1.7. EFFICIENCY IMPROVING METHODS OF TRANSMISSION OF CONFIDENTIAL INFORMATION BY PUBLIC CHANNELS

В настоящее время количество областей, в которых средства электронной связи заменяют бумажную переписку, быстро увеличивается. В результате увеличивается и доступный для перехвата объем информации (носящий конфиденциальный характер), а сам перехват становится более легким. В связи с бурным развитием технологий мультимедиа остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде.

Одно из перспективных направлений защиты информации сформировали современные методы стеганографии, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде и представляют собой самостоятельное научное направление информационной безопасности. В цифровой носитель – контейнер при помощи некоторого стеганографического метода (СМ) встраивается дополнительная информация (ДИ), в качестве которой может выступать, например, цифровой водяной знак, персональные данные, коммерческая или государственная тайна. Контейнер с встроенной в него информацией принято называть стеганографическим контейнером (СК), который хранится или передается каналами связи между его пользователями. Стеганографические методы находят все большее применение в оборонной и коммерческой сферах деятельности, в медицине в силу их легкой адаптируемости при решении задач защиты информации, а также отсутствия явно выраженных признаков средств защиты, использование которых может быть ограничено или запрещено.

До недавнего времени стеганография, как наука, в основном изучала отдельные методы сокрытия информации и способы их технической реализации. Разнообразие принципов, заложенных в СМ, отсутствие единого математического аппарата, который обеспечил бы создание методов для проведения априорного анализа свойств стегосистем (СС), сравнение различных алгоритмов их генерации и обработки, тормозило развитие стеганографии, замедляло процесс формирования ее в виде самостоятельной науки со своими теоретическими положениями и единой концептуальной системой. В частности до настоящего момента не были формализованы и унифицированы в целом требования к СМ и стеганографическим алгоритмам (СА), обеспечивающие их устойчивость к возмущающим воздействиям. Это часто не позволяло гарантировать эффективную работу существующих и вновь разрабатываемых СА, в условиях активных атакующих действий, что оставляет *актуальной* задачу разработки общего теоретического базиса, включающего способы получения формальных качественных и количественных оценок устойчивости СМ, и его практического воплощения при генерации СА.

Целью работы является повышение эффективности процесса передачи секретной информации по каналам общего пользования путем разработки общих теоретических принципов и их использования для создания стеганографических методов и алгоритмов, устойчивых к возмущающим воздействиям.

Одной из задач, для достижения поставленной цели, является формализация требований и получение достаточных условий обеспечения устойчивости произвольных стеганографических методов к возмущающим воздействиям на основе общего математического подхода к анализу и оценке состояния и технологии функционирования систем защиты информации (ОПАИС), основанного на теории возмущений[49].

В качестве математической модели цифрового сигнала – контейнера рассматривается двумерная матрица F. Согласно ОПАИС преобразование контейнера за счет встраивания в него ДИ, независимо от способа и области встраивания, рассматривается как возмущение ΔF матрицы F: $\overline{F} = F + \Delta F$, где $\Delta F = f(F)$, то есть ΔF является некоторой функцией

[49] Кобозева А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованій на теорії збурень / А.А. Кобозева// Информационные технологии и компьютерная инженерия. – 2008. – №1. – с. 164-171.

матрицы F, $\overline{F}$ – матрица СК. Стеганографическое преобразование (СП) контейнера, а также любые преобразования СК при его транспортировке или хранении, включая активные атакующие действия, представимы в виде элементарных матричных операций. Поэтому в качестве формальных параметров, однозначно определяющих и всесторонне характеризующих контейнер (СК), можно использовать любой из наборов, который однозначно определяет произвольную двумерную матрицу: а) совокупность сингулярных чисел (СНЧ) и ортонормированных лексикографически положительных сингулярных векторов (СНВ), которые могут быть получены при помощи нормального сингулярного разложения (СНР) $F = U\Sigma V^T$, где U, V – матрицы размерности $m \times n$ и $n \times n$ соответственно; $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$. При этом U, V удовлетворяют соотношениям: $U^T U = I,\ V^T V = I$, где I – единичная матрица соответствующей размерности, т.е. являются ортогональными. Столбцы $u_1,...,u_n$ матрицы U и $v_1,...,v_n$ матрицы V называют соответственно левыми и правыми СНВ матрицы F, величины $\sigma_1,...,\sigma_n$ – СНЧ; б) спектр (совокупность собственных значений (СЗ)) и множество ортонормированных лексикографически положительных собственных векторов (СВ), которые однозначно определяются нормальным спектральным разложением (СР) матрицы $F = U\Lambda U^T$ в случае ее симметричности, где $\Lambda = diag(\lambda_1,...,\lambda_n)$ – матрица СЗ.

Из вышеизложенного следует, что любое преобразование, в частности, СП матрицы контейнера определенным образом возмутит ее СНЧ (СЗ) и СНВ (СВ). В силу этого любое СП представимо в виде совокупности возмущений СНЧ (СЗ) и (или) СНВ (СВ) матрицы контейнера, определяемых нормальным СНР (СР). Для СНЧ $\sigma_j(F),\ \sigma_j(F+\Delta F),\ j = \overline{1,n}$, матриц F и $F + \Delta F$ соответственно имеет место соотношение:

$$\max_{1 \leq j \leq N} \left| \sigma_j(F) - \sigma_j(F + \Delta F) \right| \leq \left\| \Delta F \right\|_2, \quad (1)$$

где $\left\| \bullet \right\|_2$ – спектральная матричная норма (СМН). В силу соотношения (1) возмущения СНЧ сравнимы с возмущением данных – $\left\| \Delta F \right\|_2$, поэтому для оценки чувствительности задачи СП с матрицей F имеет смысл анализировать лишь возмущения СНВ F, происшедшие в ходе преобразования.

