УДК 004.056.5
Бобок И.И., Кобозева А.А., Костырка О.В.

РАЗРАБОТКА УСТОЙЧИВОГО СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА, ОБЛАДАЮЩЕГО ВНУТРЕННИМ ПАРАЛЛЕЛИЗМОМ

Введение

Развитие и совершенствование комплексной системы защиты информации сегодня невозможно без наличия в ее составе эффективной стеганографической системы, основывающейся на современных стеганографических алгоритмах [1-4].

Стеганографирование осуществляется различными способами, при этом скрываемое сообщение (конфиденциальная информация (КИ)) после предварительного кодирования, результатом которого является дополнительная информация (ДИ) (как правило – бинарная числовая последовательность [1,2]), встраивается в контейнер, или основное сообщение (ОС), не привлекающий внимание, который затем открыто транспортируется по каналу связи или хранится в таком виде. Наиболее подходящими объектами, используемыми в качестве ОС, являются неподвижные изображения, файлы аудио и видеоданных [1,2]. В настоящей работе контейнером выступает цифровое изображение (ЦИ). Процесс погружения ДИ в ОС далее будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС).

Типичный вид стеганографической системы представлен на рис.1, где штриховой линией выделена составная часть системы, необходимая в случае, если погружаемая ДИ играет роль цифрового водяного знака (ЦВЗ), часто применяемого сегодня для защиты от несанкционированного использования информационного контента [1,2].

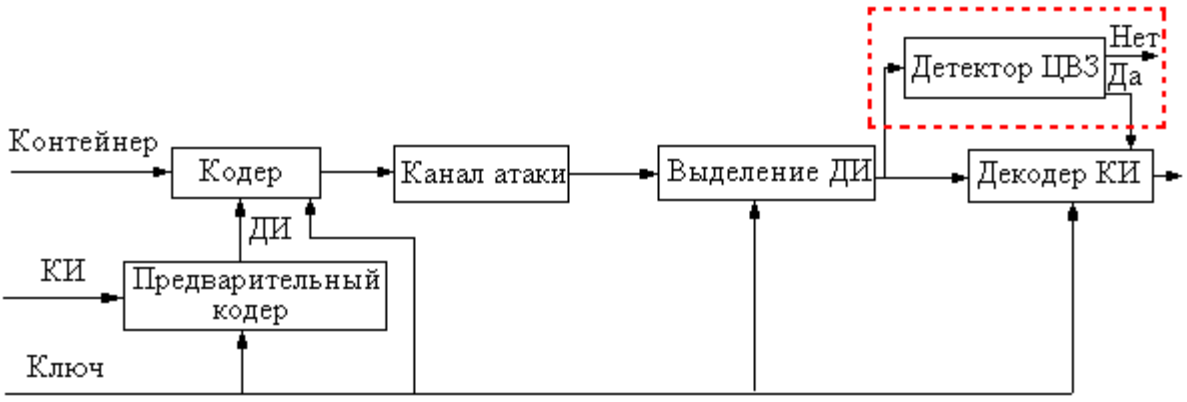


Рис.1. Основные элементы используемой стеганосистемы

В настоящий момент стеганография переживает этап своего бурного развития, связанный с многими объективными и субъективными причинами [1,2,5], среди которых ограничение или даже запрет на использование криптографических методов во многих странах мира, в том числе, в Украине. В силу этого остро встают вопросы совершенствования существующих и разработки новых стеганоалгоритмов, удовлетворяющих определенным требованиям, среди которых одним из основных является требование устойчивости алгоритма к различным возмущающим воздействиям, которые претерпевает стеганосообщение в канале атаки (рис.1).

В свете выводов, сделанных в [4,6,7], можно утверждать, что обеспечение устойчивости стеганоалгоритма не зависит напрямую от того, в какой области контейнера-изображения – пространственной или области преобразования происходит погружение ДИ. А с учетом того, что пространственная область обладает рядом преимуществ при организации СП [8], по сравнению с другими областями ОС, вопрос разработки устойчивых к возмущающим воздействиям стеганометодов и алгоритмов, работающих в пространственной области ЦИ, является своевременным и *актуальным*.

