УДК 004.056.5: 518

А. А. КОБОЗЕВА, д-р техн. наук, проф. ОНПУ, Одесса;
С. АЛЬФАЛУДЖИ, аспирант ОГАХ, Одесса

СТЕГАНОГРАФИЧЕСКИЙ АЛГОРИТМ, ОБЕСПЕЧИВАЮЩИЙ БОЛЬШУЮ ПРОПУСКНУЮ СПОСОБНОСТЬ КАНАЛА СКРЫТОЙ СВЯЗИ

У роботі пропонується новий стеганографічний алгоритм, який використовує малорангові апроксимації матриці цифрового зображення як контейнер, що забезпечує більшу в порівнянні з методом модифікації найменшого значущого біта пропускну спроможність каналу прихованого зв'язку разом зі збереженням надійності сприйняття сформованого стеганоповідомлення

В работе предлагается новый стеганографический алгоритм, использующий малоранговые аппроксимации матрицы цифрового изображения в качестве контейнера, обеспечивающий бóльшую по сравнению с методом модификации наименьшего значащего бита пропускную способность канала скрытой связи наряду с сохранением надежности восприятия формируемого стеганосообщения

Proposed a new steganographic algorithm using the low-rank matrix approximation of digital images as cover that provides greater bandwidth covert communications than the LSB-method while maintaining the reliability of perception formed stegano-message

Введение. Защита информации в современных условиях является сложной и чрезвычайно актуальной проблемой, что обусловлено рядом обстоятельств, среди которых массовое распространение средств электронной вычислительной техники, усложнение шифровальных технологий, необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн, расширяющиеся возможности несанкционированных действий над информацией [1]. Очевиден вывод о необходимости создания комплексной системы защиты информации, учитывающей угрозы национальной и международной безопасности, угрозы обществу, личности, государству, экономике, финансовым учреждениям, включающей в себя в качестве важного составного звена стеганографию [2,3].

Стеганография изучает возможности сокрытия самого факта присутствия секретной, или дополнительной, информации (ДИ) в некотором общедоступном информационном контенте – основном сообщении (ОС), или контейнере [4], и является областью исследования настоящей работы. Не ограничивая общности рассуждений, для простоты изложения далее в качестве ОС рассматривается монохромное изображение. Процесс погружения в контейнер ДИ, в качестве которой рассматривается бинарная последовательность, сформированная случайным образом, будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС).

Любой стеганографический метод (СМ) характеризуется тремя основными параметрами: устойчивостью (степенью обеспечения нечувствитель-

ности СС к возмущающим воздействиям [4]), надежностью восприятия (СС не должно визуально отличаться от ОС [2]) и пропускной способностью. В соответствии с [2] под пропускной способностью канала передачи скрываемых сообщений или просто под скрытой пропускной способностью (СПС) будем понимать максимальное количество информации, которое может быть вложено в один элемент контейнера. Поскольку канал скрытой связи образуется внутри канала открытой связи, СПС будет меньше пропускной способности канала открытой связи [5], в котором за одно использование канала передается один элемент СС, содержащего ДИ [2].

Очевидно, что при организации канала связи, используемого для передачи секретной информации, чрезвычайно важным является обеспечение большой СПС, но существующие СМ, информация о которых доступна из открытой печати, не могут в полной мере удовлетворить этому требованию [2-4]. Действительно, многие СМ, используя в качестве элементов контейнера 8×8-блоки, являющиеся результатом стандартного разбиения матрицы ЦИ [6], погружают в блок лишь от 1 до 8 бит секретной информации [2,3], обеспечивая при этом СПС, равную от $1/64$ до $1/8$ бит/пикс. Алгоритмом, который на сегодняшний день является наиболее предпочтительным с точки зрения обеспечения значительной СПС, является стеганографический алгоритм модификации наименьшего значащего бита (LSB), в силу чего при оценке СПС любого вновь создаваемого стеганографического алгоритма основное внимание уделяется его сравнению именно с LSB [2-4]. LSB может задействовать при СП все пиксели ЦИ-контейнера, обеспечивая при этом СПС, равную 1 бит/пикс, хотя она потенциально может быть увеличена, например, в 2 (3) раза за счет модификации не одного, а двух (трех) наименьших значащих битов. Дальнейшее увеличение СПС за счет увеличения количества модифицированных битов может привести к нарушению надежности восприятия СС. Таким образом, проблема разработки алгоритмов, обладающих большой СПС является актуальной и нерешенной до настоящего момента. В силу этого