Для СЗ симметричной матрицы имеет место оценка, аналогичная (1):

$$\max_{1 \leq j \leq n} \left| \lambda_j(F) - \lambda_j(F + \Delta F) \right| \leq \left\| \Delta F \right\|_2. \quad (2)$$

Таким образом, для оценки чувствительности задачи СП с симметричной матрицей СК имеет смысл анализировать лишь возмущения СВ.

СК будет *чувствительным*, если даже незначительные возмущающие воздействия, которым он подвергается, способны разрушить значительную часть погруженной ДИ и привести к большому росту количества ошибок при ее декодировании. В противном случае СК называется *нечувствительным*.

Пусть A – симметричная матрица контейнера, модули СЗ которой попарно различны. Возмущенная матрица $\overline{A}$ и матрица произвольного возмущающего воздействия E рассматриваются как симметричные. Тогда СР $\overline{A}$ только за счет возмущения U представимо в виде $\overline{A} = A + E = \overline{U}\Lambda\overline{U}^T$. Пусть $u_i, \overline{u}_i$ – нормированные соответственно исходный и возмущенный СВ, соответствующие λ_i, а θ_i - острый угол между ними. Назовем абсолютной отделенностью *СЗ* λ_i число:

$$gap_{abs}(i, A) = \min_{i \neq j} \left\| \left| \lambda_j \right| - \left| \lambda_i \right| \right|. \quad (3)$$

Поскольку доказано, что

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|E\|_2}{gap(i,A)}, \quad \frac{1}{2}\sin 2\theta_i \le \frac{\|E\|_2}{gap(i,A+E)} \tag{4}$$

имеет место вывод: мерой чувствительности СВ является абсолютная отделенность СЗ, которому соответствует данный вектор.

Достаточным условием обеспечения малой чувствительности СК к возмущающим воздействиям является соответствие возмущенных при СП контейнера собственных векторов его матрицы A собственным значениям матрицы СК $\overline{A}$, имеющим большие, по сравнению с другими СЗ, абсолютные отделенности. Если возмущенные в результате СП контейнера СВ соответствуют СЗ матрицы СК с малыми абсолютными отделенностями, то полученный СК оказывается *чувствительным* к возмущающим воздействиям, что, как правило, приводит к недостаточной эффективности декодирования ДИ.

Как следует из (2), учитывая, что все возмущения, воздействующие на контейнер и СК, являются малыми (для обеспечения надежности их восприятия (должны быть незаметны)), абсолютные отделенности СЗ матриц $\overline{A}$ и A незначительно отличаются друг от друга. В силу этого достаточным условием обеспечения малой чувствительности СК к возмущениям является соответствие возмущенных при СП СВ собственным значениям матрицы контейнера, имеющим большие абсолютные отделенности.

СМ является *неустойчивым к возмущениям* (далее – неустойчивым), если малые возмущающие воздействия могут привести к значительному или полному уничтожению встроенной в контейнер при помощи этого СМ секретной информации, и *устойчивым* к возмущениям (далее – устойчивым) в противном случае.

Таким образом, СМ будет неустойчивым, если генерируемый им СК будет чувствительным к возмущениям (в соответствии с определением 1).

Аналогично (3) *отделенностью* СНЧ σ_i матрицы F назовем величину $svdgap(i,F) = \min\limits_{i \ne j} \left|\sigma_j - \sigma_i\right|$. Если $F + \Delta F$ – возмущенная матрица, θ_i – угол между соответствующими исходным и возмущенным СНВ u_i и $\overline{u}_i$, тогда имеют место соотношения:

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F)}, \qquad \frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F+\Delta F)}. \tag{5}$$

Поскольку любое СП, согласно (1), можно представить в виде аддитивного погружения некоторой информации в пространственной области, то из соотношения (5) вытекает следующее утверждение:

Достаточным условием обеспечения малой чувствительности к возмущениям СК с матрицей произвольной структуры, а значит устойчивости используемого СМ, независимо от области погружения ДИ (пространственной или области какого-либо преобразования), является соответствие возмущенных СНВ сингулярным числам с большой отделенностью. *Отделенность СНЧ, отвечающих возмущенным в процессе СП СНВ матрицы контейнера, является мерой чувствительности полученного СК к возмущающим воздействиям.*

Результатом СП является возмущение матрицы СНВ U, которая получена при нормальном СНР матрицы контейнера F. Если возмущение U отвечает СНВ, соответствующим СНЧ с малой отделенностью, то получаемый СК окажется чувствительным к возмущающим воздействиям, независимо от стегометода и используемой области погружения.

Требование устойчивости метода обеспечивается при возмущениях СНВ, отвечающих СНЧ с наибольшими отделенностями. Преодоление возникшего противоречия достигается, когда СП возмущает СНВ, отвечающие СНЧ со средними по значению отделенностями среди совокупности СНЧ.

