УДК 681.322:621.391

А. С. Васюра, к.т. н., проф.; В. В. Лукичёв

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДА ШАБЛОННОГО ВСТРАИВАНИЯ ДАННЫХ В ИЗОБРАЖЕНИЯ

Предложен метод встраивания данных в изображение, которые в дальнейшем подлежат обработке JPEG-алгоритмом. Рассмотрены особенности встраивания, которые определяют секретность и стойкость скрытых данных. С целью разработки эффективного стеганографического метода синтезирован критерий, который использовано в качестве целевой функции при встраивании. Таким образом, процедура скрытия данных реализуется путем решения задачи оптимизации.

***Ключевые слова**: стеганография, метод шаблонного встраивания, секретность, робастность, JPEG-алгоритм, вейвлет-преобразование.*

Введение

Стеганография изображений является областью, которая достала отвесного развития на протяжении последних десяти лет. Ее цель может быть очерчена как тайное и стойкое к разнообразным преобразованиям сокрытии данных. Соответственно практические задачи, которые решаются в ее границах, в большей или меньшей мере касаются аспектов секретности и робастности [1, 2].

Поскольку нарушение секретности может привести к полной потере сообщения, то именно указанное качество задает основные ограничения при проектировании стегосистемы. Надо отметить, что относительный характер этого показателя обуславливает существование большого количества критериев, эффективность которых неодинаковая для разных методов встраивания.

Другим важным аспектом является требование стойкости. Поскольку широко распространенные схемы избыточного кодирования с защитой от ошибок, то вопрос робастности может быть решено с эффективностью, которая определяется достоверностью восстановленной информации [3].

Таким образом, проектирование любой стегосистемы можно рассматривать как задачу условной оптимизации, где целевая функция определенным образом связывает робастность со степенью секретности, а ограничения определяют область адекватности критерия. Такой универсальный подход разрешит обеспечить высокую адаптивность к условиям непосредственного функционирования стегосистемы.

В стеганографии изображений особенно распространенной есть схема слепого встраивания, где передается лишь стегоконтейнер. Это определяет особенности стегоанализу, задача которого состоит в бинарной классификации изображений на основе свойств, которые испытывают наибольших изменений при встраивании. Особенно перспективными есть критерии на основе аппаратов векторного деления (SVM) [4], наибольшим преимуществом которых является эффективность классификации точек-характеристик в многомерном пространстве признаков.

Среди методов обработки изображений наибольшей популярностью пользуются методы сжатия. Наибольший коэффициент уплотнения способны обеспечить методы сжатия с потерями [5]. Стандарт сжатия JPEG и до сих пор используется широко, несмотря на внедрение более эффективных форматов на основе вейвлет-преобразований (например JPEG2000). Такая ситуация, очевидно, обусловленная инертностью концепций разработки программного обеспечения в этой сфере, которая в свою очередь разрешает прогнозировать значительную продолжительность перехода.

Поэтому в качестве основного фактора влияния на стегоконтейнер рассматривается

обработка JPEG. С другой стороны, стеганографичиское использование вейвлет-преобразований дает основания надеяться на неприметность внесенных изменений. С помощью разработанного критерия предлагается исследовать комплексную связь между секретностью и робастностью указанного использования в области вейвлет-преобразований.

Коэффициенты решенные модифицировать соответственно распространенному подходу векторной квантизации. Его разновидностью является шаблонная схема встраивания, для которой значение тайной порции данных зависит от соотношений набора коэффициентов с определенным эталонным значением [6]. Основным преимуществом шаблонной схемы есть возможность многовариантного представления порции тайных данных, которая разрешает повысить их стойкость.

Во время разработки современных методов скрытия в большинстве случаев оптимизируется одно из качеств секретности или робастности. Использование критерия, который объединяет определенные качества, призвано повысить эффективность стегозащиты. Аспект актуальности не исчерпывается лишь данным критерием: предложен адаптивный путь его улучшения. Для этого учитываются свойства каждого объекту стеганографического манипулирование, который несет элементарную частицу тайных данных.

Предполагается, что особенности предложенного в статье подхода обеспечат высокую эффективность стегометода на его основе. Разработка такого метода является целью данного исследования.

Критерий стеганографической эффективности

Комплексную оценку эффективности стегометода предлагается осуществлять с использованием независимых показателей секретности и робастности. Меру робастности определено как частицу сохраненных элементарных порций тайных данных после обработки стегоизображения. В качестве критерия секретности избрано стегоаналитический критерий, предложен в [4]. Он использует SVM для классификации изображений. Для этого каждое изображения характеризуется вектором постоянной длины, значения которого получают путем сравнения соседних пикселов.

