15. *Trajkovich M. and Handley M.* Fast corner detection // Image and Vision Computing. – 1998, No. 16. – pp. 75–87.

16. *Rad A.A., Faez K. and Qaragozlou N.* Fast Circle Detection Using Gradient Pair Vectors // Proc. VIIth Digital Image Computing, Sydney, Australia. – 2003. – pp. 879–887.

17. *Moravec H.* Obstacle avoidance and navigation in the real world by a seeing robot rover // Technical Report CMU-RI-TR-3, Carnegie-Mellon University, Robotics Institute. – 1980.

18. *Harris C. J., Stephens M.* A combined corner and edge detector // Plessey Research Roke Manor, UK. - Proc. 4th Alvey Vision Conferences, Manchester. – 1988. – pp. 147–151.

19. *Bertin E., Marchand-Maillet S., Chassery J-M.* Optimization in Voronoi Diagrams // Kluwer Academic Publishers. – 1994. – pp. 209–216.

20. *Delaunay B.* Sur la sphère vide // Izvestia Akademii Nauk SSSR, Otdelenie Matematicheskikh i Estestvennykh Nauk. – 1934, No. 7. – pp. 793-800.

21. *Скворцов А.В.* Триангуляция Делоне и её применение. – Томск: Изд-во Том. ун-та, 2002. – 128 с.

22. *Hernandez J. R.,Perez-Gonzalez F.* Statistical analysis of watermarking schemes for copyright protection of images // Proceedings of the IEEE. – 1999. – Vol. 87, No. 7. – pp. 1142–1166.

23. *Wiener N.* The Extrapolation, Interpolation and Smoothing of Stationary Time Series. – New York: The Technology Press of MIT and J. Wiley, 1949. – 163 p.

24. *Duric Z., Johnson N.F.* Recovering watermarks froms images // Information and Software Engineering Tehcnical Report, San Diego. –1999. – CA 92152-5000.

25. *Sun Q., Wu J., and Deng R.* Recovering modified watermarked image with reference to originale image // In Proc. SPIE. – 1999. – pp. 415–424.

УДК 004.056.5: 518: 512.624.3 **Кобозева А.А.**

ПРОБЛЕМА ВЫБОРА КОНТЕЙНЕРА ДЛЯ ЗАДАННОГО СЕКРЕТНОГО СООБЩЕНИЯ В КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Введение

Появление глобальных компьютерных сетей, интенсивное развитие и распространение компьютерных технологий сделало недопустимо простым получение доступа к одному из ценнейших предметов современной жизни – информации. Поэтому в настоящий момент во всем мире назрел вопрос разработки методов защиты информации, представленной в цифровом виде, среди которых важнейшее место занимают методы криптографии и стеганографии.

Целью криптографии [1] является сокрытие содержимого сообщений за счет их шифрования. Однако возникает ряд ситуаций в компьютеризированных системах хранения, обработки, приема, передачи информации, когда применение криптографических методов не решает возникающих проблем. Одним из выходов из подобных ситуаций является использование методов цифровой стеганографии [2,3]. 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. В настоящий момент наибольшего развития достигло практическое приложение стеганографии, которое часто не имеет под собой строгого теоретического обоснования.

Одной из часто встречающихся в стеганографии задач является задача о выборе для заданного секретного сообщения наилучшего в некотором смысле ОС, или контейнера, из имеющегося конечного множества контейнеров. Одним из основных требований, выдвигаемых к стегосообщению, является требование его малой чувствительности к любым возмущающим воздействиям. Стегосообщение будем называть чувствительным, если малые возмущающие воздействия вызывают значительный рост вероятности возникновения ошибок при декодировании, и нечувствительным в противном случае.

До сих пор в открытой печати не был представлен общий математический подход, позволивший бы независимо от конкретики стегоалгоритма оценить свойства получаемого им стегосообщения, а также провести априорное сравнение различных стегосообщений с точки зрения их чувствительности к возмущающим воздействиям, используя для этого значения некоторых параметров, однозначно характеризующих любое ОС и любое стегосообщение.

Целью настоящей работы является разработка новой универсальной методики априорного качественного сравнения чувствительности различных стегосообщений к возмущающим воздействиям на основе матричного анализа, что даст возможность выбора из конечного имеющегося набора ОС такого контейнера, который обеспечит наименьшую чувствительность получаемого на его основе стегосообщения при заданном секретном сообщении.

Стегопреобразование как возмущение спектра и собственных векторов матрицы основного сообщения

В качестве ОС для удобства и простоты изложения рассматривается изображение в градациях серого, прямоугольную (или квадратную) матрицу которого обозначим F.

Погружение ДИ в ОС, или стегопреобразование ОС, независимо от способа и области этого погружения, можно представить как возмущение ΔF исходной матрицы F. Результатом погружения ДИ в ОС является стегосообщение, матрица которого $\overline{F}$ очевидно удовлетворяет соотношению:

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

Формула (1) дает матричное представление для произвольного стегопреобразования. Из (1) вытекает истинность следующего утверждения:

Утверждение 1. Любое 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. Тогда имеет место следующее утверждение:

Утверждение 2. Стегопреобразование исходного ОС, а также любые преобразования стегосообщения при его транспортировке или хранении, включая активные атакующие действия, эквивалентным образом представимы в виде элементарных матричных операций [4].