Одной из основных характеристик сигнала, представлением которого является матрица F размерности $m \times n$, является его энергия E[50]: $E = \sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij}^2 = \sum_{u=0}^{m-1}\sum_{v=0}^{n-1} P(u,v)$, где $P(u,v), u = \overline{0, m-1}, v = \overline{0, n-1}$, – энергетический спектр сигнала F. Энергия двумерного цифрового сигнала F также может быть определена как сумма квадратов СНЧ (СЗ в случае $F = F^T$) его матрицы[51]: $E = \sigma_1^2 + ... + \sigma_n^2$. Одновременная модификация всех СНЧ (СЗ при $F = F^T$) F в общем случае отразится на всех составляющих частотного спектра сигнала. Учитывая это, можно утверждать, что погружение ДИ в вектор СНЧ (или СЗ) матрицы контейнера приведет к расширению частотного спектра ДИ до частотного спектра сигнала-контейнера.

Аппроксимацией ранга k изображения F является

$$F_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T \qquad (6)$$

$F_{k_d} = \sum_{i=k+1}^{n} \sigma_i u_i v_i^T$ – дополнение к аппроксимации F_k, $S_k = \sigma_k u_k v_k^T$ – k-й составляющей изображения F

Существует определенное соответствие между элементами энергетического спектра и сингулярными тройками матрицы исходного сигнала.

Сингулярные тройки (σ_i, u_i, v_i), отвечающие наибольшим СНЧ, соответствуют главным образом низкочастотным, а наименьшим – главным образом высокочастотным составляющим сигнала.

Из теории обработки цифровых изображений известно, что в зависимости от величины частоты среза идеального низкочастотного фильтра (ИФНЧ) или идеального высокочастотного фильтра (ИФВЧ) пропускается определенное количество энергии двумерного сигнала. Один из способов ввести эталонный набор положений обрезающих частот состоит в том, чтобы определить круги, в которых (для ИФНЧ) или вне которых (для ИФВЧ) заключена заданная часть полной энергии изображения. Частота $r(\mu)$ определяется как радиус круга с центром в центре частотного прямоугольника дискретного преобразования Фурье (ДПФ), в котором (для ИФНЧ) или вне которого (для ИФВЧ) заключено μ процентов энергии спектра. С другой стороны, используя результаты, полученные выше и формулу (6), выбирая ранг k, также можно получить заданный процент энергии спектра матрицы изображения. На рис.1 приведены тестовые примеры, которые демонстрируют связь частотных составляющих спектра ДПФ и СНЧ спектра матрицы изображения. Аппроксимация изображения ранга 3 (сингулярные тройки, отвечающие первым трем наибольшим СНЧ) обеспечивает практически тот же процент энергии, что и ИФНЧ с частотой среза, равной $r = 5$ – рис.1(б, в). Спектр убывает весьма быстро, 93% полной энергии заключено в относительно малом круге радиуса 5 и примерно столько же энергии заключают в себе сингулярные тройки малоранговой аппроксимации порядка 3. Сильное размывание на обоих рисунках указывает, что основная информация о резких деталях и контурах содержится в 7% отсеченных фильтром и в 6,2% СНЧ не включенных в аппроксимацию. С увеличением радиуса фильтра (рис.1(г)) и ранга аппроксимации (рис.1(д)) все меньшая и меньшая часть энергии подлежит отсечению – уменьшается степень размывания изображения. Рис.1(е) и рис.1(ж) демонстрируют соответствие между высокочастотным спектром ДПФ и сингулярными тройками, отвечающим малым СНЧ.

[50] Гонсалес Р. Цифровая обработка изображений / Р.Гонсалес, Р.Вудс; пер. с англ. под ред. П.А.Чочиа. – М.: Техносфера, 2005. – 1072 с.

[51] Кобозева А.А. Стеганографические SS-методы, использующие сингулярное и спектральное разложения матрицы контейнера/ А.А. Кобозева, И.И.Борисенко//Зв'язок. – 2007. – №7(75). – С. 34 – 38.

Учитывая то что любое СП контейнера эквивалентным образом представимо в виде возмущений СНЧ и (или) СНВ его матрицы и связь между энергетическим спектром сигнала и сингулярными тройками его матрицы, а также тот факт, что при погружении ДИ в частотной области контейнера для обеспечения устойчивости СМ к возмущениям и надежности восприятия СК приоритетной является модификация средней части частотного спектра, можно сделать вывод, что аналогичными с точки зрения устойчивости окажутся СМ, для которых СП вызовет возмущение сингулярных троек, отвечающих средним по значению сингулярным числам матрицы контейнера (соответствующих средней части частотного спектра контейнера), независимо от непосредственно используемой этими методами области погружения.