Таким образом, для каждого стегоаналитического критерия связь между PSNR и энтропией детектирования $e^{\det} = -p\log p - \overline{p}\log\overline{p}$ есть прямым, где $\overline{p} = 1 - p$, p – вероятность верной классификации. Для данного критерия экспериментально установлена высокая корреляция между этими показателями. Поэтому в дальнейшем эта связь рассматривается по умолчанию.

Оценка эффективности встраивания предусматривает учет следствий определенных характерных влияний со стороны третьего лица. В случае применения JPEG-компрессии, результат зависит от параметров сжатия, которые задаются пользователем. Квантование коэффициентов ДКП описывается зависимостью

$$dct_{i,j}^{jpeg} = \frac{Q_{i,j}}{q}\,\mathrm{round}\left(\frac{dct_{i,j}}{Q_{i,j}}\,q\right), \qquad (1)$$

где $Q_{i,j}$ – соответствующий элемент матрицы квантования Q, $i, j = 1\ldots8$, q – параметр, который задается пользователем и определяет качество и размер сжатого изображения [5]. Конечно, невозможно в каждом конкретном случае предусмотреть значение q, однако использование статистического распределения f_q разрешает перейти к обоснованной оценке. Рис. 1 отображает типичное распределение f_q. Поскольку результат обработки JPEG-алгоритмом (квантование) зависит от значений коэффициентов ДКП, то стойкость встроенных данных для разных блоков изображения будет разной. Такое же замечание

касается количественной меры искажений встраивания. При JPEG-сжатии блоки изображения 8×8 обрабатываются независимо. Поэтому при условии независимого встраивания в эти блоки, можно получить адаптивную к требованиям секретности и робастности стегосистему.

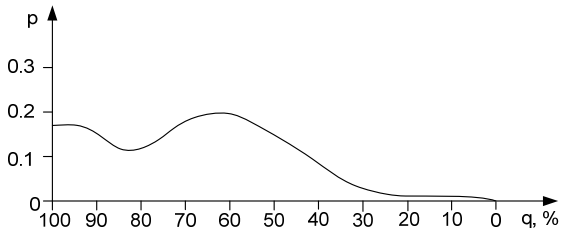

Рис.1. Типичное распределение значений параметра q

Критерий эффективности встраивания должны быть интегральным, поскольку вместо значения q известно лишь распределение f_q. Таким образом определенному i-му условию квантования, которое полностью определяется q_i, отвечает вероятность f_{q_i} и комплексная характеристика эффективности системы z_i. Если z_i определить как произведение стегоаналитической энтропии детектирования $e_i^{\det}$ и показателя робастности $r_i = 1 - \mathrm{BER}_i$, где BER – показатель битовых ошибок, то критерий общей эффективности встраивания можно представить выражением:

$$E = \sum_i z_i f_{q_i} = \sum_i e_i^{\det} r_i f_{q_i} . \tag{2}$$

Учитывая, что значение показателей $e_i^{\det}$ и r_i являются зависимыми от энергии встраивания $d = \left\| I^{org} - I^{stg} \right\|^2$ (искажение стегоизображения I^{stg} в сравнении с оригинальным I^{org}), предыдущее выражение принимает вид

$$E(d) = \sum_i e_{i,d}^{\det} r_{i,d} f_{q_i} . \tag{3}$$

Для случая непрерывного изменения условий квантования имеем:

$$E(d) = \int e^{\det}(q,d) r(q,d) f(q) dq . \tag{4}$$

Однако предложенный адаптивный подход требует дополнительного определения критерия эффективности встраивания. За вышеупомянутым предположением $e^{\det}(q,d)$ является однозначной функцией. Для большинства популярных стегометодов это касается и показателя робастности $r(q,d)$. В случае адаптивного встраивания, аргументов (q,d) недостаточно для адекватного представления уровня робастности, поскольку каждый из объектов стеганографического манипулирование может испытывать неоднозначное влияние. Поэтому ключевым моментом максимизации $E(d)$ будет поиск $r(q,d,\Omega)$, где $\Omega = \{\Omega_j\}$, $j = 1 \ldots m$, Ω_j – вектор состояния j-го объекта. Конечная задача проектирования стегометода формализуется:

$$\max_d \left(\max_{\Omega} \int e^{\det}(q,d) r(q,d,\Omega) f(q) dq \right). \tag{5}$$

Очевидно, эффективность встраивания будет определяться не только методами оптимизации при решении поставленной выше задачи. Способ встраивания (схема) в первую

очередь задает ограничение и существенно влияет на результат [2]. Хотя предложенный подход можно соединить с любой схемой, решено использовать шаблонную. Этот выбор объясняется высокой степенью свободы манипулирования.