Целью настоящей работы является разработка стеганографического алгоритма, обладающего бóльшей по сравнению с алгоритмом LSB СПС наряду с большой вероятностью обеспечения надежности восприятия формируемого им СС.

Для достижения поставленной цели необходимо решить следующие *задачи*:

- Формализовать процесс СП;
- Учитывая достаточные условия высокой вероятности обеспечения надежности восприятия СС, получить достаточные условия обеспечения значительной СПС разрабатываемым алгоритмом.

Основными математическими инструментами при создании алгоритма являются матричный анализ и теория возмущений [7,8].

Основная идея стеганографического алгоритма, обеспечивающего большую скрытую пропускную способность. Обозначим матрицу ОС F. Процесс СП, независимо от метода и области, выбранных для погружения ДИ, можно представить как возмущение ΔF матрицы F [9,10]. Тогда матрица СС $\overline{F}$ удовлетворяет соотношению:

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

где $\Delta F = f(F)$, т.е. ΔF является некоторой функцией матрицы контейнера F [4].

Если F — матрица произвольной структуры размерами $m \times n$ с элементами $f_{ij}, i = \overline{1,m}, j = \overline{1,n}$, ($m \geq n$), для нее справедливо представление, называемое нормальным сингулярным разложением [9,10]: $F = U\Sigma V^T = \sum_{i=1}^{n} \sigma_i u_i v_i^T$, где U, V — ортогональные матрицы размерности $m \times n$ и $n \times n$ соответственно, столбцы $u_1,...,u_n$ матрицы U, называемые левыми сингулярными векторами (СНВ), лексикографически положительны [9,10] (столбцы $v_1,...,v_n$ матрицы V называют правыми СНВ матрицы F); $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$ — сингулярные числа (СНЧ); (σ_i, u_i, v_i) называется сингулярной тройкой F.

В случае, когда F — симметричная $n \times n$-матрица, для нее справедливо представление, называемое нормальным спектральным разложением (НСР) [9,10]: $F = U\Lambda U^T = \sum_{i=1}^{n} \lambda_i u_i u_i^T$, где U — ортогональная матрица, столбцы $u_1,...,u_n$ которой, называемые собственными векторами (СВ), лексикографически положительны, $\Lambda = diag(\lambda_1,...,\lambda_n)$, $\lambda_1,...,\lambda_n$ – собственные значения (СЗ), для которых $|\lambda_1| \geq ... \geq |\lambda_n|$; (λ_i, u_i) называется собственной парой. Если все $|\lambda_1|,...,|\lambda_n|$ попарно различны, то НСР определяется однозначно [4].

В соответствии с [4] любое преобразование ОС, в частности, СП, а также любое преобразование самого СС, формально будем описывать совокупностью возмущений соответствующих параметров, входящих в используемый полный набор – множество СЗ и СВ или множество СНЧ и СНВ.

Требование соблюдения надежности восприятия СС с одновременным требованием большой СПС, предъявляемые нами к создаваемому стеганографическому алгоритму, качественно находятся в обратной зависимости друг к другу.

