ниже в роли контейнера выступает цифровое монохромное изображение, $n \times n$-матрица которого обозначается F; ДИ – сформированная случайным образом последовательность $p_1, p_2, ..., p_k$, где $p_i \in \{0,1\}, i = \overline{1,k}$; $\overline{p}_1, \overline{p}_2, ..., \overline{p}_k$, $\overline{p}_i \in \{0,1\}$, $i = \overline{1,k}$, – декодированное из СС секретное сообщение. Объем восстановленной при декодировании информации (ОВИ) определяется в соответствии с формулой:

$$\frac{k - \sum_{i=1}^{k} p_i \oplus \overline{p}_i}{k} \times 100\%,$$

где $\oplus$ – операция логического исключающего ИЛИ.

СС будем называть чувствительным, если чувствительной окажется задача декодирования ДИ, т.е. если незначительные возмущающие воздействия, которым подвергается СС, способны привести к значительному снижению ОВИ, и нечувствительным в противном случае.

Погружение ДИ в ОС, независимо от способа и области (пространственной, частотной) этого погружения, формально представляется как возмущение ΔF матрицы F. Тогда матрица СС $\overline{F}$ удовлетворяет соотношению: $\overline{F} = F + \Delta F$, где $\Delta F = f(F)$, т.е. ΔF является некоторой функцией матрицы контейнера F. Отсюда вытекает, что произвольное СП можно представить в виде аддитивного погружения некоторой информации, формальным представлением которой является матрица ΔF, в пространственной области.

Любые преобразования, которые производятся над СС, формализуются как дополнительные возмущения матрицы ОС F.

Определим набор математических параметров, который полностью характеризует любое ОС (СС). Поскольку формальным представлением ОС (СС) является матрица, то в качестве набора искомых характеристик можно использовать множество сингулярных чисел и ортонормированных лексикографически положительных сингулярных векторов, а также спектр (совокупность собственных значений (СЗ)) и множество ортонормированых лексикографически положительных собственных векторов (СВ) соответствующей матрицы [2]. В случае симметричности матрицы ОС F второй из наборов является предпочтительным в силу следующих замечаний. Во-первых, построение спектрального разложения симметричной матрицы, результатом которого является определение СЗ и СВ, обладает рядом преимуществ в вычислительном смысле по сравнению с построением сингулярного разложения для матрицы произвольной структуры того же размера и уровня заполненности, результатом которого является определение сингулярных чисел и сингулярных векторов [20,21]; во-вторых, СЗ симметричной матрицы (как и сингулярные числа произвольной матрицы) являются хорошо обусловленными [22], т.е.

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

где

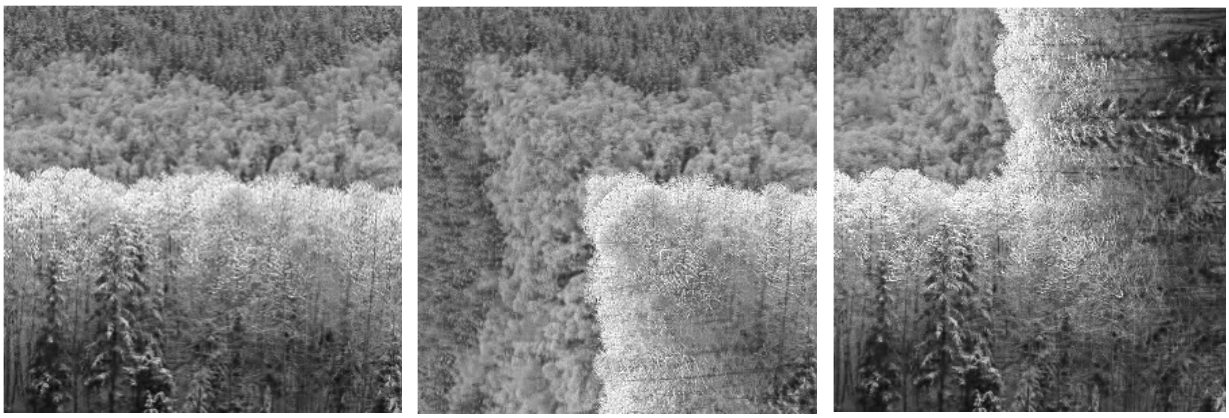
$\lambda_j(\cdot)$ – СЗ соответствующей матрицы,

$\|\cdot\|_2$ – спектральная матричная норма [20] (чего нельзя утверждать в общем случае для несимметричных матриц [20]).