Модель шаблонного встраивания данных в вейвлет-коэффициенты

Шаблонная схема, которая взята за основу стегометода, является набором условий, которые однозначно интерпретируются при извлечении порции тайных данных. Но при встраивании порция одинаковых данных может отображаться разными условиями. Таким образом, имеет место зависимость «один-много». Набор условий избранной шаблонной схемы описывает соотношение между четырьмя скалярными значениями и единой пороговою константой TH при встраивании двух бит тайных данных (табл. 1). Каждое условие описывается четырьмя битами, которые отвечают логическому результату выполнения неровности $a_l^j \geq TH, l = 1\ldots 4, j = 1\ldots m$, где a_l^j – l-и элемент j-го объекта манипулирования [6].

Таблица 1

Логические условия встраивания данных по шаблонной схеме

Тайные данные	0 0	0 1	1 0	1 1
Условие	0 0 0 1	0 1 1 1	0 0 0 0	1 1 1 1
	0 0 1 0	1 0 1 1	0 0 1 1	1 0 0 1
	0 1 0 0	1 1 0 1	0 1 0 1	1 0 1 0
	1 0 0 0	1 1 1 0	0 1 1 0	1 1 0 0

Преимуществами такой схемы есть гибкость и возможность обеспечения высокой робастности. С другой стороны это приводит к избыточности и как следствие - больших искажений, поскольку два биты встраиваются в четыре элемента. Тем не менее, выбор данной схемы связан с возможностью использования свойства гибкости с целью обеспечения оптимального соотношения между искажениями и робастностью.

Определение метода преобразования для получения элементов, которые используются шаблонной схемой, существенно будет влиять на общую эффективность [7]. Главной особенностью вейвлет-преобразований является масштабируемое отображение сигнала x:

$$\varphi_{j,n}(x) = \sqrt{2^j}\varphi(2^j x - n),\ \psi_{j,n}(x) = \sqrt{2^j}\psi(2^j x - n), \tag{6}$$

где $\varphi_{j,n}(x)$, $\psi_{j,n}(x)$ – функция масштабирования и вейвлет-функция соответственно, j – уровень разложения, n – сдвиг [8, 9]. Например, с помощью ортонормального базиса Добеши

$$\mathbf{D} = \begin{bmatrix} h_0 & h_1 & h_2 & h_3 & \underbrace{0 \ \ldots \ 0}_{n-4} \\ 0 & 0 & h_0 & h_1 & h_2 & h_3 & \ldots \\ & & & \vdots & & & \\ & & & n/2-3 & & & \\ & & & \vdots & & & \\ h_2 & h_3 & 0 & \ldots & 0 & h_0 & h_1 \\ g_0 & g_1 & g_2 & g_3 & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & \ldots \\ & & & \vdots & & & \\ g_2 & g_3 & 0 & \ldots & 0 & g_0 & g_1 \end{bmatrix} \tag{7}$$

преобразование сигнала $\mathbf{S} = [s_1 \ \ldots \ s_i \ \ldots \ s_n]$ может быть представлено в матричной форме:

$$\mathbf{W} = \mathbf{D} \times \mathbf{S}^T, \tag{8}$$

где $\mathbf{W}^T = [\underbrace{w_1 \quad \dots \quad w_{n/2}}_{low} \quad \underbrace{w_{n/2+1} \quad \dots \quad w_n}_{high}]$. Путем дальнейшего разложения компоненты *low* получают систему масштабируемых отображений сигнала $\mathbf{S}$. Для изображений используется двухмерное вейвлет-преобразование:

$$\begin{aligned} \varphi_{j,k,n}(x,y) &= 2^j \varphi(2^j x - k)\varphi(2^j y - n), \quad \psi^H_{j,k,n}(x,y) = 2^j \varphi(2^j x - k)\psi(2^j y - n), \\ \psi^V_{j,k,n}(x,y) &= 2^j \psi(2^j x - k)\varphi(2^j y - n), \quad \psi^D_{j,k,n}(x,y) = 2^j \psi(2^j x - k)\psi(2^j y - n). \end{aligned} \tag{10}$$

Масштабирование с помощью вейвлетов разрешает избрать оптимальный с точки зрения критерия E уровень отображения.