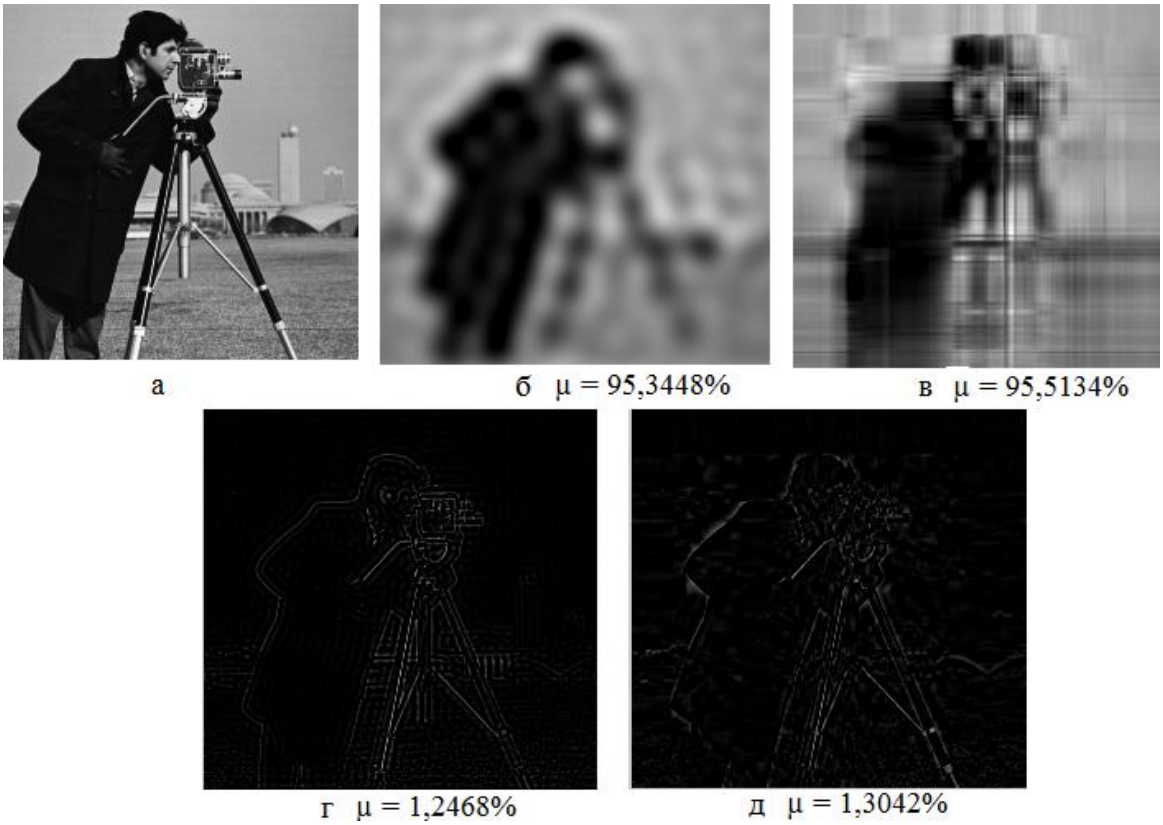


Рис. 1. Энергия изображения как функция расстояния от центра ДПФ и ранга аппроксимации изображения Cameraman.tif: исходное изображение (а), отфильтрованное изображение ИФНЧ $r = 5$ (б) и $r = 10$ (г), отфильтрованное изображение ИФВЧ $r = 45$ (е), аппроксимация ранга $k=3$ (в), $k=5$ (д) и $k \geq 20$ (ж).

Приоритетность с точки зрения устойчивости на практике методов, использующих частотную область для погружения ДИ, можно объяснить лишь несовершенством известных из открытой печати методов, работающих в пространственной области, где обеспечение выполнения достаточного условия устойчивости СМ не является тривиальным, в то время, как обеспечить его выполнение в частотной области гораздо проще, учитывая соответствие между энергетическим спектром и сингулярными тройками матрицы сигнала.

Таким образом, устойчивость СМ, как и другие его свойства, зависит не от области погружения ДИ, а от локализации возмущений, являющихся результатом СП, для множества сингулярных троек.

В усовершенствованном методе SLAU[52] используется двухэтапное декодирования ДИ, что обеспечивает повышение устойчивости СМ. Метод основан на решении систем

[52] Борисенко И.И. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений / И.И. Борисенко, А.А. Кобозева // Праці УНДІРТ. – 2006. – №3(47). – С. 78-83.

линейных алгебраических уравнений и применим для произвольного контейнера. Повышение устойчивости СМ SLAU обеспечивается за счет уменьшения числа обусловленности задачи декодирования ДИ по сравнению с индивидуальной работой СМ, т.е. уменьшения чувствительности СК к возмущающим воздействиям.

Обозначим через F матрицу контейнера размерности $n \times n$, $\det F \neq 0$, а в качестве ДИ выступает бинарная числовая последовательность, содержащая n элементов из множества $\{-1, 1\}$, которую будем рассматривать ниже как вектор x длины n. Для получения СК вычисляется произведение

$$b = F\,x \tag{7}$$

В предположении отсутствия ошибок машинной арифметики, вектор x является точным решением СЛАУ $F\,x = b$. Вектор b погружается в F выбранным стеганографическим алгоритмом. Декодирование ДИ включает два этапа. Сначала из полученного СК извлекается погруженный вектор b – в общем случае получаем вектор b_B, поскольку СК мог подвергнуться возмущениям при пересылке, а выделение информационного вектора x будет происходить на втором этапе при решении неоднородной СЛАУ. После извлечения вектора b_B матрица изображения F_B, в общем случае, будет отлична от F: $F_B\,x_{пр} = b_B$, где $F_B = F + \delta F, b_B = b + \delta b$; $\delta F, \delta b$ – возмущения матрицы системы F и вектора правой части b соответственно; $x_{пр}$ – результат декодирования x в условиях возмущенных входных данных.

Достаточное условие устойчивости предложенного метода обосновывается использованием числа обусловленности Скила $k\left(F\right) = \left\| \left|F^{-1}\right| \left|F\right| \right\|$, где $\left|F\right|$ ($\left|F^{-1}\right|$) – матрица абсолютных значений элементов F (F^{-1}). Если матрица изображения, используемого в качестве контейнера, имеет малое число обусловленности Скила, то метод SLAU будет устойчивым.