Однако, как правило, матрица ОС не удовлетворяет свойству: $F=F^T$. Поставим в соответствие F две симметричные $n\times n$-матрицы A, B по следующему правилу:

$$F=\begin{pmatrix}a_{11}\,a_{12}\,\ldots a_{1n}\\ a_{21}\,a_{22}\,\ldots a_{2n}\\ \ldots\ldots\ldots\\ a_{n1}\,a_{n2}\,\ldots a_{nn}\end{pmatrix}\rightarrow A=\begin{pmatrix}a_{11}\,a_{12}\ldots a_{1n}\\ a_{12}\,a_{22}\ldots a_{2n}\\ \ldots\ldots\ldots\\ a_{1n}\,a_{2n}\ldots a_{nn}\end{pmatrix},\ B=\begin{pmatrix}a_{11}\,a_{21}\ldots a_{n1}\\ a_{21}\,a_{22}\ldots a_{n2}\\ \ldots\ldots\ldots\\ a_{n1}\,a_{n2}\,\ldots a_{nn}\end{pmatrix}, \qquad (2)$$

которые будем рассматривать ниже как матрицы ОС (рис. 1).



а **б** **в**

Рис. 1. Исходное цифровое изображение с несимметричной матрицей F (а); соответствующие изображения с симметричными матрицами A (б); B (в)

При встраивании ДИ в исходный контейнер СП представляется в виде погружения в верхний (нижний) треугольник матрицы $A(B)$ с последующим виртуальным симметричным отражением результата относительной главной диагонали $A(B)$. Результат СП обозначим $\overline{A}$ и $\overline{B}$ ($\overline{A}=\overline{A}^T$, $\overline{B}=\overline{B}^T$). При окончательном формировании матрицы СС используется верхний треугольник $\overline{A}$ и нижний треугольник матрицы $\overline{B}$. Применение такого подхода, дающего возможность рассматривать матрицы ОС, СС как симметричные и, в силу этого, использовать для их формального описания спектр и соответствующие СВ, было предложено в [23] и используется в настоящей работе.

Пусть E – $n\times n$-матрица произвольного возмущающего воздействия, которому подвергается ОС (СС). В общем случае $E\neq E^T$. Матрице E поставим в соответствие две симметричных матрицы той же размерности, используя правило (2), рассматривая матрицу, отвечающую верхнему (нижнему) треугольнику E как возмущающую для контейнера (СС), полученного на основе $A(B)$, что дает принципиальную возможность

матрицу произвольного возмущающего воздействия также рассматривать ниже как симметричную.

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

$$A=U\Lambda U^T \tag{3}$$

– спектральное разложение (СР) матрицы A [20] (здесь $\Lambda=diag(\lambda_1,...,\lambda_n),\ U=[u_1,...,u_n]$), которое в общем случае определяется неоднозначно. СР (3) назовем нормальным, если элементы матрицы Λ удовлетворяют соотношению: $|\lambda_1|\geq...\geq|\lambda_n|$, а СВ $u_i,\ i=\overline{1,n}$, лексикографически положительны [2]. Если A – невырожденная симметричная $n\times n$-матрица, модули СЗ которой попарно различны, для нее существует единственное нормальное СР [2].

Далее будем считать, что все матрицы, отвечающие рассматриваемым ОС, симметричны (в силу (2)) и удовлетворяют достаточным условиям, обеспечивающим единственность нормального СР.

Произвольное возмущающее воздействие, в частности, СП матрицы ОС, определенным образом возмутит ее спектр и (или) СВ. В силу этого результат любого СП – завершенное погружение ДИ в контейнер – формально может быть представлен в виде совокупности возмущений спектра и (или) СВ матрицы ОС, однозначно определяемых нормальным СР, которые произошли в ходе СП.

Поскольку согласно (1), все СЗ симметричной матрицы ОС являются нечувствительными к возмущающим воздействиям, независимо от того, чувствительным или нечувствительным окажется полученное СС, целесообразным для оценки чувствительности СС является анализ возмущений СВ матрицы ОС, которые произошли в процессе СП. СС отличается от контейнера содержанием в нем ДИ. Таким образом, совокупность возмущений СВ матрицы контейнера может рассматриваться как формальное представление погруженной ДИ (для $n=3$ геометрическая интерпретация дана на рис.2, где $u_i, i=\overline{1,3}$, – СВ матрицы ОС, а $u_i, i=\overline{1,3}$, – СВ СС).

СП, а также возмущающие воздействия, которым подвергается СС в ходе пересылки и (или) хранения, должны обеспечивать надежность его восприятия [4], т.е. так возмутить матрицу ОС (СС), чтобы зрительно возмущение оказалось незаметным. В силу этого везде ниже рассматриваются малые возмущающие воздействия [2, 4].

Качественная оценка чувствительности стеганосообщения к возмущающим воздействиям

Пусть A - произвольная симметричная матрица контейнера. Назовем абсолютной отделенностью СЗ λ_i матрицы A число, определяемое в соответствии с формулой: $gap_{abs}(i,A)=\min\limits_{i\neq j}\left\|\lambda_j|-|\lambda_i\right\|$.