Поскольку во время компрессии JPEG коэффициенты ДКП квантуются неодинаково, можно выделить часть ДКП базиса, где искажение квантования будут меньшими. Соответственно полнота отображения области манипулирования в этой части базиса будет более желательной для обеспечения робастности. Выбор уровня вейвлет-отображений для встраивания напрямую связан с этим приоритетом. Это можно продемонстрировать путем сравнения значений проекций векторов вейвлет-базису на значащую часть базиса ДКП. Понятие значащей части есть довольно условным, но в большинстве параметры JPEG сжатия предусматривают ненулевое значение части коэффициентов ДКП, что отделенные границей на рис. 2,а.

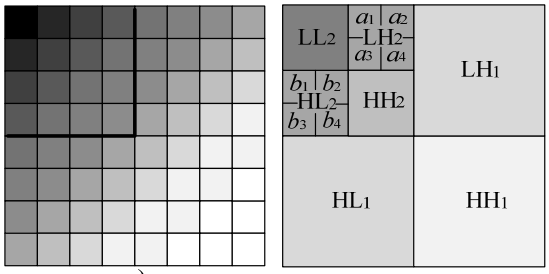

Рис.2. а) Степень значимости коэффициентов ДКП; б) Значимость коэффициентов разных уровней вейвлет-преобразований

Коэффициенты ДКП задаются выражением:

$$y(k) = \varpi(k) \sum_{n=1}^{N} x(n) \cos \frac{\pi(2n-1)(k-1)}{2N}, \quad k = 1, \dots, N, \tag{11}$$

где $\varpi(k) = \begin{cases} 1/\sqrt{N}, & k = 1 \\ \sqrt{2/N}, & 2 \le k \le N \end{cases}$, $x(n)$ – сигнал, N – количество коэффициентов ДКП [5].

Соответственно двухмерное ДКП определяется как

$$\begin{aligned} B_{pq} &= \alpha_p \alpha_p \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1; \\ 0 \le q \le N-1; \end{matrix} \\ \alpha_p &= \begin{cases} 1/M, & p = 0; \\ \sqrt{2/M}, & 1 \le p \le M-1; \end{cases} \quad \alpha_q = \begin{cases} 1/N, & q = 0; \\ \sqrt{2/N}, & 1 \le q \le N-1. \end{cases} \end{aligned} \tag{12}$$

Пусть значащую часть ДКП базиса для преобразования фрагмента изображения 8×8 обозначим $\mathbf{C}^{pr}_{16}$. Тогда проекции $T_i, i = 1 \dots 16$ части вейвлет-базиса $\mathbf{H}^{pr}_{16}$, который определяет левую верхнюю четверть коэффициентов на рис. 2,б, будут вычисляться как $T_i = \sum_j (v_{i,j})^2$, $\mathbf{V} = \mathbf{H}^{pr}_{16} (\mathbf{C}^{pr}_{16})^T$, $v_{i,j} \subset \mathbf{V}$ (поскольку оба базиса есть ортонормальными) [8, 9]. Гистограммы значений проекций для вейвлетов Хаара и Добеши приведены на рис. 3,а и 3,б

соответственно.

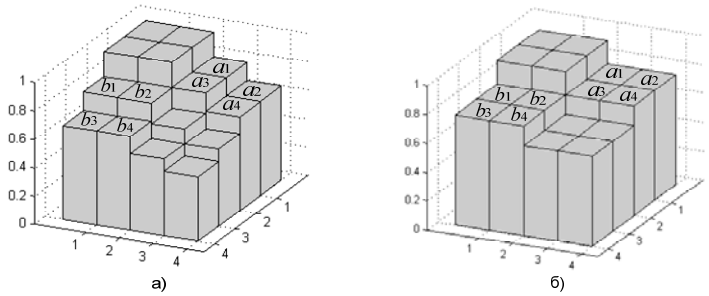

Рис.3. Значение проекций векторов вейвлет-базисов на «главную» часть базиса ДКП: а) базис Добеши; б) базис Хаара

Установленная с помощью проекций связь между базисами позволяет выбирать элементы для формирования объектов стеганографического манипулирования. Выбор совокупностей элементов $\{a_1, a_2, a_3, a_4\}$ и $\{b_1, b_2, b_3, b_4\}$ объясняется соображением о последствиях их изменения на изображении (искажение) с одного стороны и чувствительность отображения этих изменений при условии JPEG-сжатия (робастность) с другой.