Алгоритм реализации метода SLAU содержит шаг, обеспечивающий малость числа обусловленности Скила для любого контейнера. Значение $k(F) \approx 1$ достигается, если выполняется свойство:

$$\left| f_{ii} \right| >> \sum_{j=1,\, j \neq i}^{n} \left| f_{ij} \right|, \; i = 1,\ldots, n. \tag{8}$$

Реальные изображения редко удовлетворяют свойству (8). Чтобы обеспечить значительное диагональное преобладание элементов матрицы контейнера F ей ставится в соответствие нижняя треугольная матрица $\overline{F}$ с элементами

$$\overline{f}_{ij} = \begin{cases} 0, \textit{ если } f_{ij} \le 127, \\ 1, \textit{ если } f_{ij} > 127 \end{cases}, \quad j = \overline{1, n-1}, \; i = \overline{j+1, n}, \; \overline{f}_{11} = m, \; \overline{f}_{ii} = m \sum_{j=1}^{i-1} \overline{f}_{ij}, \; i = \overline{2, n}, \; m \in N, \tag{9}$$

где m- параметр, который призван обеспечить для матрицы $\overline{F}$ наличие свойств, близких к (8). Вычисляем вектор $\overline{b} = \overline{F}x$. Тогда x есть решение СЛАУ :

$$\overline{F}x = \overline{b}\,, \tag{10}$$

матрица которой $\overline{F}$ по построению имеет малое число обусловленности Скила.

Поскольку в дальнейшем предполагается погружать именно вектор $\overline{b}$ в матрицу F контейнера, а его значения могут оказаться достаточно большими, то для обеспечения надежности восприятия СК по $\overline{b}$ генерируется вектор b^* все элементы которого принадлежат интервалу [-α, α], а СЛАУ (10) для восстановления x принимает вид $\overline{F}x = b^*$. Выделение нужного информационного вектора x происходит при решении неоднородной

СЛАУ $\overline{F}_B x_{np} = b_B^*$, где $b_B^* = b^* + \delta b^*$ – возмущенный вектор b^*, матрица $\overline{F}_B$ получается по возмущенной матрице $F_B = F + \delta F$ контейнера.

Учитывая вид множества, которому принадлежат элементы *x*, нас не столько интересуют непосредственные значения элементов x_{np}, сколько их знак. Окончательный шаг декодирования отвечает формуле:

$$\overline{x}_i = sign\left((x_{np})_i\right), \ i = \overline{1,n}.$$

В качестве СМ использовался неустойчивый к возмущениям метод аддитивного встраивания ДИ в пространственную область, а именно в один из выбранных контуров изображения – контейнера, где в качестве ДИ фигурировала случайно сформированная бинарная последовательность. Увеличение эффективности декодирования СМ при его совместной работе с SLAU по сравнению с эффективностью декодирования при его индивидуальной работе (без SLAU) подтверждено результатами вычислительного эксперимента, который проводился для 200 цифровых изображений. Так при увеличении параметра m от 2 до 15 при различных уровнях шума, который накладывался на СК, объем правильно восстановленной информации при помощи SLAU превысил соответствующий объем без его использования на 10-35%.

На основе классической непрерывной модели связи с расширением спектра полезного сигнала, применяемой в радиотехнических системах передачи информации в работе[53] разработан СМ, главным требованием к которому является устойчивость при наличии значительных возмущающих воздействий, которым подвергается СК. Если СП при встраивании ДИ приводит к возмущению всех СНЧ (СЗ) матрицы контейнера, то такой СМ является SS-методом (Spread-Spectrum). SS-метод расширяет энергетический спектр ДИ до спектра контейнера.

В качестве ДИ, обозначаемую далее как b, используется бинарная последовательность элементы которой принадлежат множеству $\{-1,1\}$. Расширение спектра b происходит за счет моделирующего сигнала специального вида, который вызывает возмущение всех СНЗ (СЗ) матрицы контейнера. Для получения моделирующего сигнала матрица контейнера F разбивается на блоки $F_1,..,F_n$. Затем строится ее автокорреляционная матрица R – $R = \frac{1}{n}\sum_{i=1}^{n} \overline{Z}_i \overline{Z}_i^T$. Моделирующий сигнал $\overline{S}$ – это собственный вектор, отвечающий наименьшему собственному значению *R*. В качестве реализации стеганографического SS-метода разработаны три его реализации: алгоритмы SING_NUMBER, EIG_NUMBER, SPACE_SS[54], отличающиеся способом получения $\overline{Z}_i$, формирующие матрицу R. В алгоритме SING_NUMBER $\overline{Z_i}$ определяется в результате СНР матриц F_i, в EIG_NUMBER – СР матриц F_i, в SPACE_SS – вектор $\overline{Z}_i$ сформирован из элементов матрицы F_i по определенному правилу. В алгоритмах SING_NUMBER и SPACE_SS в каждый блок встраивается один бит ДИ, согласно формулам: $\overline{Y_i} = Ab_i \overline{S} + \overline{Z_i} + \overline{\overline{n_i}}$, $diag(\overline{\Sigma_i}) = \overline{Y_i}$, $\overline{F_i} = U_i \overline{\Sigma_i} V_i^T$, где A – числовой параметр, $\overline{\overline{n_i}}$ – аддитивный белый гауссовский шум – для SING_NUMBER ; $\overline{Y_i} = Ab_i \overline{S} + \overline{Z}_i$, затем из элементов вектора $\overline{Y_i}$ формируется $\overline{F_i}$ по правилу, согласующимся с тем, которое применялось на шаге формирования вектора $\overline{Z}_i$ – для

[53] Кобозева А.А. Стеганографический SS-метод, использующий модулирующий сигнал специального вида /А.А. Кобозева, И.И. Борисенко // Вісник Східноукр-го нац-го ун-ту ім. В.Даля. – 2007. – №5(111),ч.1. – С.24-32.