Погружение одного и того же секретного сообщения при помощи одного СА в разные контейнеры в общем случае приводит к разным по чувствительности СС. Действительно, спектры матриц различных ОС отличаются друг от друга не только по непосредственным значениям СЗ, но и, что главное, по абсолютным отделенностям СЗ. Поэтому понятие малой (наименее возможной) чувствительности, рассматривается в данном разделе по отношению к конкретному ОС (СС) как качественная характеристика.

Теорема 1. Достаточным условием обеспечения малой (наименьшей из возможных) чувствительности СС к возмущающим воздействиям для используемого контейнера является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы СС, имеющим большие, по сравнению с остальными, (максимальные из всех) абсолютные отделенности.

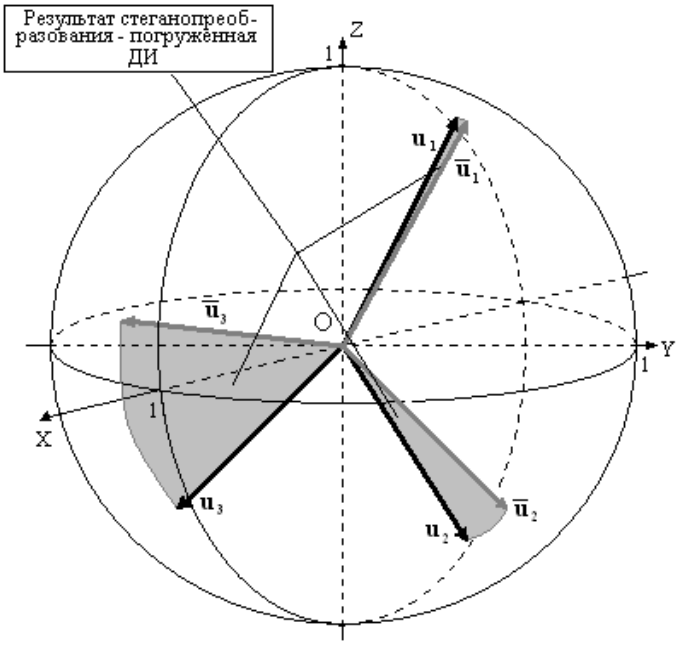


Рис. 2. Формальное представление дополнительной информации, погруженной при стеганопреобразовании

Доказательство. При погружении ДИ в контейнер СВ матрицы A ОС возмутятся, отклонившись от первоначального положения на некоторые углы (рис. 2). Это произойдет всегда, если только алгоритм погружения ДИ не базируется на непосредственной модификации лишь СЗ матрицы ОС, как, например, в [24]. Этот случай требует отдельного обсуждения, которое не проводится в настоящей работе. Поскольку формальным представлением результата СП (погруженной информации) является совокупность возмущений СВ матрицы контейнера, чувствительность полученного СС будет определяться чувствительностью возмущенных при стеганопреобразовании СВ матрицы A. В соответствии с [20] СВ является чувствительным, если малое возмущающее воздействие может привести к значительному возмущению вектора, т.е. значительному углу его поворота от первоначального положения. Очевидно, чтобы сохранить неизменной погруженную ДИ при возмущающем воздействии, направленном на СС, возмущения СВ, возникшие в результате СП, должны остаться неизменными после воздействия.

Пусть $\overline{A}$ – симметричная матрица СС, нормальное СР которой в соответствии с (3) представляется в виде: $\overline{A} = \overline{U}\overline{\Lambda}\overline{U}^T$; E – матрица некоторого возмущающего воздействия, направленного на СС $\overline{A}$, $E = E^T$; $\overline{A} + E = \overline{\overline{U}}\,\overline{\overline{\Lambda}}\,\overline{\overline{U}}^T$ – нормальное СР $\overline{A} + E$. Пусть $\overline{u}_i$, $\overline{\overline{u}}_i$ – нормированные лексикографически положительные СВ $\overline{A}$ и $\overline{A} + E$ соответственно, отвечающие *i*-му СЗ, а θ_i – угол между ними. Легко показать, опираясь на [20], что:

$$\sin\theta_i \le \frac{2\|E\|_2}{gap_{abs}\left(i,\overline{A}\right)}. \qquad (4)$$

В соответствии с (4) СВ, возмущенные при СП контейнера, а значит и СС в целом, будут тем менее чувствительными к возмущающим воздействиям, чем большие абсолютные отделенности $gap_{abs}\left(i,\overline{A}\right)$ имеют соответствующие СЗ матрицы $\overline{A}$, а наименьшая чувствительность СС будет обеспечиваться в том случае, когда возмущению при СП подверглись только те СВ матрицы ОС, которые отвечают СЗ СС с максимальными абсолютными отделенностями.

