УДК 004.056.5: 518: 512.624.3 **Кобозева А.А., Трифонова Е.А.**

УЧЕТ СВОЙСТВ НОРМАЛЬНОГО СПЕКТРАЛЬНОГО РАЗЛОЖЕНИЯ МАТРИЦЫ КОНТЕЙНЕРА ПРИ ОБЕСПЕЧЕНИИ НАДЕЖНОСТИ ВОСПРИЯТИЯ СТЕГОСООБЩЕНИЯ

Аннотация

В работе разработан новый подход к проблеме обеспечения надежности восприятия стегосообщения, основой которого является использование некоторых особенностей спектрального разложения матрицы, а реализация сводится к анализу возмущений собственных векторов и собственных значений матрицы контейнера при его стегопреобразовании. Приводятся результаты вычислительного эксперимента.

1. Введение.

В связи с высокой информатизацией современного общества чрезвычайно актуальной на сегодняшний день является проблема защиты информации (ЗИ), решение которой невозможно без привлечения методов стеганографии.

Общей чертой стеганогафических методов (СМ) является то, что секретные данные, или дополнительной информации (ДИ), встраиваются в некоторый непривлекающий внимания объект, называемый *контейнером* (или *основным сообщением* (ОС)), который затем открыто пересылается адресату по каналу связи или хранится в таком виде. Таким образом, скрытым остается сам факт существования ДИ при ее передаче, хранении и обработке [1,2]. Результатом встраивания ДИ в ОС, или *стегопреобразования* контейнера, является *стегосообщение*.

Основной задачей любого СМ является сохранение в секрете наличия тайного канала передачи информации, в связи с чем СМ должен обеспечивать *надежность восприятия стегосообщения*, т.е. искажение ОС за счет погружения ДИ не должно быть заметно. Таким образом, в систему стеганографической передачи данных включается человек, что вносит дополнительные, непреодоленные до настоящего момента трудности в процесс математической формализации обеспечения рассматриваемого требования, хотя работа в этом направлении ведется очень активно, с привлечением обширного математического аппарата [3,4,5].

Целью настоящей работы является разработка нового подхода к проблеме обеспечения надежности восприятия стегосообщения, основой которого является использование математических особенностей спектрального разложения (СР) матрицы, теоретическое обоснование которых проводится в статье, а также определение достаточных условий обеспечения высокой вероятности надежности восприятия стегосообщения на основе анализа возмущений спектра и собственных векторов матрицы контейнера при стегопреобразовании.

2. Использование теории матриц в компьютерной стеганографии.

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

Погружение ДИ в ОС, независимо от способа и области этого погружения, можно представить как возмущение ΔF исходной матрицы F. Матрица стегосообщения $\overline{F}$ очевидно удовлетворяет соотношению: $\overline{F} = F + \Delta F$, где $\Delta F = f(F)$, т.е. ΔF является некоторой функцией F.

Любые преобразования, которые производятся над стегосообщением при его транспортировке или хранении, включая активные атакующие действия, будем рассматривать как дополнительные возмущения матрицы ОС F, представляя эти преобразования в виде элементарных матричных операций [6].

Определим набор параметров, которые однозначно и всесторонне характеризуют любое ОС и стегосообщение. Поскольку математической моделью изображения является матрица, а все преобразования над ОС и стегосообщением могут быть представлены в эквивалентном матричном виде, то в качестве искомого набора характеристик можно использовать, например, множество сингулярных чисел и соответствующих сингулярных векторов матрицы или спектр и множество собственных векторов (СВ) матрицы [7]. Если бы матрица F ОС была симметричной, то предпочтение следовало бы отдать второму набору параметров в силу следующих замечений:

1) построение СР симметричной матрицы обладает рядом преимуществ в вычислительном смысле по сравнению с построением сингулярного разложения для матрицы произвольной структуры той же размерности [7,8];

2) собственные значения (СЗ) симметричной матрицы являются хорошо обусловленными [9], т.е. $\max\limits_{1\le j\le n}\left|\lambda_j(F)-\lambda_j(F+\Delta F)\right|\le\left\|\Delta F\right\|_2$, где $\lambda_j(\bullet)$-СЗ соответствующей матрицы, $\left\|\bullet\right\|_2$ - спектральная матричная норма (СМН) [7], чего нельзя утверждать в общем случае для несимметричных матриц.