Увеличение размера скрываемого сообщения (что вызовет обязательное увеличение возмущения ΔF контейнера) рано или поздно приведет к нарушению надежности восприятия СС [11]. До настоящего времени при анализе уровня визуальных искажений, которые вносятся в контейнер при СП, широко применяются разностные показатели, основывающиеся на различных модификациях отношения «сигнал-шум» [3], 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 [11]. Таким образом, до настоящего момента надежность восприятия в подавляющем большинстве случаев оценивается путем субъективного ранжирования, что включает в систему стеганографической передачи данных человека и вносит непреодоленные до настоящего момента трудности в процесс математической формализации обеспечения рассматриваемого требования. С уверенностью можно утверждать лишь то, что надежность восприятия сохраняется с большой вероятностью только тогда, когда норма матрицы возмущения $\|\Delta F\|$ при СП будет малой [11].

Таким образом, значительное увеличение СПС путем увеличения ΔF при СП без предварительного преобразования ОС осуществить принципиально невозможно, т.к. в этом случае с ростом $\|\Delta F\|$ возрастает вероятность нарушения надежности восприятия получаемого СС. В силу этого основная идея предлагаемого алгоритма заключается в следующем. Пусть ЦИ с матрицей $F_{исх}$ — основа для контейнера. В качестве контейнера используется предварительно преобразованное ЦИ с матрицей $F_{исх}$. Результатом преобразования должно явиться (визуальное) ухудшение изображения за счет некоторого возмущающего воздействия с матрицей $\Delta F_{исх}$. Именно это «ухудшенное» ЦИ и будет рассматриваться в качестве ОС с матрицей F: $F = F_{исх} + \Delta F_{исх}$. Процесс СП должен работать на «возвращение» первоначально «испорченного» контейнера F в исходное состояние $F_{исх}$ после погружения ДИ. Формально это требование с использованием формулы (1) будет иметь вид:

$$\overline{F} = F + \Delta F = \left(F_{исх} + \Delta F_{исх}\right) + \Delta F \approx F_{исх}.$$

Это даст возможность обеспечить надежность восприятия СС даже при значительном возмущающем воздействии ΔF, возникающем за счет СП, в случае, когда

$$\Delta F \approx \Delta F_{исх}, \qquad (2)$$

т. е. чем сильнее будет «испорчено» исходное ЦИ $F_{исх}$, тем большую СПС можно будет обеспечить при возвращении ОС с матрицей F к первоначальному состоянию $F_{исх}$ путем СП.

Предварительное преобразование контейнера. Многие известные СМ производят СП с использованием различных предварительных преобразований контейнера [2-4], однако эти преобразования в подавляющем большинстве случаев не являются для исходного ЦИ возмущающими воздействиями, а являются лишь другими, но равносильными его представлениями (при предположении отсутствия ошибок округления).

Для определенности в качестве предварительного преобразования ЦИ с матрицей $F_{исх}$ рассмотрим процесс сжатия с потерями путем замены матрицы $F_{исх}$, для которой сингулярное разложение определяется как $F_{исх} = \overline{\overline{U}}\,\overline{\Sigma}\,\overline{V}^{T} = \sum_{i=1}^{n} \overline{\sigma}_i \overline{u}_i \overline{v}_i^{T}$ (а в случае $F_{исх} = F_{исх}^{\ T}$ спектральное разложение определяется как $F_{исх} = \overline{\overline{U}}\,\overline{\Lambda}\,\overline{U}^{T} = \sum_{i=1}^{n} \overline{\lambda}_i \overline{u}_i \overline{u}_i^{T}$), на ее малоранговую аппроксимацию [7], при этом под аппроксимацией ранга k будем понимать

$$F_{исх}^{(k)} = \sum_{i=1}^{k} \overline{\sigma}_i \overline{u}_i \overline{v}_i^{T} \quad (\text{или } F_{исх}^{(k)} = \sum_{i=1}^{k} \overline{\lambda}_i \overline{u}_i \overline{u}_i^{T} \text{ в случае } F_{исх} = F_{исх}^{\ T}), \qquad (3)$$

что эквивалентно обнулению наименьших СНЧ (наименьших по модулю СЗ, если $F_{исх} = F_{исх}^{\ T}$) матрицы $F_{исх}$. Таким образом для контейнера F: $F = F_{исх}^{(k)}$. В этом случае процесс СП должен будет вернуть обнуленные СНЧ (СЗ) к значениям, близким к исходным. Такое преобразование является приемлемым и желаемым в нашем случае: возмущения наименьших СНЧ (наименьших по модулю СЗ) не должны значимо сказаться на надежности восприятия СС [11].