Таким образом, абсолютная отделенность СЗ является мерой чувствительности соответствующего СВ к возмущающим воздействиям, а абсолютные отделенности СЗ, соответствующих возмущенным при стеганопреобразовании СВ, определяют чувствительность полученного СС. СС будет наименее чувствительным к возмущающим воздействиям, если СП возмутит СВ, соответствующие СЗ матрицы СС, имеющим наибольшие абсолютные отделенности. Более того, как показывает вычислительный эксперимент, наибольшие абсолютные отделенности СЗ, присутствующих в спектре матрицы СС, таковы, если в процессе СП были возмущены только СВ, отвечающие этим СЗ, то они обеспечивают нечувствительность СС в указанном случае: углы поворота соответствующих СВ при возмущающем воздействии, сохраняющем надежность восприятия СС, составляют, как правило, доли секунды.

Следствие 1. Если возмущенные в результате стеганопреобразования ОС СВ соответствуют СЗ матрицы СС с малыми абсолютными отделенностями, то полученное СС оказывается чувствительным к возмущающим воздействиям, что приводит к недостаточной эффективности декодирования ДИ, оцениваемой ОВИ.

Как следует из (1), абсолютные отделенности СЗ матриц $\overline{A}$ и A незначительно отличаются друг от друга, откуда вытекает истинность следствия 2.

Следствие 2. Достаточным условием обеспечения малой (наименьшей из возможных) чувствительности СС к возмущающим воздействиям для используемого контейнера является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы ОС, имеющим большие, по сравнению с остальными, (максимальные из всех) абсолютные отделенности.

Заметим, что на практике для реальных ЦИ наибольшие абсолютные отделенности имеют максимальные по модулю СЗ соответствующих матриц.

Теорема 2. Достаточным условием обеспечения малой чувствительности (нечувствительности) СС к предполагаемому возмущающему воздействию E является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы СС, имеющим абсолютные отделенности, значительно превосходящие $\|E\|_2$.

Доказательство теоремы непосредственно следует из соотношения (4) в случае, когда $gap_{abs}\left(i,\overline{A}\right) >> \|E\|_2$.

Следствие. Достаточным условием обеспечения малой чувствительности (нечувствительности) СС к предполагаемому возмущающему воздействию E является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы ОС, имеющим абсолютные отделенности, значительно превосходящие $\|E\|_2$.

Из всего вышесказанного следуют *выводы*:

- чувствительность СС к возмущающим воздействиям определяется характером возмущений СВ матрицы ОС при СП, и не зависит от области погружения ДИ, используемого СА. Исходя из значений возмущений и абсолютных отделенностей соответствующих СЗ возможно сделать качественные априорные оценки чувствительности СС к возмущающим воздействиям;

▪ при разработке новых (модификации существующих) устойчивых к возмущающим воздействиям СА, т.е. алгоритмов, формирующих нечувствительные (малочувствительные) СС, необходимо обеспечить следующее требование: СП должно осуществляться так, чтобы при его формальном представлении в виде совокупности возмущений СВ матрицы ОС, возмущенные СВ соответствовали СЗ с большими, по сравнению с другими СЗ, абсолютными отделенностями. Наименьшая чувствительность СС будет достигаться при соответствии возмущенных СВ СЗ с наибольшими абсолютными отделенностями (здесь возможно нарушение надежности восприятия СС [19]). Для обеспечения сформулированного требования не имеет значения используемая СА для погружения ДИ область ОС – пространственная, частотная, что нивелирует так называемое преимущество с точки зрения устойчивости к возмущениям для СА, осуществляющих погружение секретной информации в частотной области.

Замечание. Возмущения СВ, происходящие в результате СП, в частотной и пространственной области изображения одинаковы (независимо от того, в какой области происходит погружение ДИ).

Действительно, если A – симметричная матрица яркости ЦИ, а A_J – соответствующая матрица частотных коэффициентов (например, коэффициентов дискретного косинусного преобразования), то они связаны соотношением [25]:

$$A_J = PAP^T, \tag{5}$$

где P – ортогональная матрица. С учетом (3) формула (5) примет вид:

$$A_J = PAP^T = PU\Lambda U^T P^T = (PU)\Lambda(PU)^T. \tag{6}$$

В силу того, что матрица PU является ортогональной, правая часть (6) дает спектральное разложение A_J, из которого вытекает, что СЗ A_J и A – одинаковые, а СВ $u^{(J)}$ матрицы A_J представляются как

$$u^{(J)} = Pu,$$

где u – соответствующие СВ A. Если $\bar{A}$ и $\bar{A}_J$ – матрицы СС в пространственной и частотной областях соответственно, СВ которых $\bar{u}$ и $\bar{u}^{(J)}$, то

$$\left(u^{(J)}, \bar{u}^{(J)}\right) = \left(Pu, P\bar{u}\right) = \left(u, \bar{u}\right), \tag{7}$$

где (a,b) – скалярное произведение векторов a,b. Из (7) вытекает, что углы между векторами $u,\bar{u}$ и $u^{(J)},\bar{u}^{(J)}$ одинаковы, что и требовалось показать.