Однако, как правило, матрица F ОС не удовлетворяет свойству: $F=F^T$. Чтобы «исправить» это, поставим в соответствие F две симметричные матрицы той же размерности по следующему правилу:

$$F=\begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{pmatrix} \rightarrow FV=\begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{12} & f_{22} & \cdots & f_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ f_{1n} & f_{2n} & \cdots & f_{nn} \end{pmatrix}, FN=\begin{pmatrix} f_{11} & f_{21} & \cdots & f_{n1} \\ f_{21} & f_{22} & \cdots & f_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{pmatrix} \qquad (1)$$

Формула (1) дает принципиальную возможность рассматривать в качестве матрицы ОС симметричную матрицу, поведение которой описывается ее спектром и СВ, что и делается ниже. Аналогично, матрица произвольного возмущения, которому подвергается ОС, рассматривается как симметричная.

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

3. Достаточные условия обеспечения высокой вероятности надежности восприятия стегосообщения.

Пусть A – произвольная 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.

$$A=U\Lambda U^T \qquad (2)$$

-СР матрицы A [9] (здесь $\Lambda=diag(\lambda_1,...,\lambda_n)$, $U=[u_1,...,u_n]$), в общем случае определяемое неоднозначно. СР (2) назовем *нормальным*, если элементы матрицы Λ удовлетворяют соотношению: $\left|\lambda_1\right|\ge...\ge\left|\lambda_n\right|$, а СВ $u_i,\ i=\overline{1,n}$, *лексикографически положительны*, т.е. первая ненулевая компонента каждого вектора положительна. Имеет место теорема.

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

Доказательство. Из условия теоремы следует, что размерность каждого собственного подпространства матрицы A равна единице [9]. Тогда для любого 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 СЗ λ_i, определится однозначно, кроме того, все столбцы U попарно ортогональны [9]. Порядок столбцов однозначно соответствует порядку элементов диагонали Λ.■

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

В силу однозначности НСР имеет место

Утверждение 1. Любое преобразование, в частности стегопреобразование, матрицы ОС эквивалентным образом представимо в виде возмущения спектра и (или) собственных векторов матрицы ОС, определяемых НСР.

До настоящего времени при анализе уровня визуальных искажений, которые вносятся в контейнер при стегопреобразовании, широко применяются разностные показатели, основывающиеся на различных модификациях отношения «сигнал-шум» [2]: $SNR=\frac{\|F\|_F^2}{\|\Delta F\|_F^2}$; $PSNR=\frac{n^2\max\limits_{i,j} f_{ij}^2}{\|\Delta F\|_F^2}$; $IF=1-\frac{\|\Delta F\|_F^2}{\|F\|_F^2}$, где $\|\bullet\|_F$ - матричная норма Фробениуса [7], хотя слабые места таких показателей давно известны (например, отсутствие корреляции этих показателей со зрением человека). Это объясняется тем, что все существующие модели зрительного восприятия являются лишь частичным и ограниченным отражением зрительной системы человека в силу ее сложности, а показатели искажения, основанные на таких моделях, информация о которых доступна из открытой печати, все еще остаются несовершенными и достаточно сложными в реализации, как, например, предложенные в [3,5].

В упомянутых выше разностных показателях (и не только в них) используется матричная норма Фробениуса. Эта норма не обладает никакими преимуществами по сравнению с любой другой матричной нормой, в частности, СМН, использование которой в некоторых случаях является предпочтительным, о чем будет сказано ниже. Более того, имеет место

Лемма 1. Пусть F произвольная $n\times n$-матрица. Матричные нормы Фробениуса и СМН эквивалентны с константами эквивалентности 1 и $n^{1/2}$, т.е. имеет место неравенство:

$$\|F\|_2 \le \|F\|_F \le n^{1/2}\|F\|_2. \qquad (3)$$

Доказательство. Известно [7], что векторная 2-норма ($\|\bullet\|_2$) и матричная норма Фробениуса (L^2-норма) связаны соотношением: $\|Fz\|_2 \le \|F\|_F\|z\|_2$, где z - вектор длины n. поскольку СМН индуцированна [7] векторной 2-нормой, то $\|F\|_2=\max\limits_{z\ne 0}\frac{\|Fz\|_2}{\|z\|_2}\le\max\limits_{z\ne 0}\frac{\|F\|_F\|z\|_2}{\|z\|_2}=\|F\|_F$, что доказывает левую часть (3).