На эффективность шаблонной схемы встраивания существенно влияет выбор значения TH. При условии манипулирования в области вейвлет-коэффициентов $LH2$ и $HL2$, их значения будут колебаться возле нуля. Потому выбор $TH = 0$ разрешит увеличить количество встроенных двухбитовых порций тайных данных при фиксированных ограничений на искажение (рис. 4).

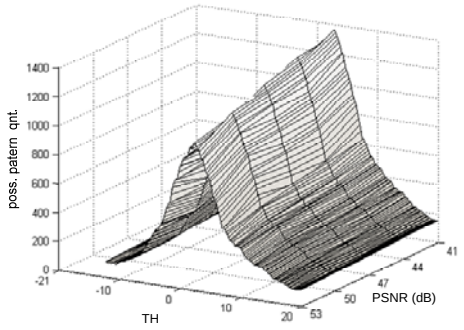

Рис. 4. Зависимость количества встроенных шаблонов от значения TH и допустимого уровня PSNR

Возвращаясь к решению задачи

$$\max_{d}\left(\max_{\Omega}\int e^{\det}(q,d)r(q,d,\Omega)f(q)dq\right) \qquad (13)$$

относительно предложенной схемы и объекта стеганографического манипулирования, необходимо определить особенности формирования Ω. Очевидно, интерпретация Ω в области изображения должна быть однозначной. С другой стороны Ω является единым аргументом первого этапа оптимизации, но формируется постепенно с помощью $\Omega_j, j = 1\ldots m$. Поэтому необходимо, чтобы всем возможным значением Ω_j отвечало оптимальное соотношение между робастностью и уровнем искажений. Поэтому для каждого j-го объекта при всех заведомо установленных (табулированых) значениях q_i нужно поставить и решить задачу минимизации искажений.

Однако особенности ограничений не разрешают применять методы классической оптимизации для решения сформулированной задачи [10]. Это объясняется, во-первых,

необходимостью получения целочисельного результата (значение пикселов – целые числа), во-вторых, после ДКП и соответствующего q_i квантования шаблонная интерпретация значений вейвлет-коэффициентов должна совпадать с порцией встроенных данных:

$$\left\| P^{org} - P^{stg} \right\|^2 \to \min, \tag{14}$$

за ограничений

$$\begin{cases} p_{i,j}^{stg} \in Z, \quad i,j = 1\ldots 8; \\ \mathbf{M}^{emb} \times (\mathbf{D} \times \mathbf{C} \times Q_i(\mathbf{C} \times \overline{P}^{stg}) - \mathbf{TH}) \le \mathbf{0}, \end{cases} \tag{15}$$

где $\overline{P}^{stg}$ – столбец, который представляет пиксели P^{stg}; $Q_i(\bullet)$ – оператор квантования соответственно i-ого условия; $\mathbf{M}^{emb}$ – маска, которая интерпретирует порцию данных для встраивания; **TH** и **0** – столбец, которые содержат лишь значение TH и 0 соответственно.

Этапы оптимизации стеганографической модели

В разделе, прежде всего, предлагается метод, призван обеспечить субоптимальность решение для всех возможных значений Ω_j, $j = 1\ldots m$, потом – метод оптимального формирования Ω.

Единой преградой на пути решения поставленной в конце предыдущего раздела задачи методом наименьших квадратов с линейными ограничениями является нелинейность оператора $Q_i(\bullet)$. Это объясняет необходимость итеративного подхода использования данного метода при приближении к оптимуму [11].

Предложен эволюционный алгоритм, суть которого заключается в следующем. Генотипом является вектор G_i длиной 64, элементы которого принимают значение с $\{0,1\}$. Каждое поколение p формируется совокупностью $\mathbf{G}^p = \{G_i^p\}$, $i = 1\ldots g$. Для образования $\mathbf{G}^{p+1}$:

1) осуществляется выбор c наилучших носителей $\dot{G}_i^p$ генотипа с наименьшим значением показателей

$$A_i = \sum_{j=1}^{64} (G_{i,j}^p - \dot{G}_{i,j}^p), \tag{16}$$

$$\dot{G}_{i,j}^p = \begin{cases} 0, G_{i,j}^p = 0; \\ 1, Q_i^i(\mathbf{C} \times \overline{P}^{stg^p}) \ne Q_i^i(\mathbf{C} \times \overline{P}^{stg^{p-1}}); \\ -1, Q_i^i(\mathbf{C} \times \overline{P}^{stg^p}) = Q_i^i(\mathbf{C} \times \overline{P}^{stg^{p-1}}), \end{cases}, \tag{17}$$