Для достижения поставленной цели определим набор параметров, которые

а) однозначно и всесторонне характеризуют любое ОС и стегосообщение, независимо от того, каким именно способом это стегосообщение было получено;

б) по изменению которых однозначно можно судить о мере возмущения ОС, стегосообщения.

Поскольку математической моделью ОС является матрица, а все преобразования над ОС и стегосообщением могут быть представлены в эквивалентном матричном виде, то в качестве искомого набора характеристик можно использовать множество сингулярных чисел

и соответствующих сингулярных векторов матрицы, спектр и множество собственных векторов матрицы [4]. Отдадим предпочтение второму набору параметров для симметричной квадратной матрицы F размерности n ОС в силу следующих замечений:

1) построение спектрального разложения симметричной матрицы обладает рядом преимуществ в вычислительном смысле по сравнению с построением сингулярного разложения для матрицы произвольной структуры той же размерности [5,6];

2) собственные значения симметричной квадратной матрицы являются хорошо обусловленными [7], т.е.

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

где $\lambda_j(\bullet)$ - собственные значения соответствующей матрицы, $\|\bullet\|_2$ - спектральная матричная норма [5], т.е. задача вычисления собственных значений симметричной матрицы не является чувствительной к возмущениям в исходных данных [6], чего нельзя утверждать в общем случае для несимметричных матриц.

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

$$F=\begin{pmatrix}a_{11}\,a_{12}\,a_{13}\ldots a_{1n}\\ a_{21}\,a_{22}\,a_{23}\ldots a_{2n}\\ a_{31}\,a_{32}\,a_{33}\ldots a_{3n}\\ \ldots\ldots\ldots\ldots\\ a_{n1}\,a_{n2}\,a_{n3}\ldots a_{nn}\end{pmatrix}\rightarrow FV=\begin{pmatrix}a_{11}\,a_{12}\,a_{13}\ldots a_{1n}\\ a_{12}\,a_{22}\,a_{23}\ldots a_{2n}\\ a_{13}\,a_{23}\,a_{33}\ldots a_{3n}\\ \ldots\ldots\ldots\ldots\\ a_{1n}\,a_{2n}\,a_{3n}\ldots a_{nn}\end{pmatrix},FN=\begin{pmatrix}a_{11}\,a_{21}\,a_{31}\ldots a_{n1}\\ a_{21}\,a_{22}\,a_{32}\ldots a_{n2}\\ a_{31}\,a_{32}\,a_{33}\ldots a_{n3}\\ \ldots\ldots\ldots\ldots\\ a_{n1}\,a_{n2}\,a_{n3}\ldots a_{nn}\end{pmatrix} \tag{3}$$

Формула (3) дает принципиальную возможность рассматривать в качестве матрицы ОС симметричную матрицу, что и делается ниже.

Пусть E^* - матрица произвольного возмущения, которому подвергается ОС. В общем случае $E^*\neq\left(E^*\right)^T$. Матрице E^* поставим в соответствие две симметричных матрицы EV, EN той же размерности, используя правило (3). При этом EV - матрица возмущения для FV, а EN - для FN. Исходя из этого, далее матрица произвольного возмущения рассматривается как симметричная.

Формирование матрицы стегосообщения происходит с использованием верхнего треугольника FV и нижнего треугольника матрицы FN, которые несут в себе непосредственно информацию об ОС.

Связь чувствительности стегосообщения и возмущений собственных векторов матрицы контейнера

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

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

-спектральное разложение (СР) матрицы A [5] (здесь $\Lambda=diag(\lambda_1,\ldots,\lambda_n)$, $U=[u_1,\ldots,u_n]$). В общем случае СР определяется неоднозначно.

Спектральное разложение (4) назовем нормальным, если элементы матрицы Λ удовлетворяют соотношению: $|\lambda_1|\ge\ldots\ge|\lambda_n|$, а собственные вектора $u_i,\ i=\overline{1,n}$,

лексикографически положительны, т.е. первая ненулевая компонента каждого вектора положительна. Имеет место следующая теорема.

Теорема 1. Пусть A – невырожденная симметричная $n \times n$-матрица, модули собственных значений которой попарно различны. Тогда для нее существует единственное нормальное спектральное разложение (НСР).

Доказательство. Поскольку модули собственных значений A попарно различны, то каждое из собственных значений имеет кратность, равную единице, которая определяет и размерность любого собственного подпространства матрицы A [7]. Тогда для каждого λ_i, $i = \overline{1,n}$, нормированный базис такого подпространства может определяться двумя способами: это вектора единичной длины противоположных направлений. Очевидно, только один из них является лексикографически положительным. Таким образом, столбец матрицы U, отвечающий собственному значению λ_i, определится однозначно, кроме того, все столбцы U попарно ортогональны [7]. Порядок столбцов однозначно соответствует порядку элементов диагонали Λ.

Далее будем считать, что все рассматриваемые матрицы удовлетворяют условию теоремы. Как показывает вычислительный эксперимент, результаты которого приведены ниже, большинство симметричных матриц, которые ставятся в соответствие матрицам реальных изображений, удовлетворяют условию теоремы 1. Более того, при стандартном разбиении матрицы изображения на квадратные блоки фиксированной размерности лишь сравнительно небольшое количество блоков исключаются из рассмотрения в силу вырожденности матрицы. Если же матрица не является вырожденной, то, как правило, она не имеет кратных собственных значений, что позволяет построить для нее нормальное спектральное разложение.