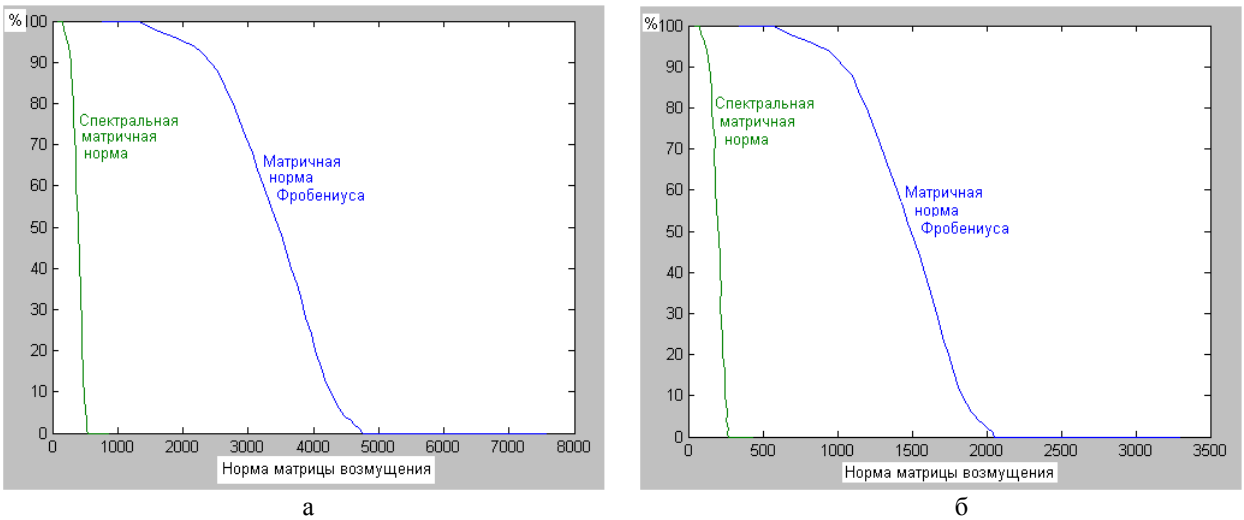
Пусть вектор $z^{(1)}=(1,0,...,0)^T$, тогда $\frac{\|Fz^{(1)}\|_2^2}{\|z^{(1)}\|_2^2}=f_{11}^2+\ldots+f_{n1}^2\le\max\limits_{z\ne 0}\frac{\|Fz\|_2^2}{\|z\|_2^2}$. Аналогично для любого вектора вектора z вида $z^{(k)}=(0,\ldots,0,\underset{k}{1},0,\ldots,0)^T$ имеем:

$$\frac{\|Fz^{(k)}\|_2^2}{\|z^{(k)}\|_2^2}=f_{1k}^2+f_{2k}^2+\ldots+f_{nk}^2\le\max_{z\ne 0}\frac{\|Fz\|_2^2}{\|z\|_2^2},\ k=\overline{1,n}. \qquad (4)$$

Просуммировав неравенства (4) для всех $k=\overline{1,n}$, получим: $\sum_{i,j=1}^{n} f_{ij}^2 \le n \max_{z\neq 0} \frac{\|Fz\|_2^2}{\|z\|_2^2}$, откуда следует правая часть неравенства (3).■

Из леммы 1 непосредственно вытекает, что при малых n значения СМН и нормы Фробениуса сравнимы между собой. Мы вернемся к этому в п. 4.

Поскольку стегопреобразование ОС, а также возмущающие воздействия, которым подвергается стегосообщение, должны обеспечивать надежность его восприятия, то $\|\Delta F\|$ не может быть бесконечно большой (ΔF - матрица возмущения ОС или стегосообщения), т.к. в этом случае достоверным событием окажется нарушение выдвинутого требования. Кроме того, при $\|\Delta F\| \to 0$ вероятность обеспечения надежности восприятия будет стремиться к единице для каждого ОС [10]. Значения упомянутых выше разностных показателей для *заданного* изображения F определяются $\|\Delta F\|_F$: чем меньше $\|\Delta F\|_F$, тем лучше количественный показатель визуального искаженния F, получаемый при использовании каждого из них. Принимая это во внимание, далее будем считать, что, *чем меньше* $\|\Delta F\|_F$, *тем больше вероятность обеспечения надежности восприятия для изображения с матрицей* $F+\Delta F$ *при заданном исходном изображении* F, *причем вместо* $\|\Delta F\|_F$ *можно рассматривать* $\|\Delta F\|_2$. Данная гипотеза подтверждается вычислительным экспериментом. Эксперимент проводился в среде MATLAB с использованием 100 разнообразных как по контрастности, так и по жанру (пейзажи, портреты, натюрморты и др.) изображений одинаковой размерности (300*300 пикселей). Возмущение исходного изображения проводилось при помощи наложения шума (аддитивного гауссова, мультипликативного) с различными характеристиками. Результаты приведены на рис.1, где по оси Oy откладывался процент (от общего числа изображений) зашумленных изображений, для которых соблюдалась надежность восприятия, устанавливаемая при помощи субъективного ранжирования. Рассчеты при построении графиков проводились с использованием СМН и нормы Фробениуса.