где $\overline{P}^{stg^p}$ получаем вследствие решения задачи

$$\left\| P^{org} - P^{stg^p} \right\|^2 \to \min, \tag{18}$$

за ограничений

$$\begin{cases} p_{i,j}^{stg^p} \in Z, \quad i,j = 1\ldots 8; \\ \mathbf{M}^{emb} \times (\mathbf{D} \times \mathbf{C} \times (\hat{\mathbf{C}}^{G_i^p} \times \overline{P}^{mid^p} + \check{\mathbf{C}}^{G_i^p} \times \overline{P}^{stg^{p-1}}) - \mathbf{TH}) \le -\Delta^p; \end{cases} \tag{19}$$

тогда промежуточное стегоизображение на итерации p будет:

$$\overline{P}^{stg^p} = \mathbf{C} \times (\hat{\mathbf{C}}^{G_i^p} \times \overline{P}^{mid^p} + \check{\mathbf{C}}^{G_i^p} \times \overline{P}^{stg^{p-1}}), \tag{20}$$

где $\hat{c}_{l,m}^{G_i^p} = G_{i,l}^p \cdot c_{l,m}$; $\check{c}_{l,m}^{G_i^p} = (1 - G_{i,l}^p) \cdot c_{l,m}$; $\hat{c}_{l,m}^{G_i^p} \subset \hat{\mathbf{C}}^{G_i^p}$, $\check{c}_{l,m}^{G_i^p} \subset \check{\mathbf{C}}^{G_i^p}$; $\overline{P}^{mid^p}$ – столбець

промежуточных значений пикселов, Δ^p – столбец элементов со значением Δ^p, которое есть положительным и определяется на основе $\mathbf{G}^p$ и Δ^{p-1};

2) получаем $g = C_c^2$ комбинаций скрещенных последовательностей $\ddot{G}_i^p$ путем образования одной точки разрыва для двух $\dot{G}_l^p$ и $\dot{G}_m^p$, $l \neq m$, и попарным их совмещением;

3) реализуется замена со случайным результатом (мутация) для всех значений -1, вследствие чего получаем $\mathbf{G}^{p+1}$: $\mathbf{G}^{p+1} \Leftarrow \ddot{\mathbf{G}}^p$,

$$\forall i, j \; G_{i,j}^{p+1}(-1) = \begin{cases} 1, \; p^{mut}(1) = y; \\ 0, \; p^{mut}(0) = 1 - y, \end{cases} \tag{21}$$

где y – определенное постоянное значение. Эволюция будет длиться, пока не выполнится условие (15), или Δ^p не превысит определенный установленный порог $T\Delta$.

Таким образом, основное свойство решения предложенным методом заключается в итеративном генерировании директив встраивания, которое призвано обеспечить высочайшую чувствительность при условии квантования с параметром q_i. Однако сходимость к условиям (15) не может быть обоснованная, поэтому, с целью сбережения вычислительных ресурсов, установлено $T\Delta$ [10, 11].

Следующий этап предусматривает определение Ω. Для упрощения при постановке и решении задачи используются лишь значение искажений d_i^j, которые отвечают сохранению соответствующей порции тайных данных в j-ом фрагменте изображения за i-ого условия квантования коэффициентов ДКП при JPEG-сжатии. Если соотношение между d_i^j и q_i есть наиболее удачным, это отображает единицей в i-ой позиции вектора Ω_j, где остальные позиции есть нулями. Для определения таких соотношений необходимо принимать во внимание все m объекты и общее ограничение на искажение Td. Главной особенностью, которая используется при решении, есть возможность определения влияния на значение целевой функции и искажение при выборе Ω_j независимо от остальных объектов.