Отметим, что реализация процесса сжатия с использованием малоранговых аппроксимаций может проводиться как с использованием матрицы всего ЦИ, так и с использованием блоков матрицы изображения, на которые оно разбивается предварительно. Обнуление наименьших СНЧ (наименьших по модулю СЗ) при замене матрицы ЦИ или блока матрицы на малоранговую аппроксимацию практически всегда будет являться возмущением для исходной матрицы даже тогда, когда ранг аппроксимации k будет близок к размеру матрицы. Действительно, для TIF-ЦИ СНЧ (СЗ) матрицы всего изображения или блока практически никогда не содержат нулевых СНЧ (СЗ). Так при

стандартном разбиении матрицы TIF-ЦИ на блоки размером 8×8 в среднем лишь $\approx 1.5\%$ от общего числа блоков будут иметь нулевые СНЧ (СЗ) [11].

Симметризация контейнера и стеганосообщения. Если матрица $F_{исх}$ симметрична, то в качестве определяющего ее полного набора параметров можно использовать, как множество СНЧ и СНВ, так и спектр матрицы и множество СВ специального вида. Предпочтение в этом случае безоговорочно следует отдать второму набору параметров, т.к. построение НСР симметричной матрицы обладает рядом преимуществ в вычислительном смысле по сравнению с построением сингулярного разложения для матрицы произвольной структуры той же размерности и того же уровня заполненности [4,7]. Однако, как правило, матрица ЦИ $F_{исх}$ не является симметричной. Предположим, что $F_{исх}$ — $n\times n$-матрица. Для обеспечения ее виртуальной симметричности поставим в соответствие ей две симметричные $n\times n$-матрицы A_V, A_N по следующему правилу:

$$F_{исх}=\begin{pmatrix} f_{11} & f_{12} & f_{13}\cdots f_{1n} \\ f_{21} & f_{22} & f_{23}\cdots f_{2n} \\ f_{31} & f_{32} & f_{33}\cdots f_{3n} \\ \cdots & \cdots & \cdots \\ f_{n1} & f_{n2} & f_{n3}\cdots f_{nn} \end{pmatrix} \rightarrow AV=\begin{pmatrix} f_{11} & f_{12} & f_{13}\cdots f_{1n} \\ f_{12} & f_{22} & f_{23}\cdots f_{2n} \\ f_{13} & f_{23} & f_{33}\cdots f_{3n} \\ \cdots & \cdots & \cdots \\ f_{1n} & f_{2n} & f_{3n}\cdots f_{nn} \end{pmatrix}, AN=\begin{pmatrix} f_{11} & f_{21} & f_{31}\cdots f_{n1} \\ f_{21} & f_{22} & f_{32}\cdots f_{n2} \\ f_{31} & f_{32} & f_{33}\cdots f_{n3} \\ \cdots & \cdots & \cdots \\ f_{n1} & f_{n2} & f_{n3}\cdots f_{nn} \end{pmatrix}, \quad (4)$$

которые будем рассматривать ниже как основу для ОС. Контейнер будет сформирован как совокупность $AV^{(k)}$ и $AN^{(k)}$, которые очевидно также являются симметричными.

При встраивании ДИ в контейнер СП представляется в виде погружения в верхний (нижний) треугольник матрицы $A_V{}^{(k)}$ ($A_N{}^{(k)}$) с последующим виртуальным симметричным отражением результата относительной главной диагонали. Пусть итогом такого погружения явились симметричные матрицы $\overline{A}_V$ и $\overline{A}_N$. При окончательном формировании матрицы СС $\overline{F}$ используется верхний треугольник $\overline{A}_V$ и нижний треугольник матрицы $\overline{A}_N$.