а б

а - возмущающее воздействие - аддитивный гауссовский шум; б- возмущающее воздействие - мультипликативный шум

Рис.1. Зависимость количества зашумленных изображений (%), сохранивших надежность восприятия, от нормы матрицы возмущающего воздействия.

Из сказанного выше следует, что для обеспечении достаточно высокой вероятности сохранения надежности восприятия стегосообщения при заданном контейнере СМ

должен обеспечивать малую норму (в частности, Фробениуса, СМН) матрицы возмущения при стегопреобразовании.

В [11] было показано, что если погружение ДИ вызывает возмущения $\delta_{k_1},...,\delta_{k_p}$ СЗ $\lambda_{k_1},...,\lambda_{k_p}$ симметричной матрицы A ОС, то величина возмущения E матрицы контейнера A, вызванного таким стегопреобразованием, не зависит от того, какие именно СЗ были возмущены, а зависит лишь от абсолютной величины этих возмущений в соответствии с формулой: $\|E\|_2 = \max\limits_{1\le j\le p}\left|\delta_{k_j}\right|$ (или $\|E\|_F \le p \max\limits_{1\le j\le p}\left|\delta_{k_j}\right|$).

Теорема 2. Пусть стегопреобразование вызвало возмущение СВ матрицы ОС. Достаточным условием для обеспечения малости нормы матрицы возмущения является соответствие возмущенных СВ малым по модулю СЗ матрицы ОС.

Доказательство. Пусть $\Delta_{k_1},...,\Delta_{k_p}$ - вектора возмущений СВ $u_{k_1},...,u_{k_p}$, отвечающих СЗ $\lambda_{k_1},...,\lambda_{k_p}$. Обозначим $\overline{A}$ матрицу стегосообщения. Для $\overline{A}$ имеет место выражение

$$\overline{A} = \sum_{i=1,i\ne k_1,...,k_p}^{n}\lambda_i u_i u_i^T + \sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}+\Delta_{k_j})(u_{k_j}+\Delta_{k_j})^T = \sum_{i=1}^{n}\lambda_i u_i u_i^T + \tag{5}$$

$$+\sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}\Delta_{k_j}{}^T + \Delta_{k_j}u_{k_j}^T + \Delta_{k_j}\Delta_{k_j}{}^T) = A + \sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}\Delta_{k_j}{}^T + \Delta_{k_j}u_{k_j}^T + \Delta_{k_j}\Delta_{k_j}{}^T)$$

Из (5) получаем:

$$\left\|A-\overline{A}\right\|_2 = \left\|\sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}\Delta_{k_j}{}^T + \Delta_{k_j}u_{k_j}^T + \Delta_{k_j}\Delta_{k_j}{}^T)\right\|_2 \le$$

$$\le \sum_{j=1}^{p}\left|\lambda_{k_j}\right|(\left\|u_{k_j}\right\|_2\left\|\Delta_{k_j}\right\|_2 + \left\|\Delta_{k_j}\right\|_2\left\|u_{k_j}\right\|_2 + \left\|\Delta_{k_j}\right\|_2^2) = \sum_{j=1}^{p}\left|\lambda_{k_j}\right|(2\left\|\Delta_{k_j}\right\|_2 + \left\|\Delta_{k_j}\right\|_2^2). \blacksquare$$

Пусть E - возмущение матрицы A только за счет возмущения СВ, а $u_i, \overline{u_i}$ - нормированные исходный и возмущенный СВ, отвечающие λ_i, а θ_i - острый угол между ними. Назовем абсолютной отделенностью СЗ λ_i число: $gap_{abs}(i,A) = \min\limits_{i\ne j}\left\|\lambda_j\right| - \left|\lambda_i\right\|$. Тогда, используя [12], несложно показать, что:

$$\sin\theta_i \le \frac{2\|E\|_2}{gap_{abs}(i,A)}, \tag{6}$$

Теорема 3. Пусть стегопреобразование возмутило СВ вектора матрицы ОС. Достаточным условием для обеспечения малости нормы матрицы возмущения является соответствие возмущенных СВ собственным значениям матрицы ОС с малой абсолютной отделенностью.