[54] Борисенко И.И. Стеганографический алгоритм, основанный на SS – методе и использующий пространственную область контейнера/ И.И.Борисенко// Вісник східноукраїнського національного університету ім. В.Даля. – 2011. – №7. – С. 41-45.

SPACE_SS. Пропускная способность алгоритма EIG_NUMBER в два раза больше благодаря приведению матрицы блока F_i к симметричному виду. Блоку F_i ставится в соответствие две симметричных матрицы A_i и B_i размерности $n \times n$ и $(n-1)\times(n-1)$ соответственно:

$$F_i = \begin{pmatrix} f_{11}^{(i)} & f_{12}^{(i)} \dots f_{1n}^{(i)} \\ f_{21}^{(i)} & f_{22}^{(i)} \dots f_{2n}^{(i)} \\ \dots\dots\dots\dots \\ f_{n1}^{(i)} & f_{n2}^{(i)} \dots f_{nn}^{(i)} \end{pmatrix} \rightarrow A_i = \begin{pmatrix} f_{11}^{(i)} & f_{12}^{(i)} \dots f_{1n}^{(i)} \\ f_{12}^{(i)} & f_{22}^{(i)} \dots f_{2n}^{(i)} \\ \dots\dots\dots\dots \\ f_{1n}^{(i)} & f_{2n}^{(i)} \dots f_{nn}^{(i)} \end{pmatrix}, \; B_i = \begin{pmatrix} f_{21}^{(i)} & f_{31}^{(i)} \dots f_{n1}^{(i)} \\ f_{31}^{(i)} & f_{32}^{(i)} \dots f_{n2}^{(i)} \\ \dots\dots\dots\dots \\ f_{n1}^{(i)} & f_{n2}^{(i)} \dots f_{n,n-1}^{(i)} \end{pmatrix}$$

Каждая из матриц A_i и B_i используется для переноса одного бита ДИ. Погружение b_{2i-1} и b_{2i} ДИ осуществляется в соответствии: $\overline{Y_i^A} = Ab_{2i-1}\overline{S^A} + \overline{Z_i^A} + \overline{\overline{n_i^A}}$; $\overline{Y_i^B} = Ab_{2i}\overline{S^B} + \overline{Z_i^B} + \overline{\overline{n_i^B}}$; формирование блока F_i СК: $diag\,\overline{\Lambda_i^A} = \overline{Y_i^A}$, $\overline{A_i} = U_i^A \overline{\Lambda_i^A} (U_i^A)^T$; $diag\,\overline{\Lambda_i^B} = \overline{Y_i^B}$, $\overline{B_i} = U_i^B \overline{\Lambda_i^B} (U_i^B)^T$; верхний треугольник $\overline{F_i}$ отвечает верхнему треугольнику матрицы $\overline{A_i}$, нижний треугольник $\overline{F_i}$, исключая главную диагональ, отвечает аналогично расположенному треугольнику матрицы $\overline{B_i}$.

При проведении вычислительного эксперимента различные возмущающие воздействия моделировались при помощи гауссового шума с нулевым математическим ожиданием и различным значением дисперсии.

Без наложения шума при $A = 1$ объем правильно восстановленной при декодировании информации P для SING_NUMBER и EIG_NUMBER составил 70%, а для SPACE_SS – 60%. При $A = 2$, для всех трех алгоритмов, P находился в пределах 92-99%. При $A = 3$ для SPACE_SS $-P = 100\%$, а для SING_NUMBER и EIG_NUMBER значение P не превысило 99%; дальнейшее увеличение значения A не приводит к росту P для SING_NUMBER и EIG_NUMBER. Такой результат объясняется присутствием внутреннего шума, который возникает на этапе перехода от вещественных значений элементов СК к целочисленным при возвращении из спектральной области матрицы в пространственную. Реакция алгоритмов на наличие внешнего шума представлена в таблице 1. Результаты работы SING_NUMBER и EIG_NUMBER примерно совпадают, поэтому в таблице отображены данные для одного из них – EIG_NUMBER.

Таблица 1. Зависимость P (%) от параметра A в условиях моделируемого шума

	D=0,0001		D=0,001		D=0,01	
A	Eig_number	Space_SS	Eig_number	Space_SS	Eig_number	Space_SS
1	60	50	55	50	53	50
2	77	65	73	55	66	52
3	85	89	75	68	73	54
4	91	92	78	70	75	55
7	93-94	98,5	80-83	82	77	63
10	94	100	83	90	78	67
29			83	100	78	80
50					78	100

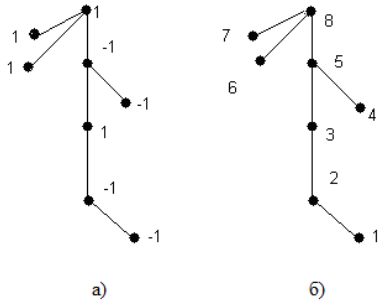
В таблице не отображены данные для D=0,1, поскольку изображение практически не информативно, но в целях эксперимента такая ситуация тоже рассматривалась и при A=300 было получено 100% правильно декодируемой информации Для остальных двух алгоритмов P составил лишь 76%. Анализируя полученные результаты следует отдать предпочтение алгоритму, использующего пространственную область для погружения ДИ (поскольку всегда удается добиться P=100%), что еще раз подтверждает выводы, о том, что

устойчивость стегоалгоритма не зависит от области, используемой для СП. К достоинствам алгоритма SPACE_SS также следует отнести то, что погружение ДИ в пространственную область требует меньше вычислительных операций, по сравнению с алгоритмами SING_NUMBER и EIG_NUMBER, которые используют сингулярное и спектральное разложение матрицы контейнера соответственно.