Пусть E — матрица произвольного возмущения, которому подвергается ОС (или СС). В общем случае $E\neq E^T$. Матрице E поставим в соответствие две симметричных матрицы той же размерности, используя правило (4), рассматривая матрицу, отвечающую верхнему (нижнему) треугольнику E как возмущающую для контейнера (СС), полученного на основе $A_V{}^{(k)}$ ($A_N{}^{(k)}$), что дает принципиальную возможность матрицу произвольного возмущения и, как следствие, матрицу СС также рассматривать ниже как симметричные.

Таким образом, получена принципиальная возможность для рассмотрения матрицы контейнера, СС, а также матрицы результата любого возмущающего воздействия, относящегося как к ОС, так и к СС, в симметричном виде, что позволяет сократить вычислительную работу для осуществления, обработки и анализа процесса СП и любого атакующего действия.

Стеганографический алгоритм, использующий малоранговые аппроксимации матрицы контейнера. Определим матрицу разности $C(G,H)$ между двумя произвольными матрицами G и H одинакового размера естественным образом: $C(G,H) = G - H$. Обозначим $\overline{C}^{(k)} = C(A_V, A_V{}^{(k)})$, $\underline{C}^{(k)} = C(A_N, A_N{}^{(k)})$.

Пусть $p_1, p_2, \ldots$, где $p_i \in \{0,1\}$, — секретное сообщение. Для удобства далее элементы матрицы A_V (A_N) будем обозначать v_{ij} (n_{ij}), элементы $A_V{}^{(k)}$ $(A_N{}^{(k)})$ — $v_{ij}{}^{(k)}$ $(n_{ij}{}^{(k)})$, элементы $\overline{A}_V$ $(\overline{A}_N)$ — $\overline{v}_{ij}$ $(\overline{n}_{ij})$, элементы $\overline{C}^{(k)}$ $(\underline{C}^{(k)})$ — $\overline{c}_{ij}{}^{(k)}$ $(\underline{c}_{ij}{}^{(k)})$, $i, j = \overline{1,n}$.

Основные этапы при погружении ДИ нового стегоалгоритма, использующего малоранговые аппроксимации матрицы контейнера (САМАК), следующие.

Шаг 1. Для исходной матрицы $F_{исх}$ в соответствии с (4) получить A_V, A_N;

Шаг 2. Для матриц A_V, A_N построить НСР, на основе которого в соответствии с (3) получить $A_V{}^{(k)}$, $A_N{}^{(k)}$ — аппроксимации ранга k;

Шаг 3. Вычислить $\overline{C}^{(k)}$, $\underline{C}^{(k)}$;

Шаг 4. (*Погружение ДИ в* $A_V{}^{(k)}$). Пусть p_l — очередной бит секретного сообщения, подлежащий встраиванию, а биты, следующие за ним в ДИ – это $p_{l+1}, p_{l+2}, p_{l+3}, \ldots,$

если

$$p_l = 1,$$

то

- Найти очередной по заданному порядку элемент $v_{mj}{}^{(k)}$, $m < j$, матрицы $A_V{}^{(k)}$, такой, что соответствующий $\overline{c}_{mj}{}^{(k)} = t > 0$.
- В последовательности p_l, p_{l+1}, ... выделить такую ее часть $p_l, \ldots, p_{l+r}$ максимальной длины, что при рассмотрении ее в виде двоичного

представления десятичного числа, это число, обозначаемое w, будет меньше t.

- Погружение $p_l,...,p_{l+r}$ осуществить в соответствии с формулой: $\bar{v}_{mj} = v_{mj}^{(k)} + w$, где $\bar{v}_{mj}$ — соответствующий элемент стеганосообщения $\overline{A}_V$.