Таким образом, анализ возмущений СВ матрицы ЦИ, происходящих в результате СП, возможно проводить как в пространственной, так и в частотной области изображения в зависимости от специфики конкретной задачи.

Количественная оценка чувствительности стеганосообщения к возмущающим воздействиям

Для получения количественной оценки чувствительности СС вернемся к соотношению (4). Заметим, что если правая часть (4) превзойдет единицу, т.е.

$$\|E\|_2 \geq \frac{gap_{abs}\left(i, \overline{A}\right)}{2},$$

то оценка возмущения СВ приобретет вид: $\sin\theta_i \leq 1$, превращаясь в тривиальную, и сделать заключение о реальной чувствительности такого вектора не представляется возможным. Кроме того, в этой ситуации в общем случае для θ_i принципиально нельзя найти никакой практической оценки. Для иллюстрации сказанного рассмотрим пример, когда возмущение E таково, что СЗ матрицы $\overline{A} + E$, достаточно отдалившись от СЗ $\overline{A}$ (соотношение (1)), превратились в кратные:

$$\overline{A} = \begin{pmatrix} 1.0005 & 0 \\ 0 & 0.9995 \end{pmatrix}, \text{ а } \overline{A} + E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Поскольку любой ненулевой вектор размерности 2 является СВ для $\overline{A} + E$, то нет никакой принципиальной возможности оценить угол θ_i.

Будем говорить, что СЗ λ_i имеет достаточную (недостаточную) абсолютную отделенность по отношению к возмущению E, если

$$gap_{abs}\left(i, \overline{A}\right) > 2\|E\|_2 \quad (gap_{abs}\left(i, \overline{A}\right) \leq 2\|E\|_2).$$

СВ, 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 (4); СВ, отвечающие СЗ с большими (максимальными) абсолютными отделенностями, являются защищенными от любого из рассматриваемых (малых) возмущений. 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 СП увеличивается и количество ДИ, которая хранится в возмущении этого вектора. СВ «распределяют между собой» погруженную ДИ. Конечно, такое допущение будет не совсем оправданным, если алгоритм погружения связан с определенной непосредственной модификацией СВ, например, с изменением знаков их компонент, как, например, в [23]. Однако это лишь незначительно сужает область рассмотрения и является предметом исследования другой работы одного из авторов.

На основе сделанного выше допущения предположим, что СС тем менее чувствительно, чем большему возмущению при СП подверглись СВ, отвечающие СЗ с максимальными абсолютными отделенностями, чем большая «часть» погруженной ДИ является защищенной от возмущающих воздействий.

В качестве количественной оценки чувствительности СС рассмотрим объем ЗИ, определяемый с учетом возмущений защищенных СВ и абсолютных отделенностей соответствующих СЗ, непосредственное вычисление которого сводится к следующему.

Пусть A и $\overline{A}$ – симметричные $n \times n$-матрицы контейнера и СС, полученного при помощи некоторого СА, соответственно;

$$A = U\Lambda U^T,$$

$$\overline{A} = \overline{U}\,\overline{\Lambda}\,\overline{U}^T$$

– их нормальные СР. Определим вектор $V=(v_1,\ldots,v_n)^T$ весовых коэффициентов при учете возмущений СВ матрицы ОС в процессе СП, в соответствии с абсолютными отделенностями СЗ матрицы СС:

$$v_i=\frac{\overline{v}_i}{\left\|\overline{V}\right\|},\quad i=\overline{1,n},$$

где $\overline{V}$ – вектор с элементами $\overline{v}_i=gap_{abs}\left(i,\overline{A}\right),\ i=\overline{1,n}$.

Возмущения СВ матрицы контейнера в процессе СП учитываются естественным образом в процессе формирования вектора $P=(p_1,\ldots,p_n)^T$:

$$p_i=\frac{\overline{p}_i}{\left\|\overline{P}\right\|},\quad i=\overline{1,n},$$

где

$\overline{P}$ – вектор с элементами $\overline{p}_i=\sin\theta_i,\ i=\overline{1,n}$;

θ_i – угол между СВ u_i, $\overline{u}_i$ матриц A и $\overline{A}$ соответственно.