Любое преобразование, в частности стегопреобразование матрицы ОС, определенным образом возмутит ее спектр и (или) собственные вектора, однозначно определяемые НСР. Очевидно имеет место следующее утверждение:

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

Стегопреобразование ОС с симметричной матрицей A, а также любое преобразование стегосообщения, должны обеспечивать надежность восприятия стегосообщения, т.е. настолько мало возмутить матрицу ОС, чтобы зрительно это возмущение оказалось незаметным. Тогда из утверждения 1 непосредственно вытекает, что необходимым условием обеспечения надежности восприятия стегосообщения является малость любой нормы матрицы возмущения ΔA матрицы A ОС. В силу соотношения (2), возмущения всех собственных значений матрицы ОС при стегопреобразовании, а также при любом преобразовании стегосообщения, обеспечивающем его надежность восприятия, необходимо будут иметь малые значения, а, значит, являются нечувствительными к любым малым возмущающим воздействиям, независимо от того, чувствительным или нечувствительным окажется полученное стегосообщение, а потому качественная оценка чувствительности стегосообщения в зависимости от возмущений спектра окажется затрудненной, чего нельзя сказать о возмущениях собственных векторов, определяемых НСР матрицы ОС. Исходя из этого, основное внимание обратим на установление связи между возмущениями собственных векторов и чувствительностью получаемого стегосообщения к возмущающим воздействиям.

Одной из важнейших характеристик собственного значения λ_i является число

$$gap(i, A) = \min_{i \neq j} |\lambda_j - \lambda_i|, \tag{5}$$

называемое отделенностью λ_i [5].

Назовем абсолютной отделенностью собственного значения λ_i число, определяемое в соответствии с формулой:

$$gap_{abs}(i,A) = \min_{i \neq j} \left\| |\lambda_j| - |\lambda_i| \right\|. \quad (6)$$

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

Доказательство. Пусть $\overline{A}$ - симметричная матрица стегосообщения, НСР которой в соответствии с формулой (4) представляется в виде: $\overline{A} = \overline{U}\overline{\Lambda}\overline{U}^T$; E - некоторое возмущение $\overline{A}$ (например, в результате пересылки стегосообщения по каналу связи, отличному от идеального), $E = E^T$. НСР $\overline{A} + E$ можно представить в виде: $\overline{A} + E = \overline{\overline{U}}\,\overline{\overline{\Lambda}}\,\overline{\overline{U}}^T$. Пусть $\overline{u}_i, \overline{\overline{u}}_i$ - нормированные исходный и возмущенный собственные векторы, отвечающие $i-му$ собственному значению, а θ_i - острый угол между ними. Тогда имеет место соотношение [5]:

$$\sin\theta_i \leq \frac{2\|E\|_2}{gap(i,\overline{A})} \quad (7)$$

при условии, что $gap(i,\overline{A}) \neq 0$.

Сравнивая (5) и (6), используя элементарные свойства модуля, получим:

$$gap(i,\overline{A}) \geq gap_{abs}(i,\overline{A}). \quad (8)$$

Тогда из (7) с учетом (8) вытекает:

$$\sin\theta_i \leq \frac{2\|E\|_2}{gap_{abs}(i,\overline{A})}. \quad (9)$$

Собственный вектор назовем чувствительным, если даже малое возмущающее воздействие может привести к значительному возмущению вектора, т.е. значительному углу его отклонения от первоначального положения. Из соотношения (9) непосредственно вытекает, что мерой чувствительности [5] собственного вектора является величина абсолютной отделенности соответствующего ему собственного значения: собственный вектор тем менее чувствителен к возмущению E, чем больше абсолютная отделенность его собственного значения.

При погружении ДИ в ОС собственные вектора матрицы A ОС возмутятся, отклонившись от первоначального положения на некоторые углы (конечно, если алгоритм погружения не базируется на модификации лишь собственных значений, при котором собственные вектора в НСР остаются неизменными, как, например, в [8]. Этот случай требует отдельного обсуждения, которое не проводится в настоящей работе). Совокупность этих возмущений, в соответствии с утверждением 3, является представлением для погруженной информации. Чувствительность полученного стегосообщения, таким образом, определяется чувствительностью возмущенных при стегопреобразовании собственных векторов матрицы A: чтобы сохранить неизменной погруженную ДИ, их углы поворота от первоначального положения, которое они занимали в матрице ОС, должны остаться неизменными. В соответствии с (9) эти собственные вектора, а, значит, и стегосообщение в целом, будут нечувствительными к малым возмущающим воздействиям, если соответствующие собственные значения матрицы $\overline{A}$ имеют наибольшие абсолютные отделенности: такие собственные вектора менее всего «пострадают» при любых

возмущающих воздействиях, а, значит, менее всего изменят свои возмущения, полученые при стегопреобразовании и сохранят ДИ.