Доказательство. Поскольку неравенство (6) имеет место для каждого СЗ матрицы A, то из него получаем:

$$\max_{1\le i\le n}\left(\frac{1}{2}\sin\theta_i\ gap_{abs}(i,A)\right) \le \|E\|_2. \tag{7}$$

Формула (7) означает, что если при возмущении исходной матрицы A ее СЗ не меняются, то даже сравнительно большие возмущения СВ, отвечающих плохо отделенным СЗ ($gap_{abs}(i,A)$ мала), приведут к малому значению $\|E\|_2$. $\blacksquare$

Вывод. *С целью обеспечения бóльшей вероятности надежности восприятия стегосообщения погружение ДИ в контейнер целесообразно производить таким образом, чтобы (при эквивалентном представлении этого погружения в виде возмущений спектра*

и СВ матрицы ОС) возмущенные СВ соответствовали малым по модулю СЗ или собственным значениям, имеющим малые абсолютные отделенности, а возмущения СЗ (причем не важно, каких именно) были малы. Чем меньше возмущения СЗ, абсолютные отделенности и модули СЗ, соответствующих возмущенным СВ, тем больше вероятность надежности восприятия стегосообщения.

4. Разностный показатель визуального искажения, основанный на СМН.

Поскольку все теоретические выводы п.3 связаны со СР, хотелось бы и оценку визуального искажения проводить, используя СМН, непосредственно получаемую из СР, а не норму Фробениуса, как в SNR, $PSNR$, IF, что требует дополнительных вычислений. В работе предлагается разностный показатель визуального искажения, в основе которого лежит СМН.

Приведем несколько вспомогательных рассуждений.

Разобьем матрицу ОС стандартным образом на блоки малой размерности [13], например, $n = 8$. Пусть F_{bl}, ΔF_{bl} - матрицы произвольного полученного при разбиении блока и его возмущения соответственно. Поскольку n мало, из леммы 1 получаем, что

$$\|\Delta F_{bl}\|_2 \approx \|\Delta F_{bl}\|_F . \qquad (8)$$

Непосредственно из соотношения (8) вытекает истинность следующего утверждения:

Утверждение 2. Пусть оценка визуального искажения после предварительного стандартного разбиения ОС на блоки производится для каждого блока в отдельности. Если в качестве такой оценки использовалась $\|\Delta F_{bl}\|_2$, то она будет сравнима с оценкой, полученной с использованием L^2-нормы (L^2-*norm*) [Конах]. Кроме того, оценки, полученные при помощи SNR, $PSNR$, IF с использованием СМН и нормы Фробениуса, будут сравнимы (переход к другой матричной норме можно трактовать, как переход к другой шкале измерений в известных разностных показателях [Сато]).

По аналогии с показателем IF, построим новый показатель: $SS = 1 - \dfrac{\|\Delta F\|_2}{\|F\|_2}$, который назовем *спектральным качеством изображения* (SS).

Утверждение 3. При малых возмущающих воздействиях показатель SS является более чувствительным к этим возмущениям, чем IF, т.е. малые возмущения приведут к бóльшим отклонениям значения SS от единицы, а значит будут количественно заметнее, чем IF.

Доказательство. Если шум отсутствует, то $IF = SS = 1$. Будем считать, что возмущающее воздействие настолько мало, что имеет место соотношение:

$$\|\Delta F\|_F < \frac{\|F\|_F}{\sqrt{n}} , \qquad (9)$$

где n - размерность матрицы или блока контейнера. Рассмотрим $\|\Delta F\|_2 \|F\|_F^2$. Для оценки этого произведения воспользуемся неравенством (3), тогда с учетом (9) получим:

$$\|\Delta F\|_2 \|F\|_F^2 \geq \frac{\|\Delta F\|_F}{\sqrt{n}} \|F\|_F^2 > \|\Delta F\|_F^2 \|F\|_F \geq \|\Delta F\|_F^2 \|F\|_2 . \qquad (10)$$

Из неравенства (10) непосредственно вытекает:

$$\frac{\|\Delta F\|_2}{\|F\|_2} > \frac{\|\Delta F\|_F^2}{\|F\|_F^2},$$

что эквивалентно тому, что показатель $SS < IF \le 1$ при малых возмущающих воздействиях, а значит, более чувствительный к ним. ■

Рис.2 является практическим подтверждением утверждения 3. На исходное изображение (рис.2(а)) накладывался аддитивный гауссовский шум (математическое ожидание равно 0, а дисперсия 0.00001). Зашумленное изображение (рис.2(б)) разбивалось на блоки. Показатели IF и SS рассчитывались для каждого блока (на рисунке они представлены в виде матриц с элементами, отвечающими блокам).