При условии известного и неизменного стегоключа и тайных данных, каждая порция данных соотносится с определенным фрагментом изображения. Пусть условие квантования, которое отвечает встраиванию j-ой порции данных с минимальным искажением $d_{\min}^j$, обозначим $q_{\min}^j$. Тогда нижняя граница общих искажений изображения $Td_{\min} = \sum_j d_{\min}^j$. При запредоставлении Td необходимо придерживаться $Td \geq Td_{\min}$. Таким образом, при робастному встраивании данных в j-ый фрагмент с параметром $q_i^j \neq q_{\min}^j$ получаем улучшение (увеличение) критерия E на ΔE_i^j и соответствующее увеличение искажений на Δd_i^j. При условии фиксированного набора значений $q_i, i = 1 \ldots r$, количество вариантов оптимизации E соответственно лишь к j-ому фрагменту не будет превышать $r - 1$. Пусть в результате каждой итерации алгоритма оптимизации получаем подтверждение или опровержение перехода от $q_{\min}^j$ к q_i^j для всех m фрагментов, где для каждого j-го фрагмента может устанавливаться независимое от других i-ых значении параметра квантования. Если для j-го фрагмента возможность перехода отброшена, то при дальнейших итерациях параметр q_i не рассматривается в качестве варианта перехода. Если переход подтвержден, на следующей итерации проверяется возможность этого же варианта перехода. Оптимизация закончена когда для все опровержения отброшены последний возможный переход, или получены m подтверждения. Ведь в случае найповільнішого решения, где в результате каждой итерации опровергается лишь один переход сред m,

требуется не больше $m(r-1)$ итераций для достижения сходимости [11].

Последним аргументом оптимизации есть Td, который определяется в результате решения задачи без ограничений.

Эксперимент

Целью эксперимента являются сравнения эффективности встраивания данных разработанным методом и методами, которые широко используются на практике. Для сравнение избрано: метод последнего значащего биту (ПЗБ) [12], шаблонный метод на основе целочисельного вейвлет-преобразования (IWT) [6] и метод, который оперирует в области ДКП [13]. В избранные изображения за единым стегоключем были встроены тайные данные. Эффективность методов определялась по двумя зависимостями: секретность стегоманипуляций и робастность встроенных данных от параметра q, который задает степень сжатия. Поскольку разработка метода велась на основе предложенного критерия эффективности встраивания, то сравнение с остальными методами по этому критерию и упомянутыми выше зависимостями разрешит установить адекватность критерия.

Соответственно описанным особенностям проектирования стегометода, для постановки и решение задачи оптимизации встраивания необходимо предварительно определить распределение $f(q)$ и функцию стегоаналитической энтропии детектирования $e^{\det}(q,d)$. Зависимость $f(q)$ установлена путем экспертного распознавания популярных и широко используемых изображений в градациях серого размером 256×256, который в зависимости от нужд рассмотренных web-страниц обрабатывались JPEG алгоритмом с разным значением параметра q. При определении $e^{\det}(q,d)$ для каждого q_i (значение q_i изменялись от 1 до 0.65 с шагом 0.05) было сформировано учебную и тестовую выборки. Первая использовалась для тренировки SVM соответственно предложенного в [4] вектора характеристик, на второй определялась средняя вероятность верного детектирования в зависимости от значения искажений d. Изображение в учебной и тестовой выборках не совпадают. Каждая выборка наполовину состоит из оригинальных изображений (количеством 400), остальные – стегоизображения, полученные из оригинальных с помощью описанной шаблонной схемы встраивания. На рис. 5 изображен график функции вероятности детектирования $p^{\det}(q,d)$.

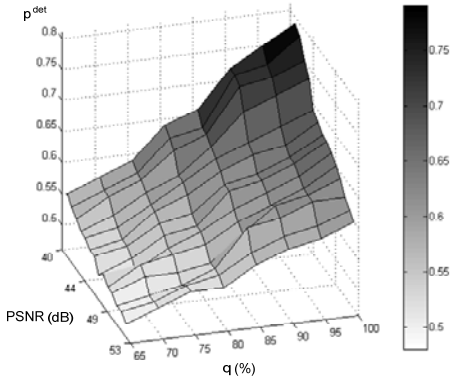

Рис.5. Зависимость вероятности детектирования от параметра q и уровня искажения(PSNR).

Вследствие проведения описанных этапов оптимизации встраивания 2000 бит тайных данных в вейвлет-коэффициенты Хаара соответственно критерию E, количественный показатель эффективности, который есть средним для 20 изображений, составил 0.63. Для описанного в [6] метода на основе целочисельного вейвлет-базису значения критерия составляет 0.48, эффективность встраивания в область ДКП [13] оценивается 0.42,

стеганографическая эффективность метода [12] на основе ОЗБ – 0.28.