иначе

- В цепочке p_l, p_{l+1}, p_{l+2},... найти первый по порядку элемент $p_{l+q} \neq 0$.
- Найти очередной по заданному порядку элемент $v_{mj}^{(k)}$, $m < j$, матрицы $A_V^{(k)}$, такой, что соответствующий $\bar{c}_{mj}^{(k)} < 0$.

если

$$q < \left|\bar{c}_{mj}^{(k)}\right|,$$

то

погружение $p_l,..., p_{l+q-1}$ осуществляется в соответствии с формулой:

$$\bar{v}_{mj} = v_{mj}^{(k)} - q. \qquad (5)$$

иначе

погружение $p_l,..., p_{l+s-1}$, где $s = \left|\bar{c}_{mj}^{(k)}\right|$, осуществляется в соответствии с формулой (5); погружение $p_{l+s},..., p_{l+q-1}$ производится в следующий по заданному порядку элемент $v_{id}^{(k)}$, $i \le d$, матрицы $A_V^{(k)}$, такой, что соответствующий $\bar{c}_{id}^{(k)} < 0$.

Шаг 5. (*Погружение ДИ в* $A_N^{(k)}$). Для матрицы $A_N^{(k)}$ повторить шаг 4, используя $\underline{C}^{(k)}$, погружая ДИ в нижний треугольник $A_N^{(k)}$, формируя на основе $A_N^{(k)}$ стеганосообщение $\overline{A}_N$.

Шаг 6. Стеганосообщение $\overline{F}$ формируется как объединение двух треугольных матриц: верхнего треугольника $\overline{A}_V$ и нижнего треугольника $\overline{A}_N$.

В качестве секретного ключа в процессе декодирования используются матрица исходного изображения $F_{исх}$, ранг аппроксимации k, порядок перебора элементов верхнего (нижнего) треугольника $A_V^{(k)}$ ($A_N^{(k)}$) при СП.

Процесс декодирования ДИ состоит из следующих основных шагов.

Шаг 1. По стеганосообщению $\overline{F}$ в соответствии с (4) получить $\overline{A}_V$, $\overline{A}_N$;

Шаг 2. Найти $\overline{\overline{C}}^{(k)} = C(\overline{A}_V, A_V^{(k)})$, $\underline{\underline{C}}^{(k)} = C(\overline{A}_N, A_N^{(k)})$;

Шаг 3. (*Декодирование ДИ, погруженной в* $\overline{A}_V$). Просматриваются в соответствии с заданным порядком элементы $\overline{\overline{c}}_{ij}, i < j$, матрицы $\overline{\overline{C}}^{(k)}$.

если

$$\overline{\overline{c}}_{ij} > 0,$$

то

десятичное значение $\overline{\overline{c}}_{ij}$ представляется в двоичном виде, давая часть ДИ;

иначе

значение $\left|\overline{\overline{c}}_{ij}\right|$ определяет количество встроенных в рассматриваемый пиксель нулей.

Шаг 4. (*Декодирование ДИ, погруженной в* $\overline{A}_N$). Аналогичные шагу 3 действия проделать с нижним треугольником матрицы $\underline{\underline{C}}^{(k)}$.

Результаты вычислительного эксперимента. Одним из ключевых вопросов реализации алгоритма является выбор параметра k – ранга аппроксимации для матрицы ОС. Поскольку ДИ – это бинарная последовательность, сформированная случайным образом, при СП алгоритмом САМАК на практике не всегда удается достичь результата, обеспечивающего (2), что может неблагоприятно сказаться на надежности восприятия получаемого СС. На основании вычислительного эксперимента, проведенного в среде Matlab в условиях идеального канала связи, в котором принимало участие 300 ЦИ размером 400*400, значение параметра k рекомендуется выбирать из промежутка $\left[\frac{n}{7}, \frac{4n}{5}\right]$, где n – размер матрицы ОС, хотя для некоторых ЦИ надежность восприятия СС будет сохраняться и для $k < \frac{n}{7}$ (рис. 1).