а

б

IF =

1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
0.9999	1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000
0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9999
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

в

SS =

0.9959	0.9959	0.9965	0.9961	0.9960	0.9967	0.9966	0.9967	0.9960	0.9966	0.9969	0.9966	0.9963
0.9964	0.9964	0.9959	0.9958	0.9951	0.9961	0.9962	0.9968	0.9954	0.9958	0.9969	0.9969	0.9965
0.9964	0.9964	0.9958	0.9965	0.9964	0.9961	0.9962	0.9966	0.9964	0.9953	0.9969	0.9960	0.9959
0.9962	0.9962	0.9962	0.9954	0.9965	0.9962	0.9961	0.9960	0.9969	0.9973	0.9965	0.9962	0.9971
0.9957	0.9955	0.9968	0.9965	0.9969	0.9959	0.9963	0.9965	0.9966	0.9973	0.9966	0.9967	0.9966
0.9959	0.9963	0.9963	0.9961	0.9961	0.9964	0.9964	0.9964	0.9962	0.9969	0.9966	0.9963	0.9962
0.9959	0.9966	0.9960	0.9963	0.9965	0.9963	0.9959	0.9964	0.9962	0.9956	0.9969	0.9965	0.9962
0.9963	0.9967	0.9968	0.9965	0.9960	0.9965	0.9954	0.9962	0.9961	0.9954	0.9966	0.9966	0.9968
0.9960	0.9966	0.9966	0.9962	0.9968	0.9961	0.9964	0.9963	0.9964	0.9968	0.9971	0.9966	0.9966
0.9964	0.9963	0.9964	0.9964	0.9956	0.9966	0.9954	0.9968	0.9962	0.9966	0.9973	0.9968	0.9967
0.9967	0.9958	0.9964	0.9966	0.9962	0.9963	0.9961	0.9970	0.9972	0.9967	0.9969	0.9967	0.9957
0.9957	0.9960	0.9966	0.9966	0.9965	0.9967	0.9968	0.9971	0.9974	0.9969	0.9976	0.9961	0.9953
0.9961	0.9966	0.9954	0.9964	0.9963	0.9961	0.9970	0.9966	0.9970	0.9956	0.9967	0.9964	0.9957

г

а - исходное изображение, б - зашумленное изображение, в - матрица блоковых значений показателя IF; г - матрица блоковых значений показателя SS

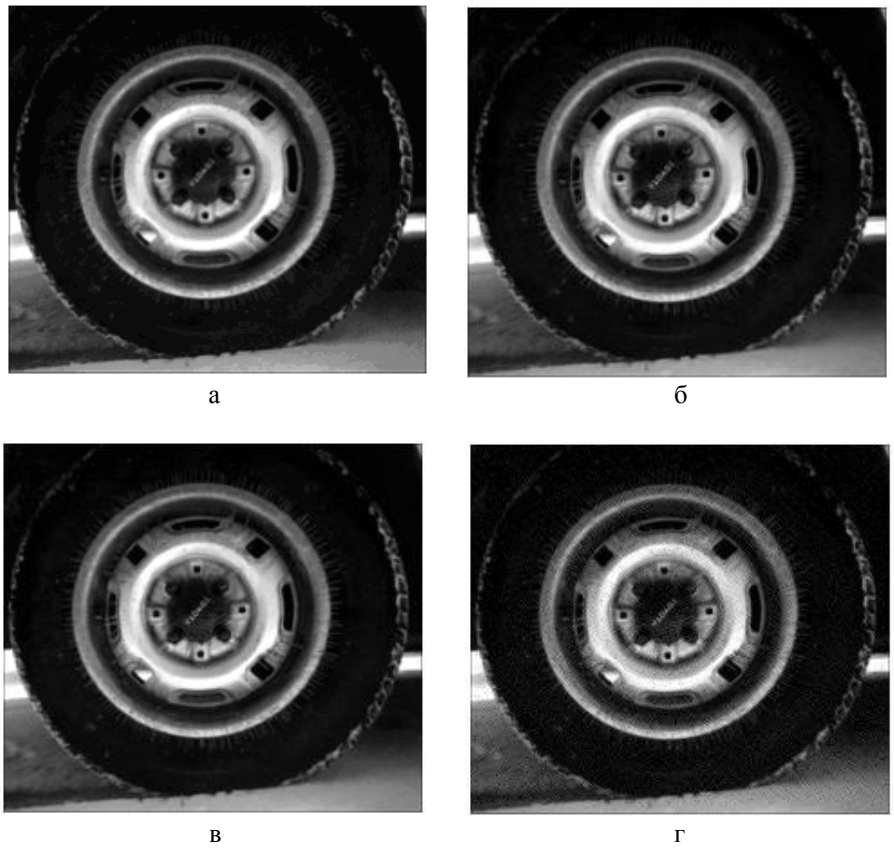
Рис.2. Сравнение использования двух разностных показателей IF и SS визуального искажения изображения.

Показатель IF, в силу погрешностей округлений, вообще не сигнализирует о наличии шума (рис.2(в)), чего нельзя сказать о показателе SS (рис.2(г)).