Замечание. Теорема 2 дает достаточное, но не необходимое условие для обеспечения малой чувствительности стегосообщения к возмущающим воздействиям. Действительно, правая часть неравенства (9) дает лишь верхнюю границу для угла поворота собственного вектора. Если эта правая часть и не имеет малого значения (в том случае, если $gap_{abs}(i,\overline{A})$ невелико), это, вообще говоря, не гарантирует, что угол отклонения θ_i соответствующего собственного вектора будет велик. Однако, как показывают результаты вычислительного эксперимента, на практике обратная пропорциональная зависимость между чувствительностью собственного вектора, численным эквивалентом которой является величина угла поворота этого вектора, и абсолютной отделенностью соответствующего собственного значения сохраняется в подавляющем большинстве случаев.

Следствие 1. Если возмущенные в результате стегопреобразования ОС собственные вектора соответствуют собственным значениям матрицы стегосообщения с малой абсолютной отделенностью, то полученное стегосообщение оказывается *чувствительным* к любым возмущающим воздействиям, что может привести к недостаточной эффективности декодирования ДИ.

Следствие 2. Необходимым условием чувствительности стегосообщения к любым возмущающим воздействиям является соответствие возмущенных в результате стегопреобразования ОС собственных векторов собственным значениям матрицы стегосообщения с малой абсолютной отделенностью.

Следствие 3. Абсолютная отделенность собственных значений матрицы стегосообщения, отвечающих возмущенным при стегопреобразовании ОС собственным векторам, является мерой чувствительности полученного стегосообщения к возмущающим воздействиям.

Как было отмечено выше, если ΔA - матрица возмущения ОС A при погружении ДИ, то оценка величины возмущения ΔA в соответствии с любой матричной нормой, в частности, $\|\Delta A\|_2$, необходимо мала. В соответствии с (2), поскольку возмущение собственных значений матрицы ОС A при стегопреобразовании также окажется малым, это приведет к малому изменению абсолютных отделенностей собственных значений матрицы стегосообщения $\overline{A}$ по сравнению с абсолютными отделенностями соответствующих собственных значений A, оставляя неизменной качественную картину: те собственные значения, которые имели большую (малую) абсолютную отделенность в A, будут соответствовать собственным значениям $\overline{A}$, имеющим большую (малую) абсолютную отделенность. Таким образом, имеет место

Следствие 4. Достаточным условием обеспечения малой чувствительности стегосообщения к различным возмущениям является соответствие возмущенных при стегопреобразовании ОС собственных векторов собственным значениям матрицы ОС, имеющим наибольшую абсолютную отделенность.

Вывод

Чувствительность стегосообщения к возмущающим воздействиям однозначно определяется возмущениями собственных векторов матрицы ОС при стегопреобразовании. Исходя из локализации и абсолютных значений этих возмущений возможно сделать качественные априорные оценки чувствительности стегосообщения к произвольным возмущающим воздействиям.

Пусть для заданного секретного сообщения из имеющегося конечного множества ОС нужно выбрать такое, которое бы порождало стегосообщение, чувствительность которого к любым возмущающим воздействиям была бы наименьшей. Методы погружения и декодирования ДИ для всех ОС одинаковые.

Пусть E - матрица, являющаяся выражением возмущающего воздействия, которому подверглось стегосообщение, обеспечивающего его надежность восприятия.

В неравенстве (9) $\|E\|_2$ участвует в оценке возмущения каждого собственного вектора. Заметим, что если правая часть (9) превзойдет единицу, т.е. $\|E\|_2 \geq \frac{gap_{abs}(i,\overline{A})}{2}$, то оценка приобретет вид $\sin\theta_i \leq 1$, т.е. дает возможность углу θ_i принимать любое значение, вплоть до $\approx \pi$, а сделать заключение о чувствительности или нечувствительности этого вектора в данном случае не представляется возможным. Таким образом, мера чувствительности собственных векторов будет, вообще говоря, зависеть от непосредственной величины возмущения $\|E\|_2$: для одних возмущающих воздействий вектор будет менее чувствительным, а для других окажется более чувствительным. Однако сравнение чувствительности различных собственных векторов одного стегосообщения между собой не зависит от величины $\|E\|_2$: при конкретном возмущающем воздействии с определенным значением $\|E\|_2$ это сравнение происходит в соответствии с соотношением только абсолютных отделенностей собственных значений.

Замечание

Достаточным условием обеспечения малой чувствительности стегосообщения к возмущающему воздействию является соответствие возмущенных при стегопреобразовании ОС собственных векторов собственным значениям матрицы стегосообщения, абсолютная отделенность которых значительно превосходит спектральную норму матрицы возмущения стегосообщения.

Конечно, заранее точное значение нормы матрицы возмущения бывает известно редко. Однако, в силу требования надежности восприятия стегосообщения, как уже было отмечено выше, эта норма мала, поэтому вместо $\|E\|_2$, фигурирующей в предыдущем замечании, там может использоваться числовая константа, являющаяся верхней границей для $\|E\|_2$, обеспечивающей надежность восприятия стегосообщения, или получаемая из каких-либо других рассуждений и требований.

Определение 1. Будем говорить, что собственное значение λ_i имеет достаточную (недостаточную) абсолютную отделенность по отношению к возмущению E, если

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

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

Только для защищенных собственных векторов имеется потенциальная возможность численно оценить максимальное возмущение при помощи неравенства (9). Для незащищенного собственного вектора такой возможности не существует: хотя неравенство (9) остается справедливым в любом случае, для незащищенного собственного вектора оно не несет полезной информации о возможном возмущении (угле поворота), превращаясь в тривиальное.