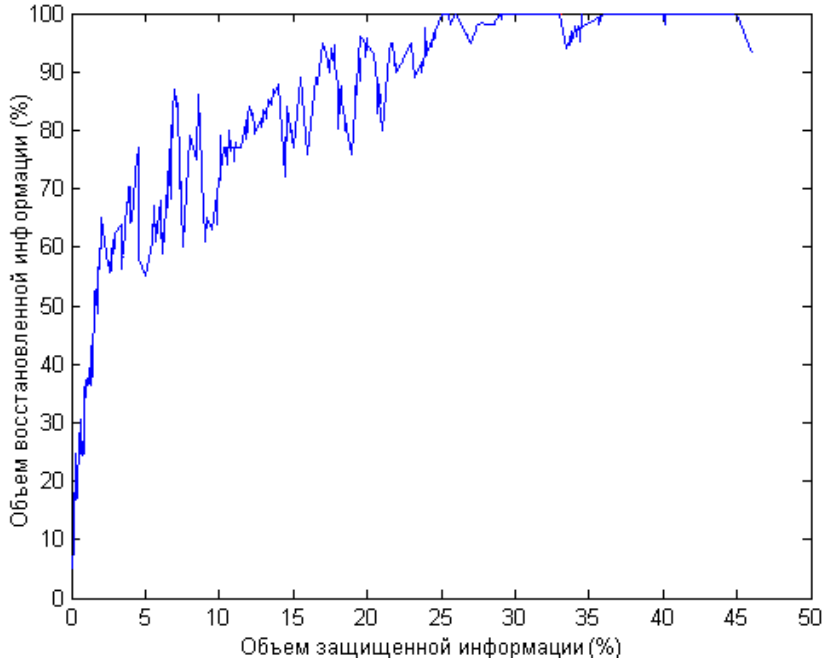
Пусть $\overline{\lambda}_{t_1},\ldots,\overline{\lambda}_{t_p}$ – СЗ $\overline{A}$ с достаточной абсолютной отделенностью по отношению к предполагаемому возмущению E (соответствующие СВ $\overline{u}_{t_1},\ldots,\overline{u}_{t_p}$ – защищенные от E), тогда окончательная формула для объема I ЗИ в СС $\overline{A}$ – количественной оценки чувствительности СС к возмущающему воздействию E – выглядит следующим образом:

$$I=\sum_{j=1}^{p}p_{t_j}v_{t_j}. \qquad (8)$$

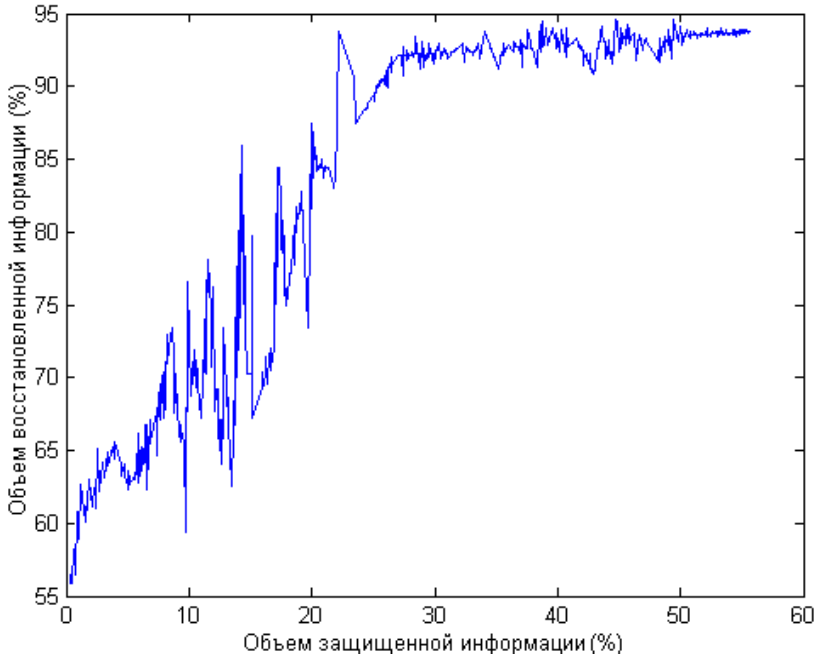
Выдвинем следующую гипотезу: чем больше объем ЗИ в СС, определяемый в соответствии с формулой (8), тем менее это СС будет чувствительным к возмущающим воздействиям, т.е. тем больше будет ОВИ при декодировании ДИ из атакованного (возмущенного) СС. Для проверки этой гипотезы был проведен вычислительный эксперимент.

Результаты вычислительного эксперимента

Вычислительный эксперимент проводился в среде *MathWorks* MATLAB более, чем с 300 монохромными ЦИ одинакового размера (100×100 пикселей), различными по контрастности, текстуре, жанру (пейзажи, портреты, натюрморты и др.), по объему ЗИ. Для СП были взяты два СА, осуществляющих погружение и декодирование ДИ в различных областях: метод квантования изображений (пространственная область) и метод относительной замены величин коэффициентов дискретного косинусного преобразования (частотная область) [5]. Случайным образом генерировалось бинарное секретное сообщение, одинаковое для всех контейнеров, после погружения которого каждое СС подвергалось одному и тому же возмущающему воздействию с матрицей E. Учитывая $\left\|E\right\|_2$, в соответствии с формулой (8) вычислялся объем I ЗИ в невозмущенном СС и производилось декодирование ДИ из возмущенных СС с последующим вычислением ОВИ. Результаты проведенных экспериментов, которые в целом подтверждают выдвинутую в предыдущем пункте гипотезу, представлены на рис. 3.