5. Результаты вычислительного эксперимента.

Основной целью вычислительного эксперимента было практическое подтверждение теоретических заключений, полученных в п.3. Эксперимент проводился в среде MATLAB с использованием более 100 монохромных изображений.

5.1. Изображение, используемое как ОС, разбивалось предварительно на блоки ($n = 8$). Каждому блоку по правилу (1) ставились в соответствие два симметричных блока, для которых строились НСР. Различные СЗ полученных спектров подвергались одинаковым возмущениям (величина возмущений менялась от опыта к опыту). Малые возмущения СЗ, независимо от того, какое именно СЗ возмущается, не дают визуальных искажений (рис.3). По мере роста возмущения эти искажения начинают проявляться. Так для приведенного на рис.3 изображения это происходит уже при аддитивном искажении СЗ, равном 30 (назовем такое значение пороговым). Для наглядной информативности



а б в г

а - исходное изображение; б - наименьшее по модулю СЗ в каждом блоке увеличено на 10; в - наибольшее СЗ в каждом блоке увеличено на 10; г - наименьшее по модулю СЗ в каждом блоке увеличено на 100

Рис.3. – Изображение TIRE и его преобразования.

приведен вариант, когда возмущение равно 100 (рис.3(г)). Для различных изображений пороговое значение возмущения СЗ различны и устанавливается экспериментально, однако важно то, что при малых возмущениях, как было теоретически установлено в п.3, надежность восприятия стегосообщения сохраняется.

Заметим, что как показывает проведенный вычислительный эксперимент и как вытекает из п.3, при наложении шума на изображение наибольшую относительную погрешность имеют наименьшие по модулю СЗ, относительная погрешность монотонно уменьшается с увеличением модуля СЗ (рис.4). Рисунок 4 соответствует наложению на испытуемые изображения аддитивного гауссова шума с нулевым математическим ожиданием и различными значениями дисперсии; для наглядности по оси Ox откладывался номер испытания (при его увеличении дисперсия уменьшается), по оси Oy - номер СЗ при НСР (1 - максимальное, ...,300 – минимальное по модулю СЗ), яркость

соответствующей клеточки на графике определялась как значение выражения: $\frac{|Исходное\ СЗ_i - Зашумленное\ СЗ_i|}{|Исходное\ СЗ_i|}$*100%, усредненное для всех рассматриваемых изображений. Из полученных результатов следует *вывод*: при использовании стеганографическим методом для погружения непосредственных возмущений СЗ, как это предлагается, например, в [11], для обеспечения достаточной эффективности декодирования нецелесообразно использовать минимальные по модулю СЗ, т.к. они более всего «пострадают» даже при малых возмущающих воздействиях на стегосообщение.

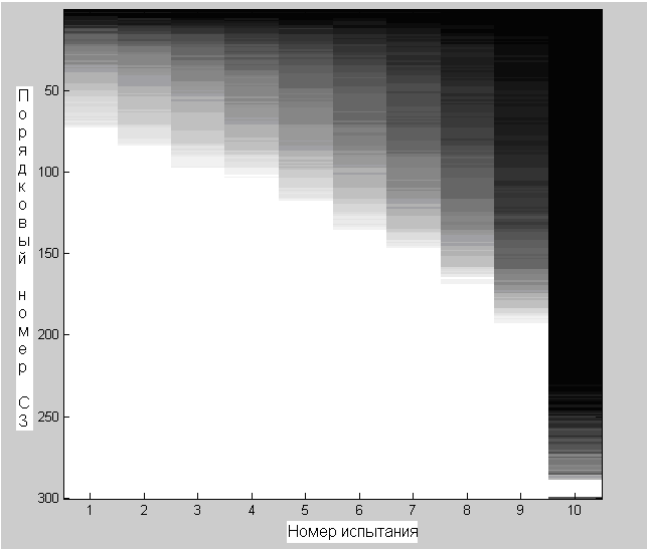


Рисунок 4. Относительная погрешность СЗ в зависимости от величины модуля СЗ и характеристики накладываемого шума

5.2. Второй этап вычислительного эксперимента заключался в следующем. После разбиения исходного изображения на блоки и вычисления НСР для симметричных матриц, отвечающих каждому блоку в соответствии с формулой (1), возмущения проводились для каждого блока в пределах матриц СВ (подробно в [12]). При проведении предварительного вычислительного эксперимента было установлено, что, как правило, малые по модулю СЗ имеют и малые абсолютные отделенности, поэтому, учитывая результаты п.3, возмущению подвергались $u_8, u_7, ..., u_4$ и, возможно, u_3, полученные из НСР, причем, принимая во внимание теорему 3, эти возмущения проводились одновременно. Иллюстрация представлена на рис.5 для изображения POUT. Результаты полностью подтверждают теоретические заключения п.3. При возмущении $u_4, ..., u_8$ надежность восприятия сохраняется, чего нельзя сказать для $u_3, ..., u_8$.