Очевидно, что собственные вектора, отвечающие собственным значениям с большими (максимальными) абсолютными отделенностями, являются защищенными от практически любого, сохраняющего надежность восприятия, возмущения.

Согласно утверждению 3, погруженную информацию можно представить в виде совокупности возмущений всех отдельно взятых собственных векторов матрицы ОС. Представим ситуацию, когда некоторый собственный вектор не отклонился от своего первоначального положения при стегопреобразовании ОС, погружение ДИ его «не

каснулось», он не участвует в хранении секретной информации. Потенциально имеется возможность к уже погруженной ДИ добавить еще некоторый объем секретной информации, сохраняя надежность восприятия стегосообщения, проводя ее погружение непосредственно при помощи возмущения этого вектора. Рассмотрим другую возможную ситуацию. Предположим, что некоторая информация погружена в ОС, что привело лишь к очень незначительному возмущению (углам отклонения) собственных векторов. В этом случае возможно осуществить погружение некоторого дополнительного объема секретной информации, приводящего к бóльшему возмущению собственных векторов (к бóльшим углам отклонения), если при этом сохранится надежность восприятия стегосообщения. Исходя из таких рассуждений, сделаем следующее допущение: будем считать, что, чем больше угол отклонения собственного вектора при стегопреобразовании, тем бóльшая «часть» ДИ хранится в возмущении этого вектора. Собственные вектора как бы «распределяют между собой» погруженную ДИ. Конечно, такое допущение будет не совсем оправданным, если алгоритм погружения связан с непосредственной модификацией собственных векторов, например, изменением знаков определенных компонент этих векторов [9]. Однако это лишь незначительно сужает область допущения и является предметом исследования другой работы автора.

Определение 3. Часть ДИ, результатом погружения которой явилось возмущение защищенных собственных векторов, будем называть информацией, защищенной от возмущения E (ЗИ).

Стегосообщения тем менее чувствительно, чем большему возмущению при стегопреобразовании подверглись собственные вектора, отвечающие собственным значениям с максимальными абсолютными отделенностями, т.е. чем бóльшая часть информации попала для хранения в упомянутые собственные вектора, т.к. эти вектора вместе с хранимой в их возмущениях информацией окажутся защищенными от любого, сохраняющего надежность восприятия стегосообщения, возмущающего воздействия.

При данном алгоритме декодирования вероятность большей эффективности декодирования менее чувствительного к возмущающим воздействиям стегосообщения выше, чем для стегосообщения, чувствительность которого больше. Очевидным является факт, следующий из вышеизложенного: если стегосообщение нечувствительно к возмущающим воздействиям, т.е. при стегопреобразовании были возмущены только собственные вектора, отвечающие собственным значениям с максимальными абсолютными отделенностями, то, независимо от конкретики алгоритма декодирования, эффективность здесь будет наиболее высокой по сравнению с другими стегосообщениями, т.к. погруженная информация осталась практически неизменной.

Учитывая результаты исследований, проведенных в [9], необходимо отметить также, что чувствительность стегосообщения для определенных стегоалгоритмов зависит и от sign-чувствительности возмущенных стегопреобразованием собственных векторов матрицы ОС.

Определение 4. Вектор $x \in R^n$ будем называть sign-чувствительным , если даже малые возмущения исходных данных могут привести к изменению знаков координат вектора x, и sign-нечувствительным в противном случае.

Предположим, что стегоалгоритм основан на установлении определенного соотношения знаков некоторых элементов собственных векторов, как, например, в [10]. В этом случае возможна ситуация, когда, даже в случае сильной чувствительности собственного вектора, хранящего в своем возмущении некоторую «часть» погруженной ДИ, достаточно большой угол поворота в n-мерном пространстве при возмущающем воздействии может не вывести его за пределы координатного ортанта, в котором он находится, а, значит, не изменит знаков его элементов, т.е. сохранит погруженную информацию без изменения. Рассмотрим другую возможную ситуацию. Пусть теперь рассматриваемый собственный вектор обладает малой чувствительностью. В общем случае это не гарантирует, что малый угол его отклонения при возмущающем воздействии не

выведет собственный вектор в другой координатный ортант, поменяв знак соответствующей координаты, что вероятно повлечет за собой ошибку при декодировании. Таким образом, очевидно, что определенной связи между чувствительностью и sign-чувствительностью собственных векторов, вообще говоря, не существует: нельзя сделать вывод об одном виде чувствительности по наличию или отсутствию другого.

Пусть собственный вектор является нечувствительным, т.е. при малых возмущающих воздействиях он практически не отклоняется от своего первоначального положения, как собственные вектора, отвечающие собственным значениям с максимальной абсолютной отделенностью, тогда, очевидно, вероятность его sign-чувствительности и выхода за пределы координатного ортанта, в котором он находится, будет мала, и, значит, определяющей для достаточности обеспечения нечувствительности стегосообщения в общем случае является нечувствительность собственного вектора.

Вывод

Нечувствительность возмущенных в процессе стегопреобразования собственных векторов является достаточным, но не необходимым условием эффективного декодирования ДИ.