На основе разработанных достаточных условий для обеспечения определенных свойств СК и СМ, которые базируются на анализе возмущений СНВ (СВ) соответствующих матриц представлен алгоритм STEGO-GRAPH и его модификации, повышающие устойчивость STEGO-GRAPH к возмущениям.

До погружения ДИ в контейнер и ДИ и контейнер подвергаются предварительной обработке. Контейнер разбивается на блоки F_i размером 8x8 и представляется в виде характеристической матрицы. Для того, чтобы обеспечить надежность восприятия СК, вычисленная яркость пикселя $f'(x,y)$ должна находится в заданных пределах $f(x,y)-\delta \le f'(x,y) \le f(x,y)+\delta$, где δ – максимально допустимая величина отклонения яркости пикселя от исходного значения, поэтому контейнер подвергается *многоуровневому пороговому преобразованию* $g(x,y)=\begin{cases}0, \text{если } f(x,y)\le T,\\ 1, \text{если } f(x,y)>T\end{cases}$, где T – порог, результатом которого является сегментация изображения на подобласти[55].

В алгоритме STEGO-GRAPH[56] в качестве ДИ используется бинарная последовательность, элементы которой принадлежат множеству $\{-1,1\}$. ДИ представляется в виде графа дерева, для которого строится матрица смежности (рис.2).



а) б)

1	1	0	0	0	0	0	0
1	**2**	1	0	0	0	0	0
0	1	**3**	0	1	0	0	0
0	0	0	**4**	1	0	0	0
0	0	1	1	**5**	0	0	1
0	0	0	0	0	**6**	0	1
0	0	0	0	0	0	7	1
0	0	0	0	1	1	1	**8**

в)

Рис. 2. Математическая модель ДИ, представленная: деревом ДИ (а), помеченным деревом ДИ (б) и матрицей смежности помеченного дерева (в)

Матрица смежности является симметричной, поэтому используется одна из ее треугольных подматриц. Структура (портрет) треугольной подматрицы вдоль второй главной диагонали однозначно определяет местонахождение 1 и -1.

Погружение информации в блок контейнера происходит в результате корректировки значений элементов его матрицы F, которая выполняется только в том случае, если обнаруживается несовпадение значений элементов характеристической матрицы контейнера и матрицы смежности ДИ вдоль их второй главной диагонали. Пикселю контейнера присваивается значение $T+1$, если 0 характеристической матрицы контейнера надо преобразовать в 1, и T в противном случае, $T=\frac{f_{start}+f_{end}}{2}$, где f_{start}, f_{end} – начало и конец подобласти соответственно (рис.3).

[55] Борисенко И.И. Особенности применения многоуровневого порогового преобразования изображения в компьютерной стеганографии /И.И. Борисенко// Праці УНДІРТ. – 2006. – №4(48). – С. 53-59.

[56] Борисенко И.И. Использование теории графов в стеганографии/ И.И. Борисенко// Спеціальна техніка у правоохоронній діяльності. Матеріали IV Міжнародної науково-практичної конференції. – 2009. – С. 90-102.

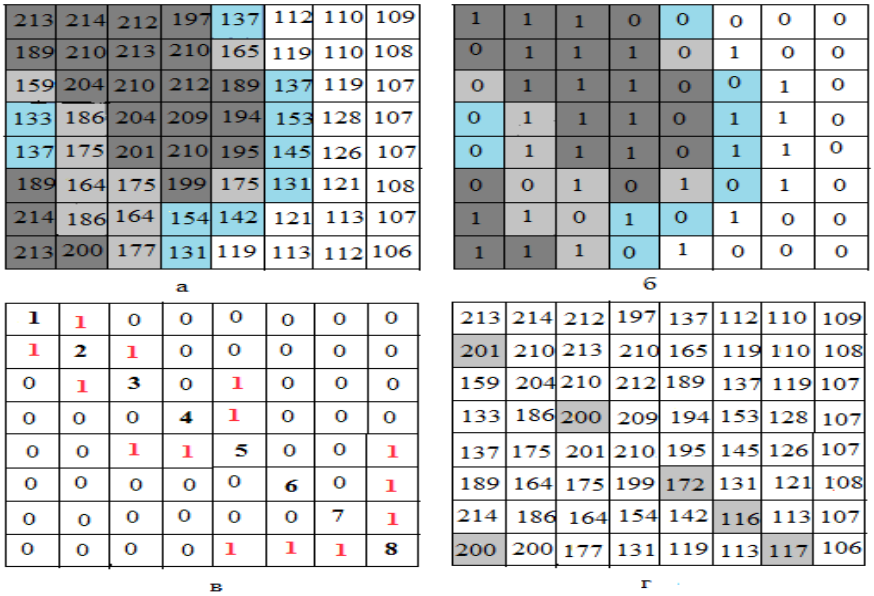


Рис. 3. Этапы погружения ДИ в контейнер: матрица F исходного изображения (а), матрица порогового преобразования F (б), матрица ДИ (в), матрица СК (г).