а



б

Рис. 3. Зависимость объема восстановленной при декодировании информации от объема защищенной информации в стеганосообщении: а – метод квантования изображения; б – метод относительной замены величин коэффициентов дискретного косинусного преобразования

Заметим, что имеющиеся различия в ОВИ для СС с близкими значениями объемов ЗИ обязаны существованию в стеганосообщениях СВ, возмущенных в процессе СП, но незащищенных от применяемого возмущающего воздействия. Как было отмечено выше, поведение незащищенных СВ является неконтролируемым. Однако, несмотря на это, из сопоставления всей совокупности полученных результатов, для всех рассмотренных СС, непосредственно вытекает, что наибольшая эффективность

декодирования, независимо от конкретики СА и возмущающего воздействия, отвечает наименее чувствительным стеганосообщениям – стеганосообщениям с наибольшим объемом ЗИ. Такие результаты дают возможность использовать предложенный подход для обоснованного выбора контейнера из данного множества контейнеров, обеспечивающего наибольшую эффективность декодирования ДИ.

Вычислительная сложность количественной оценки чувствительности СС в соответствии с формулой (8) будет определяться вычислительной сложностью процесса получения СР матрицы.

Замечание. Пусть имеется некоторое ОС, которое предварительно подвергается разбиению на блоки фиксированной малой размерности. Предложенный метод оценки чувствительности может быть применен к множеству блоков контейнера, что даст возможность для данного ОС выбрать блоки, которые будут малочувствительными к предполагаемым возмущающим воздействиям, и погружение ДИ производить именно в эти блоки. 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 $\underline{O}\left(n^2\right)$, где n – размерность матрицы ОС.

Выводы

На основе теории возмущений и матричного анализа разработан принципиально новый общий математический подход к оценке чувствительности СС к возмущающим воздействиям, в результате которого:

1) Получена универсальная математическая формализация процесса стеганопреобразования в виде совокупности возмущений собственных значений и собственных векторов специального вида матрицы контейнера, рассматриваемой в симметричном виде, позволившая выделить математические параметры, характеризующие чувствительность стеганосообщения;

2) Получены достаточные условия обеспечения нечувствительности (малой чувствительности) стеганосообщения к возмущающим воздействиям, носящие характер качественной оценки чувствительности, не зависящие от используемого при стеганопреобразовании алгоритма и области изображения, используемой для анализа – пространственной, частотной;

3) Разработан способ количественной оценки чувствительности стеганосообщения к возмущающим воздействиям, позволяющий проводить сравнение чувствительностей различных стеганосообщений. Разработанный способ может быть использован для решения одной из широко распространенных задач стеганографии – задачи о выборе контейнера из имеющегося конечного множества контейнеров для заданного секретного сообщения, обеспечивающего наименьшую чувствительность получаемого на его основе стеганосообщения к возмущающим воздействиям, т.е. наибольшую эффективность процесса декодирования дополнительной информации, оцениваемую при помощи объема восстановленной информации.

Список литературы

1. Ленков, С.В. Методы и средства защиты информации : [в 2 томах] / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко ; [под ред. В.А. Хорошко]. — Киев : Арий, 2008.
2. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
3. Грищук, Р.В. Теоретические основы моделирования процессов атак на информацию методами теорий дифференциальных игр и дифференциальных преобразований / Р.В. Грищук. — Житомир: Рута, 2010. — 280 с.

4. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
5. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
6. Cheddad, A. Digital image steganography: Survey and analysis of current methods / A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt // Signal Processing. — 2010. — Vol.90, Iss.3. — PP. 727–752.
7. Cheddad, A. A skin tone detection algorithm for an adaptive approach to steganography / A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt // Signal Processing. — 2009. — Vol.89, Iss.12. — PP. 2465–2478.
8. Luo, X.-Y. A review on blind detection for image steganography / X.-Y. Luo, D.-S. Wang, P. Wang, F.-L. Liu // Signal Processing. — 2008. — Vol.88, Iss.9. — PP.2138–2157.
9. Khatirinejad, M. Linear codes for high payload steganography / M. Khatirinejad, P. Lisoněk // Discrete Applied Mathematics. — 2009. — Vol.157, Iss.5. — PP. 971–981.
10. Chen, W.-J. High payload steganography mechanism using hybrid edge detector / W.-J. Chen, C.-C. Chang, T. Hoang Ngan Le // Expert Systems with Applications. — 2010. — Vol.37, Iss.4. — PP. 3292–3301.
11. Cetin, O. A new steganography algorithm based on color histograms for data embedding into raw video streams / O. Cetin, A. Turan Ozcerit // Computers & Security. — 2009. — Vol.28, Iss.7. — PP. 670–682
12. Eslami, Z. Secret image sharing based on cellular automata and steganography / Z. Eslami, S.H. Razzaghi, J. Zarepour Ahmadabadi // Pattern Recognition. — 2010. — Vol.43, Iss.1. — PP. 397–404.
13. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. — 2011. — Том 35, №2. — С. 262–267.
14. Карпінець, В.В. Вирішення проблеми зменшення рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків / В.В. Карпінець, Ю.Є. Яремчук // Інформатика та математичні методи в моделюванні. — 2011. — Том 1, №2. — С. 131–140.
15. Маракова, И.И. Повышение эффективности сокрытия информации для систем с зашумленными каналами связи / И.И. Маракова, А.А. Яковенко // Інформатика та математичні методи в моделюванні. — 2011. — Том 2, №1. — С. 5–17.
16. Кобозева, А.А. Проблема выбора контейнера в компьютерной стеганографии / А.А. Кобозева // Захист інформації. — 2007. — №4. — С. 63–75.
17. Кобозева, А.А. Общий подход к оценке свойств стеганографического алгоритма, основанный на теории возмущений / А.А.Кобозева // Информационные технологии и компьютерная инженерия. — 2008. — №1(11). — С.164–171.
18. Кобозева, А.А. Оценка чувствительности стегосообщения к возмущающим воздействиям / А.А. Кобозева, Е.В. Нариманова // Системні дослідження та інформаційні технології. — 2008. — №3. — С. 52–65.
19. Кобозева, А.А. Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / А.А. Кобозева, О.В. Рыбальский, Е.А. Трифонова // Вісник Східноукраїнського національного університету ім. В. Даля. — 2008. — №8(126), Ч.1. — С. 62–72.
20. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
21. Бахвалов, Н.С. Численные методы [Текст] : учебное пособие для студентов физико-математических специальностей вузов / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — 8-е изд. — М. : Физматлит ; Л. : Невский диалект, 2000. — 622 с.
22. Парлетт, Б. Симметричная проблема собственных значений: численные методы [Текст] / Б. Парлетт; Пер. с англ. Х.Д. Икрамов, Ю.А. Кузнецов. — М. : Мир, 1983. — 382 с.
23. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах / А.А.Кобозева // Вісник Східноукраїнського національного університету ім. В. Даля. — 2006. — №9(103). — С. 74–82.
24. Кобозева, А.А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы / А.А. Кобозева // Праці УНДІРТ. — 2006. — №4(48). — С. 44–52.
25. Кобозева, А.А. Повышение эффективности метода обнаружения фальсификации цифрового изображения, основанного на анализе сингулярных чисел матрицы / А.А. Кобозева, Е.А. Трифонова // Труды Одесского политехнического университета. — 2008. — №1(29). — С. 183–190.

ТЕОРІЯ ЗБУРЕНЬ ЯК ОСНОВА ЗАГАЛЬНОГО ПІДХОДУ ДО ОЦІНКИ ЧУТЛИВОСТІ СТЕГАНОПОВІДОМЛЕНЬ

А.А. Кобозєва, О.В. Наріманова

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

Розроблено загальний математичний підхід до оцінки чутливості стеганоповідомлень до збурних дій, що не залежить від використовуваного стеганографічного алгоритму, області вбудови секретної інформації, області аналізу стеганоповідомлення – просторової або частотної. Основними математичними інструментами є матричний аналіз і теорія відносних збурень. Пропонується спосіб оцінки захищеності секретної інформації, вбудованої в контейнер – цифрове зображення. Розроблено спосіб кількісної оцінки чутливості стеганоповідомлення до збурних дій, що використовується для рішення задачі про вибір контейнера із скінченної множини контейнерів для заданого секретного повідомлення. Отримуване рішення забезпечує найменшу чутливість стеганоповідомлення до збурних дій, тобто найбільшу ефективність процесу декодування додаткової інформації, оцінювану за допомогою об'єму відновленої інформації.

Ключові слова: стеганоповідомлення, збурна дія, чутливість, матриця, власне значення, власний вектор

PERTURBATION THEORY AS A BASIS OF GENERAL APPROACH TO EVALUATE SENSITIVITY OF STEGO MESSAGES

Alla A. Kobozeva, Elena V. Narimanova

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

The general mathematical approach, based on matrix theory and perturbation theory, to evaluate sensitivity of stego messages is developed. Proposed approach does not depend on the used steganography algorithm, area of hidden information, analyzed domain – spatial or frequency. Method to evaluate immunity of hidden information in cover (for example, image) is developed. The results of computational experiments are presented.

Keywords: stego message, perturbation, sensitivity, matrix, eigenvalue, eigenvector