Методика выбора контейнера, обеспечивающего для данного секретного сообщения малую чувствительность стегосообщения к возмущающим воздействиям

Предлагаемая новая методика выбора контейнера с целью обеспечения наименьшей чувствительности получаемого стегосообщения к возмущающим воздействиям заключается в исследовании возмущений собственных векторов матрицы ОС вследствии стегопреобразования на основании нормальных спектральных разложений исходной матрицы и матриц стегосообщений. Основные шаги такого исследования:

1) Пусть $A_1, A_2, ..., A_k$ - симметричные матрицы, отвечающие имеющемуся набору контейнеров, из которых предстоит сделать выбор. Погружая заданное секретное сообщение в каждый контейнер, получаем соответствующие стегосообщения $\overline{A}_1, \overline{A}_2, ..., \overline{A}_k$. Строим нормальные спектральные разложения:

$$A_j = U_j \Lambda_j U_j^T,\ \overline{A}_j = \overline{U}_j \overline{\Lambda}_j \overline{U}_j^T,\ j = \overline{1,k};$$

2) для каждого ОС $A_j, j = \overline{1,k}$ среди собственных векторов определяем те, которые претерпели возмущения при стегопреобразовании, вычисляем вектор этих возмущений, который однозначно характеризует углы поворота собственных векторов от первоначальных положений, (далее обозначаем: $NORMA_j, j = \overline{1,k}$). Чем больше значение i-го элемента вектора $NORMA_j$, т.е., чем больше возмущение i-го собственного вектора j-го ОС A_j, тем большая часть ДИ хранится в возмущении этого вектора. Для количественной визуализации этого вектор $NORMA_j$ нормируется. Результатом является вектор $CHASTDI_j$, i-ая компонента которого является выражением для той части ДИ, которая хранится в возмущении i-го собственного вектора. Если компоненты $CHASTDI_j$ умножить на 100%, то получим распределение погруженной информации по собственным векторам, выраженное в процентах.

3) для каждого стегосообщения $\overline{A}_j, j = \overline{1,k}$, используя НСР, определяем абсолютные отделенности собственных значений. Среди собственных значений находим те, которые имеют достаточную абсолютную отделенность по отношению к предполагаемому возмущению E;

4) используя результаты шага 3), определяем для каждого $\overline{A}_j, j = \overline{1,k}$ защищенные от предполагаемого возмущения собственные вектора;

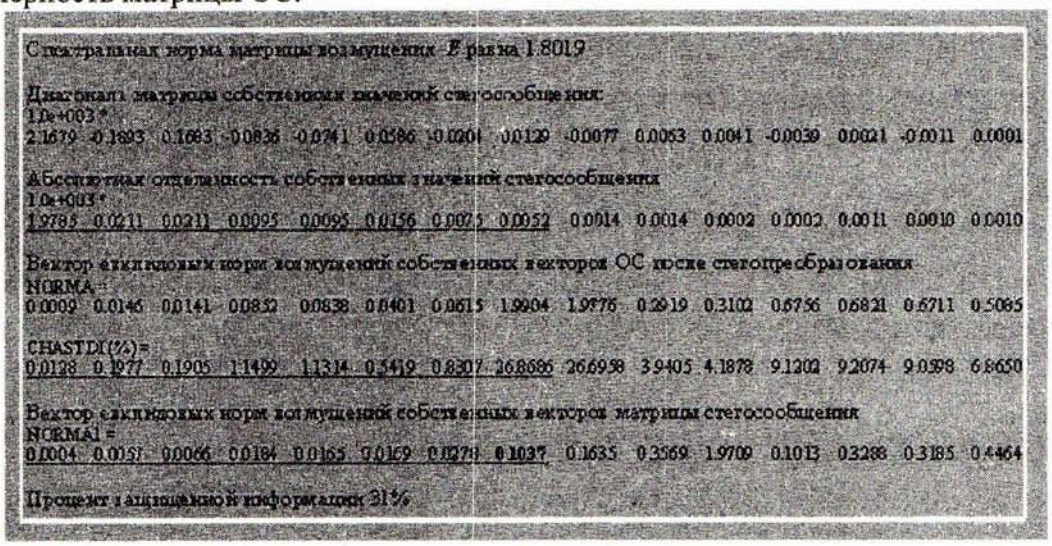
5) для каждого стегосообщения $\overline{A_j}, j=\overline{1,k}$, определяем объем защищенной информации, как сумму элементов вектора $CHASTDI_j$, отвечающих защищенным собственным векторам.

6) В качестве искомого ОС используем то, которое порождает стегосообщение с максимальным объемом защищенной информации.

Для иллюстрации полного объема исследования одного стегосообщения рассмотрим пример. Пусть в качестве контейнера используется главная подматрица размерности 15×15 матрицы изображения CELL (рис.1). На рисунке приведены результаты исследования стегосообщения, полученного при погружении случайно сформированного бинарного сообщения LSB-алгоритмом [2]. Случайным образом сформирована матрица возмущений для стегосообщения, спектральная норма которой меньше двух. В векторе абсолютных отделенностей собственных значений стегосообщения подчеркиванием выделены те, отделенность которых достаточна. Аналогично на рисунке выделены защищенные собственные вектора. Как и предполагалось, исходя из теоретических рассуждений, защищенные собственные вектора подверглись самому малому отклонению при возмущающем воздействии (вектор *NORMA*1 на рис.1). Действительно, наибольший угол поворота из всех защищенных векторов будет у вектора $\overline{u_8}$ (на рисунке жирным шрифтом), но он составляет менее 6°. В то время, как для незащищенного вектора $\overline{u_{11}}$ угол поворота будет больше 160°.