На основании эксперимента можно утверждать, что разработанный алгоритм обладает большой потенциальной скрытой пропускной способностью (см. таблицу), хотя ее реальные показатели зависят непосредственно от конкретного секретного сообщения. Среднее значение длины секретного сообщения рассчитывалось следующим образом. В тестируемые ЦИ при заданном ранге аппроксимации погружались различные случайно сформированные бинарные последовательности. Количество экспериментов с одним ЦИ равнялось 3. В каждом конкретном случае находилась длина ДИ. Среднее значение вычислялось по всем изображениям с учетом всех трех экспериментов с каждым из них. Для вычисления среднего максимально возможного зна-

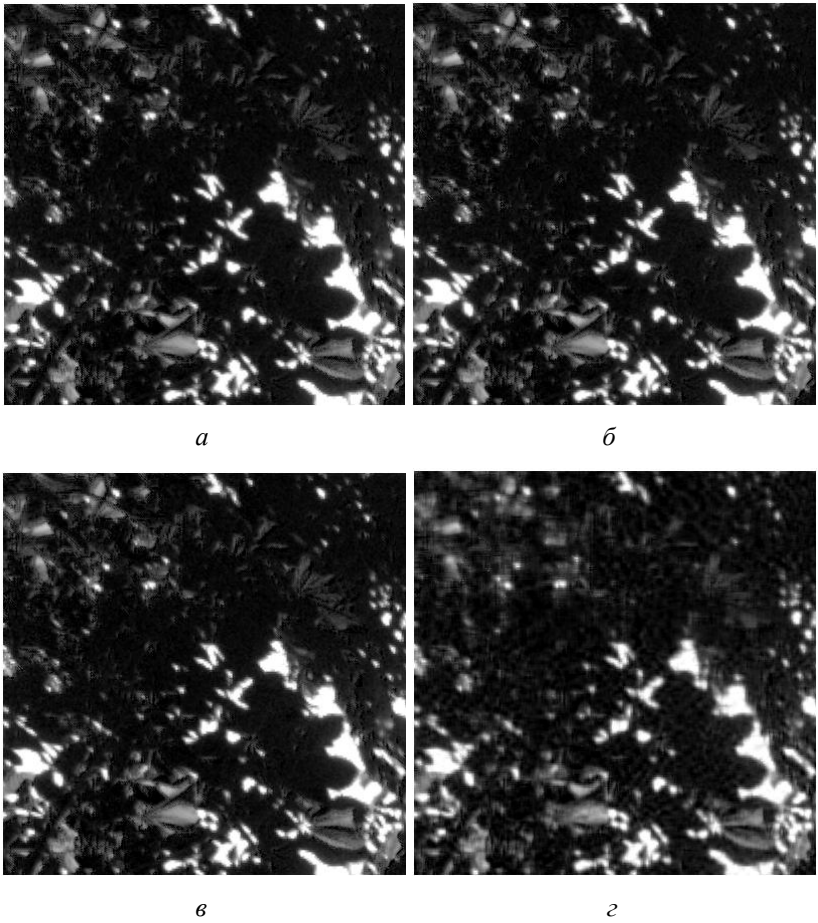
чения длины секретного сообщения для каждого ЦИ при заданном k вычислялась максимально возможная длина ДИ, а затем бралось среднее с учетом всех ЦИ.