В ходе вычислительного эксперимента при появлении незначительных помех (помеха моделировалась гауссовым шумом с нулевым математическим ожиданием и дисперсией $D = 0{,}00001$) эффективность декодирования из 100% снижалась до 65%.

Матричный анализ Stego_Graph показал, что в силу особенности погружения ДИ (элементы матрицы контейнера либо вовсе не корректируются, либо корректируются на малую величину) матрица контейнера получает достаточно малые возмущения и в первую очередь возмущаются СНВ, отвечающие малым СНЧ – рис. 4 а) (это 6,7,8 СНВ – ДИ находится в основном в возмущениях этих векторов). Чтобы уменьшить чувствительность СК к возмущающим воздействиям, следуя достаточному условию нечувствительности СНВ, сформулированному выше, Stego_Graph был модифицирован таким образом, что в результате СП возмущения получили СНВ, которые отвечают СНЧ с большими абсолютными отделенностями[57].

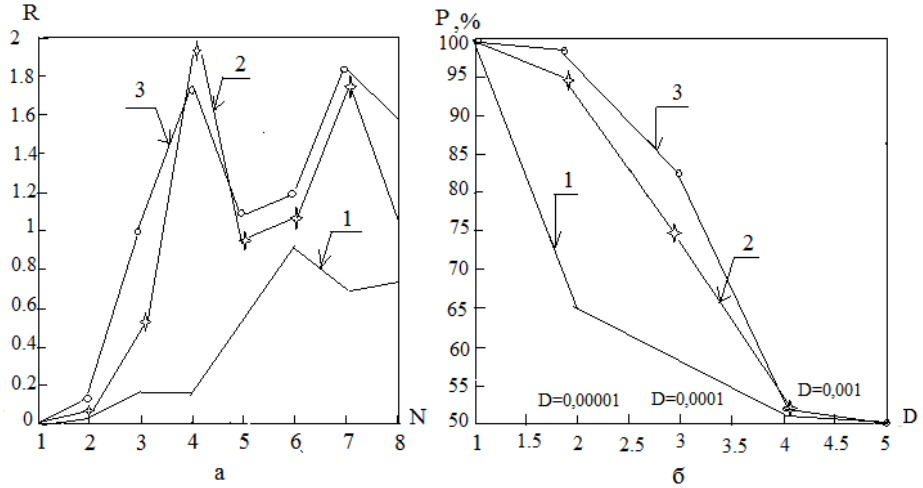


Рис. 4. Представление погруженной и восстановленной информации алгоритмами StegoGraph(1), StegoGraph1(2), StegoGraph2(3): представление погруженной информации возмущенными СНВ (P- норма разности СНВ матрицы контейнера и матрицы СК, N – номер СНВ) (а); эффективность декодирования (P,%) при различных значениях D(б).

[57] Борисенко И.И. Повышение помехоустойчивости стеганографического алгоритма/ И.И. Борисенко// Сучасний захист інформації. – 2010. – №1. – С. 36-42.

Выводы. Таким образом на базе ОПАИС разработаны общие теоретические принципы, использование которых стало основой для создания стеганографических алгоритмов, устойчивых к возмущающим воздействиям, что дало возможность повысить эффективность процесса передачи секретной информации по каналам общего пользования, а значит увеличить надежность комплексной системы защиты информации в целом.

References:

1. Кобозева А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованій на теорії збурень / А.А. Кобозева// Информационные технологии и компьютерная инженерия. – 2008. – №1. – С. 164-171.
2. Гонсалес Р. Цифровая обработка изображений / Р.Гонсалес, Р.Вудс; пер. с англ. под ред. П.А. Чочиа. – М.: Техносфера, 2005. – 1072 с.
3. Кобозева А.А. Стеганографические SS-методы, использующие сингулярное и спектральное разложения матрицы контейнера / А.А. Кобозева, И.И.Борисенко//Зв'язок. – 2007. – №7(75). – С. 34-38.
4. Борисенко И.И. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений /И.И. Борисенко, А.А. Кобозева //ПраціУНДІРТ. – 2006. – №3(47). – С. 78-83.
5. Кобозева А.А. Стеганографический SS-метод, использующий модулирующий сигнал специального вида /А.А. Кобозева, И.И. Борисенко// Вісник Східно-укр-го нац-го ун-ту ім. В.Даля. – 2007. – №5(111), ч.1. – С.24-32.
6. Борисенко И.И. Стеганографический алгоритм, основанный на SS – методе и использующий пространственную область контейнера/ И.И.Борисенко// Вісник східноукраїнського національного університету ім. В.Даля. – 2011. – №7.– С. 41-45.
7. Борисенко И.И. Особенности применения многоуровневого порогового преобразования изображения в компьютерной стеганографии /И.И. Борисенко// Праці УНДІРТ. – 2006. – №4(48). – С. 53-59.
8. Борисенко И.И. Использование теории графов в стеганографии/ И.И. Борисенко// Спеціальна техніка у правоохоронній діяльності. Матеріали IV Міжнародної науково-практичної конференції. – 2009. – С. 90-102.
9. Борисенко И.И. Повышение помехоустойчивости стеганографического алгоритма/ И.И. Борисенко// Сучасний захист інформації. – 2010. – №1. – С. 36-42.