Замечание

Данная методика может быть применена не только для выбора контейнера при заданном секретном сообщении. Пусть имеется некоторое ОС, которое предварительно подвергается стандартному разбиению на блоки фиксированной малой размерности. Предложенная методика может быть применена к каждому блоку в отдельности, что даст возможность для данного ОС выбрать блоки, которые будут мало чувствительными к 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 как $\underline{O}(n^2)$, где n - размерность матрицы ОС.


Спектральная норма матрицы возмущения E равна 1.8019

Диагональ матрицы собственных значений стегосообщения:
1.0e+003 *
2.1679 -0.1893 0.1083 -0.0836 -0.0241 0.0386 -0.0201 0.0129 -0.0077 0.0063 0.0041 -0.0039 0.0021 -0.0011 0.0001

Абсолютная отделенность собственных значений стегосообщения
1.0e+003 *
1.9785 0.0211 0.0211 0.0095 0.0095 0.0156 0.0076 0.0052 0.0014 0.0014 0.0002 0.0002 0.0011 0.0010 0.0010

Вектор евклидовых норм возмущений собственных векторов ОС после стегопреобразования
NORMA =
0.0009 0.0146 0.0141 0.0852 0.0838 0.0401 0.0615 1.9904 1.9776 0.2919 0.3102 0.6756 0.6821 0.6711 0.5085

CHASTDI(%)=
0.0128 0.1977 0.1905 1.1499 1.1314 0.5419 0.8307 26.8686 26.6938 3.9405 4.1878 9.1202 9.2074 9.0598 6.8650

Вектор евклидовых норм возмущений собственных векторов матрицы стегосообщения
NORMA1 =
0.0004 0.0057 0.0066 0.0184 0.0165 0.0159 0.0278 0.1037 0.1635 0.3569 1.9709 0.1013 0.3238 0.3185 0.4464

Процент защищенной информации 31%

Рис.1. Результаты исследования стегосообщения, построенного для главной подматрицы изображения CELL

Результаты вычислительного эксперимента

Основной целью вычислительного эксперимента является практическое опробирование новой методики выбора ОС, порождающего стегосообщение, наименее чувствительное к возмущающим воздействиям, для заданного секретного сообщения, дающее возможность подтверждения теоретических выводов, полученных в п.3.

Вычислительный эксперимент проводился в среде MATLAB. Для случайно сформированного бинарного сообщения, погружение которого осуществлялось при помощи LSB-алгоритма, наилучший контейнер выбирался из 5 возможных изображений: CAMERAMAN.TIF, POUT.TIF, CELL.TIF, MOON.TIF, TIRE.TIF (для наглядности иллюстрации здесь также рассмотрены не целые изображения, а их главные подматрицы размерности 15×15).

Таблица 1 содержит итоговые результаты вычислительного эксперимента. Как видно из результатов эксперимента, эффективность декодирования (количество возникающих при декодировании ошибок) при любой матрице возмущения определяется объемом защищенной от конкретного возмущения информации: чем больше этот объем, тем меньше количество ошибок при декодировании ДИ.

Полученный результат полностью соответствует теоретическим заключениям, проведенным в п.3.

Как видно из таблицы 1, на основе изображения CELL получается наиболее устойчивое к возмущающим воздействиям стегосообщение практически во всех случаях возмущающих матриц, что определяет и наибольшую эффективность декодирования.

Таблица 1

Результаты исследования различных стегосообщений для данного секретного сообщения

Изображение	Норма матрицы возмущения равна 1		Норма матрицы возмущения равна 1.8019		Норма матрицы возмущения равна 2.9754		Норма матрицы возмущения равна 4.8775	
	Объем ЗИ в(%)	Кол-во ошибок при декодировании	Объем ЗИ в(%)	Кол-во ошибок при декодировании	Объем ЗИ в(%)	Кол-во ошибок при декодировании	Объем. ЗИ в(%)	Кол-во ошибок при декодировании
CAMERAMAN	2.8	4	0.005	14	0.005	28	0.005	98
POUT	[illegible]	[illegible]	1.79	13	1.79	25	1.79	88
CELL	31	2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
MOON	12.1	2	0.2	14	0.2	28	0.2	100
TIRE	5.5	3	5.5	13	2	26	0.2	95

Сообщение же CAMERAMAN во всех рассмотренных случаях дает наихудший результат как по чувствительности, так и по количеству ошибок при декодировании (для каждого варианта возмущающей матрицы наилучшее и наихудшее стегосообщение в смысле чувствительности окрашено в голубой и серый цвета соответственно). Секрет такой «стабильности» становится понятен при рассмотрении абсолютных отделенностей собственных значений стегосообщений (табл.2).

Для рассматриваемой главной подматрицы матрицы стегосообщения, сформированного на основе изображения CELL,

наибольшее количество собственных значений имеет сравнительно большие абсолютные отделенности (в таблице эти абсолютные отделенности выделены подчеркиванием), в то время, как для стегосообщения, сформированного на основе изображения CAMERAMAN, такое собственное значение лишь одно, что не может гарантировать достаточного объма защищенной информации при любом возмущении.