Сравнение скрытой пропускной способности различных стеганометодов

k		150	100	$57 \approx \frac{n}{7}$
Длина секретного сообщения в LSB-алгоритме		160000	160000	160000
САМАК	Среднее значение длины секретного сообщения	112239	176002	212001
	Среднее максимально возможное значение длины секретного сообщения	221446	332135	490902

Из таблицы видно, что для достаточно малого ранга аппроксимации ($k < 150$) преимущество САМАК по сравнению с LSB-алгоритмом с точки зрения величины СПС не вызывает сомнений. Заметим, что вообще говоря, среднее максимально возможное значение длины секретного сообщения хорошо для статистики, но оно не может характеризовать конкретное ЦИ. На практике максимально возможна длина секретного сообщения может быть гораздо больше. На рис.1 приведен пример ЦИ, для которого максимально возможна длина ДИ для ранга 57 составила 751 666, для ранга 47 – 875 344 (при этом не была нарушена надежность восприятия СС (рис. *б, в*). Чтобы достичь такой же СПС в LSB-алгоритме, надо модифицировать последние 5 бит, что, как видно из рис. *г* нарушает надежность восприятия.

Заключение. В работе предложен новый стеганоалгоритм, использующий в качестве ОС малоранговые аппроксимации исходных ЦИ, применимый для любого ОС, обеспечивающий значительную СПС, рост которой достигается за счет уменьшения ранга аппроксимации, превосходящую аналогичный параметр для алгоритма модификации наименьшего значащего бита. Попытки достижения той же СПС в LSB за счет увеличения количества модифицируемых при СП битах на практике может привести к нарушению надежности восприятия соответствующего СС, что говорит в пользу алгоритма САМАК.



а *б*

в *г*

Рис.: *а* – исходное ЦИ в формате TIF; *б* – СС, сформированное на основе аппроксимации ранга 57 (длина ДИ – 362 254); *в* – СС, сформированное на основе аппроксимации ранга 47 (длина ДИ – 801 117); *г* – СС, сформированное LSB-алгоритмом.

При разработке алгоритма получена принципиальная возможность для рассмотрения матрицы ОС, СС в симметричном виде, что позволило сократить вычислительную сложность алгоритма, которая является сравнимой с количеством арифметических операций для построения НСР матрицы и составляет $\underline{O}(n^3)$, где n – размер матрицы ОС. Это количество можно уменьшить до $\underline{O}(n^2)$, если предварительно подвергнуть матрицу контейнера

операции разбиения на блоки фиксированной малой размерности, а алгоритм применять для каждого блока в отдельности.

Список литературы: 1. *Хорошко В. А.* Методы и средства защиты информации / *В. А. Хорошко*, *А. А. Чекатков*. – К. : Юниор, 2003. – 501 с. **2.** *Грибунин В. Г.* Цифровая стеганография / *В. Г. Грибунин, И. Н. Оков, И. В. Туринцев*. – М. : Солон-Пресс, 2002. – 272 с. **3.** *Конахович Г. Ф.* Компьютерная стеганография. Теория и практика / *Г. Ф. Конахович, А. Ю. Пузыренко*. – К. : МК – Пресс, 2006. – 288 с. **4.** *Кобозєва А. А.* Аналіз захищеності інформаційних систем / *А. А. Кобозєва, І. О. Мачалін, В. О. Хорошко*. – К. : ДУІКТ, 2010. – 316 с. **5.** *Шеннон К.* Работы по теории информации и кибернетики / Пер. с англ. – М. : Иностранная литература, 1963. – 829 с. **6.** *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. – М. : Техносфера, 2005. – 1072 с. **7.** *Деммель Дж.* Вычислительная линейная алгебра / *Дж. Деммель*; пер.с англ. *Х. Д. Икрамова*. – М. : Мир, 2001. – 430 с. **8.** *Кобозева А. А.* Анализ информационной безопасности / *А. А. Кобозева, В. А. Хорошко*. – К. : ГУИКТ, 2009. – 251 с. **9.** *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. **10.** *Кобозева А. А.* Стеганографический метод, основанный на преобразовании спектра симметричной матрицы / Праці УНДІРТ. – 2006. – № 4 (48). – С. 44–52. **11.** *Кобозева А. А., Трифонова Е. А.* Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / Вестник НТУ «ХПИ». – 2007. – № 18. – С.81–93.

Надійшла до редколегії 26.12.2011