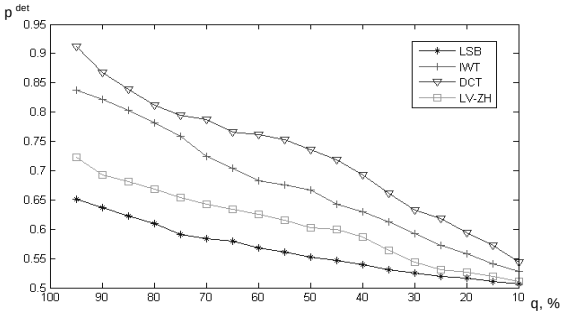

Рис.6. Зависимость вероятности детектирования p^{det} от параметра качества

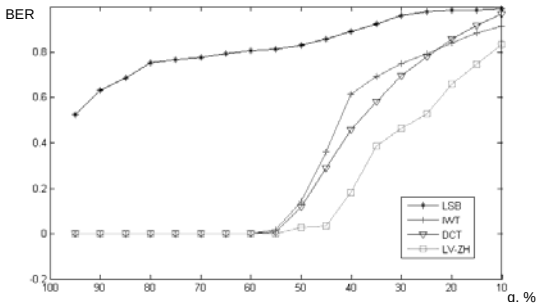

Рис.7. Связь робастности r встроенных данных от параметра q

С целью демонстрации адекватности критерия и эффективности разработанного метода, приведено два графика зависимостей вероятности детектирования p^{det} от q (рис. 6) и робастности встраивания r от q (рис. 7), что наглядно показывает преимущества и недостатки каждого из оцененных выше методов.

Выводы

Разработано стеганографический метод, который использует принцип шаблонного встраивания в области вейвлет-коэффициентов. Особенностью метода есть учеты требований секретности и робастности к JPEG-преобразованию, которая реализована путем их объединения с помощью предложенного критерия. Таким образом, задачу разработки было поставлено как задачу оптимизации с ограничениями, которая решена поэтапно.

Предложенный подход разрешает повысить общую эффективность встраивания данных, которая подтверждена экспериментально при сравнении с популярными стегометодами. Недостатком метода является сложность, которая обусловлена дифференционной особенностью встраивания и, как следствие, необходимостью итеративного решения численных задач оптимизации.

Тем не менее, использованные подходы оптимизации допускают поиск компромиссов между вычислительной сложностью и эффективностью решения, что является целью дальнейших исследований. Еще одним перспективным направлением исследований являются использования предложенного подхода встраивания за других преобразований обработки изображений (не только JPEG).

СПИСОК ЛИТЕРАТУРЫ

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – СПб.: Солон-Пресс, 2002. – 272с.

2. Johnson N., Duric Z., Jajodia S. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, New York. – NY.: Kluwer Academic Pub, 2000. – 200p.

3. Glavieux A. Channel Coding in Communication Networks. – London: Hermes Science Pub. Ltd., 2007. – 416p.

4. Zou D., Shi Y., Su W., Xuan G. Steganalysis based on Markov Model of Thresholded Prediction-Error Image // IEEE ICME Conference Record, 2006. – P. 1365-1368.

5. Pennebaker W., Mitchell J. JPEG: Still Image Compression Standard. – NY.: Kluwer Academic Pub., 1993.

6. Васюра А.С., Лукічов В.В. Метод вбудовування даних на основі алгоритму вейвлет-стиснення зображень // Матеріали XIII міжнародної конференції з автоматичного управління „Автоматика-2006”. – Вінниця: Универсум-Вінниця, 2007. – С. 491-495.

7. Marvel L. M., Retter C. T. Spread Spectrum Image Steganography // IEEE Transactions on Image Processing, 1999. – № 8. – P. 1075-1083.

8. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. – М.: Триумф, 2003. – 320с.

9. Mertin A. Signal Analysis: Wavelets, Filter Banks, Time-Frequency Transforms and Applications. – NY.: John Wiley and Sons, 1999. – 310p.

10. Fletcher R. Practical Methods of Optimization, second edition. – NY.: John Wiley and Sons, 2000. – 450p.

11. Kelley C. T. Iterative Methods for Optimization. Frontiers in Applied Mathematics. – Philadelphia: SIAM, 1999. – 196p.

12. Wu H.C., Wu N.I., Tsai C.S., Hwang M.S. Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods // IEEE Transactions on Image and Signal Processing, 2005. – № 5. – P. 611-615.

13. Quan L., Qingsong A Combination of DCT-Based and SVD-Based Watermarking Scheme // IEEE ICSP Conference Record, 2004. – № 1. – P. 873-876.

Васюра Анатолий Степанович – директор института, профессор кафедры автоматики и информационно-измерительной техники;

Лукичёв Виталий Владимирович **–** соискатель кафедры автоматики и информационно-измерительной техники.

Винницкий национальный технический университет