Таким образом, пример практической реализации новой предложенной методики выбора стегосообщения, обладающего наименьшей чувствительностью к возмущающим воздействиям, подтверждает теоретические выводы п.3.

Вычислительные затраты для реализации предлагаемого метода сравнимы с количеством арифметических операций для построения спектрального разложения матрицы, т.е. составляет $\underline{O}(n^3)$, где n - размерность матрицы ОС. Это количество операций очевидно может быть уменьшено до $\underline{O}(n^2)$, если матрицы ОС и стегосообщения подвергнуть предварительно стандартному разбиению на блоки фиксированной размерности.

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
POUT	1610.9	212.4	13.7	13.7	18.8	18.8	2.5	2.5	1.2	0.9	0.6	0.6	0.3	0.3	2.7
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
TIRE	45.5810	7.2958	7.2958	0.3644	0.3644	3.9942	0.2177	0.2177	0.2214	0.1409	0.1409	0.2234	0.2234	0.8739	0.8739

Заключение

В работе предложена новая математически обоснованная методика выбора контейнера из имеющегося ограниченного множества контейнеров для заданного секретного сообщения с целью обеспечения наименьшей чувствительности получаемого стегосообщения к возмущающим воздействиям, что никогда не делалось ранее. В качестве математического инструмента построения теоретической базы для предлагаемой методики использовалась теория матриц.

Полученная методика дает возможность формализовать процесс качественного сравнения стегосообщений, независимо от конкретики формирующего их стегоалгоритма.

Список литературы

1. *Мукачев В.А., Хорошко В.А.* Методы практической криптографии.-К.: ООО «Полиграф-Консалтинг», 2005.-215 с.

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

3. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – *К.: МК – Пресс, 2006.- 288 с.*

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

5. *Деммель Дж.* Вычислительная линейная алгебра. – М.: Мир, 2001. - 430 с.

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

7. *Парлетт Б.* Симметричная проблема собственных значений. Численные методы.- М.: Мир, 1983. 384 с.

8. *Кобозева А.А.* Стеганографический метод, основанный на преобразовании спектра симметричной матрицы // Журнал «Праці УНДІРТ».-2006.- №4(48).-С. 44-52.

9. *Кобозева А.А.* Исследование проблемы устойчивости стеганографического алгоритма, основанного на нормальном спектральном разложении матрицы // Збірник «Захист інформації».- 2007.-№1(32).-С.

10. *Кобозева А.А.* Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах // Вісник Східноукраїнського національного університету ім. В.Даля.-2006.-№9(103).- С.74-82.

УДК 621.372.

Лєнков С.В., Іванов Ю.Д., Пампуха І.В., Боряк К.Ф.

ОСОБЛИВОСТІ КОРЕГУЮЧИХ ВЛАСТИВОСТЕЙ СТРУКТУРНО-ЛОГІЧНИХ КОДІВ

Структурно-логічні коди (СЛК) використовують природну логічну надлишковість інфимумних диз'юнктивних нормальних форм (ІДНФ) булевих функцій, які є основою побудови кодів СЛК, для виправлення помилок, які виникли при передачі даних по реальним дискретним каналам, окремо по каналам с незалежними помилками. Основною задачею даної роботи являється встановлення базисних співвідношень між реалізованої кодами СЛК логічної надлишковості і граничним значенням кратності незалежних помилок, що виправляються.

В [1] показано, що в межах мінімального інтервалу декодування (МІД) n-мірного куба E^n, в якості якого приймається грань, тобто підкуб E^2 куба E^n, можливо відновлення будь-якої із чотирьох вершин $E_1^0, E_2^0, E_3^0, E_4^0$, спотвореної помилками кратності $t=1,...,n$.

Обов'язковою умовою виправлення помилок в такій скривленій вершині є коректне визначення 3-х останніх із чотирьох вершин МІД.

Таким чином, в межах МІД можливе виправлення будь-якої $t \le n$ - кратної помилки на довжині n розрядів вершини E^0 куба E^2.

Якщо помилка кратності $n \ge t>1$ спотворює одночасно розряди двох сусідніх вершин, то така помилка виправлена бути не може, оскільки порушується обов'язкова умова коректності 3-х вершин МІД при виправленні четвертої вершини, тобто спотвореними стають 2 вершини МІД.

Пакетна помилка, окремим випадком якої є t-кратна помилка, починається і закінчується завжди, як і t-кратна помилка, помилковим бітом (розрядом). У загальному випадку для пакетної помилки характерна наявність безпомилкових біт у середині пакету помилок, в той час як при t - кратній помилці безпомилкові біти відсутні.

Визначимо ймовірність помилки МІД для випадку, коли спотворена більш ніж одна вершина МІД. Нехай ймовірність неправильного прийому одного блоку (розряду) для каналу з незалежними помилками при рівномірному їх розподілі складе p_0.

При незалежних помилках ймовірність появи деякого числа спотворених біт в межах n розрядів вершини МІД не залежить від взаємного розташування спотворених біт і визначається тільки числом спотворених біт і вірогідністю помилки p_0 одного біта.