а б в

а - исходное изображение POUT; б – стегосообщение, соответствующее возмущению СВ $u_3, ..., u_8$; в – стегосообщение, соответствующее возмущению СВ $u_4, ..., u_8$

Рисунок 5 - Изображение POUT и его преобразование

Изображение на рис.5(б) содержит артефакты. Как показывают проведенные практические исследования, для подавляющего большинства блоков ОС соответствующие симметричные матрицы имеют спектры, в которых $|\lambda_1| >> |\lambda_2|, |\lambda_3|, \ldots, |\lambda_8|$, и $|\lambda_3|$ сравним по величине со значениями модулей СЗ, которые имеют бóльшие номера, а, значит, абсолютная отделенность λ_3 невелика и сравнима с отделенностями нескольких последующих СЗ. В блоках, привносящих артефакты в стегоизображение, $|\lambda_3| >> |\lambda_4|, \ldots, |\lambda_8|$, что приводит к большой абсолютной отделенности λ_3 по сравнению с λ_4, λ_5 и т.д., что является причиной недопустимых визуальных изменений стегосообщения, что соответствует п.3.

5.3. В ходе вычислительного эксперимента для подтверждения соответствия теории и практики в предложенном в работе подходе были рассмотрены несколько известных методов встраивания ДИ, в частности, метод наименьшего значащего бита (LSB) [2]. При исследовании возмущений спектра и СВ матрицы контейнера при погружении было установлено, что возмущению при стегопреобразовании подвергаются СВ, отвечающие СЗ с наименьшими абсолютными отделенностями, а возмущения СЗ очень незначительны. Исходя из теоретических положений п.3, такой алгоритм должен обеспечивать визуальную устойчивость, что подтверждается и на практике в ходе широкого применения LSB.

6. Заключение

В работе предлагается новый подход к проблеме обеспечения надежности восприятия стегосообщения, основанный на анализе возмущений спектра и СВ матрицы ОС при стегопреобразовании. Достоинством такого подхода является то, что он открывает возможности обеспечения высокой вероятности надежности восприятия стегосообщения для любого вновь создаваемого СМ. Для этого достаточно потребовать, чтобы алгоритм погружения СМ быть таким, чтобы при эквивалентном представлении стегопреобразования в виде возмущений спектра и СВ матрицы ОС, эти возмущения каснулись лишь СВ, отвечающих СЗ, малым по модулю, с малыми абсолютными отделенностями, и возмущения СЗ были малы. Кроме того, для уже существующих СМ такой анализ легко объясняет причину нарушения или устойчивое обеспечение надежности восприятия стегосообщения.

Вычислительная сложность практической реализации предложенного подхода сравнима с количеством арифметических операций для построения СР матрицы размерности $n \times n$ и составляет $\underline{O}(n^3)$, а при предварительном разбиении ОС на блоки - $\underline{O}(n^2)$ операций.

Литература.

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК – Пресс, 2006.- 288 с.
3. S.Winkler. A perceptual distortion metric for digital color images. In: Proc.ICIP, vol.3,pp.399-403,Chicago,IL,October 1998.
4. S.J.P. Westen, R.L.Lagendijk, J.Biemond. Perceptual Image Quality Based on a Multiple Channel HVS Model. In: Proceeding of ICASP, vol.4, pp.2351-2354,1995.
5. Yung-Kai Lai, C.-C. Jay Kuo, Jin Li. New image compression artifact measure using wavelets.-
6. Ф.Р.Гантмахер. Теория матриц.- М.: Наука, 1988.
7. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. - 430 с.
8. Каханер Д., Моулер К., Нэш С. Численные методы и программное обеспечение. – М.: Мир, 2001. – 575 с.
9. Парлетт Б. Симметричная проблема собственных значений. Численные методы.- М.: Мир, 1983. -384 с.

10. Маслов В.П. Асимптотические методы и теория возмущений.- М.: Наука. Гл. ред. физ.-мат. лит., 1988.-312 с.
11. Кобозева А.А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы. – Праці УНДІРТ, 2006, №4(48), - с.44-52.
12. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах. Вісник Східноукраїнського національного університету ім. В.Даля, 2006, №9(103),ч.1,-с.74-83.
13. Гонсалес Р., Вудс Р. Цифровая обработка изображений.- М.: Техносфера, 2005.- 1072 с.

Вестник НТУ «ХПИ», 2007, №18, с.81-93.

.