Одним из преимуществ пространственной области изображения для организации СП перед областью преобразования являются меньшие

вычислительные затраты. Однако уменьшения реального времени работы алгоритма принципиально можно достичь также за счет использования для его реализации (при существовании такой возможности у самого алгоритма) многопроцессорных вычислительных систем, которые сегодня широко внедряются в практику решения больших прикладных задач, в том числе, в области стеганографии. Эффективное использование различного типа параллельных вычислительных систем возможно за счет одновременного выполнения ими ветвей вычислений, не связанных между собой информационно. Поэтому целью исследования любого, в том числе, стеганографического последовательного алгоритма является поиск и выделение таких ветвей. Если они найдены, то алгоритму присущ внутренний параллелизм, и его принципиально возможно реализовать на параллельной вычислительной системе, в противном случае его использование в ней нецелесообразно.

Таким образом, *актуальным* сегодня для любого (последовательного) алгоритма, в том числе, стеганографического, является его исследование для установления возможности использования параллельных вычислительных систем при его реализации, получение сведений о параллельных свойствах алгоритма.

Цель работы и постановка заданий

Целью работы является разработка нового стеганометода и реализующего его полиномиального, обладающего внутренним параллелизмом стеганоалгоритма на основе полученных условий обеспечения устойчивости стеганоалгоритма к возмущающим воздействиям при организации стеганопреобразования в пространственной области контейнера-изображения.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1. Формализовать в пространственной области достаточное условие устойчивости стеганоалгоритма, полученное в области преобразования изображения;

2. На основе полученного достаточного условия обеспечения устойчивости к возмущающим воздействиям стеганометода/алгоритма в пространственной области контейнера разработать устойчивый стеганометод;
3. Разработать стеганоалгоритм, реализующий новый стеганометод, осуществляющий СП в пространственной области ЦИ-контейнера, устойчивый к атаке сжатием;
4. Оценить вычислительную сложность разработанного стеганоалгоритма;
5. Исследовать стеганоалгоритм на наличие внутреннего параллелизма.

Теоретические основы стеганографического метода, устойчивого к возмущающим воздействиям

На основе общего подхода к анализу состояния и технологии функционирования информационных систем [4,6], в соответствии с которым состояние любой информационной системы формально определяется характерными особенностями полного набора параметров – сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) соответствующей системе матрицы (матриц), в [9,10] было получено достаточное условие обеспечения устойчивости стеганоалгоритма к возмущающим воздействиям, в частности, к атаке сжатием, в том числе, со значительными коэффициентами. В соответствии с полученным условием для обеспечения устойчивости стеганоалгоритма СП достаточно проводить таким образом, чтобы его формальным представлением была совокупность S возмущений максимальных СНЧ блоков матрицы контейнера, полученных в результате стандартного разбиения.

Практической реализацией упомянутого достаточного условия, рассматривающего область преобразования контейнера (область сингулярного разложения матриц блоков ОС), явились стеганометод и соответствующий ему алгоритм $A1$, представленные в работе [11], где погружение ДИ, представляющей из себя случайно сформированную бинарную последовательность, проводилось

путем возмущения максимальных СНЧ блоков контейнера. Вычислительный эксперимент подтвердил высокую эффективность $A1$ при декодировании ДИ в условиях возмущающих воздействий, направленных на СС.

Для решения задачи 1 из общего перечня задач, приведенного выше, проанализируем в пространственной области ОС результат удовлетворения упомянутому достаточному условию устойчивости стеганографического алгоритма, полученному для области преобразования контейнера.

Пусть B - $l \times l$ – блок матрицы ОС. Для B существует представление вида [12]:

$$B = U\Sigma V^T = (u_1,...,u_l)\begin{pmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma_l \end{pmatrix}(v_1,...,v_l)^T, \quad (1)$$

называемое сингулярным разложением, где U, V - ортогональные $l \times l$ – матрицы, столбцы которых u_i, v_i, $i = \overline{1,l}$, - левые и правые СНВ B соответственно, $\Sigma = diag(\sigma_1,...,\sigma_l)$, $\sigma_1 \geq ... \geq \sigma_l \geq 0$ - СНЧ. Важной характеристикой сингулярного разложения, определяющей приоритетность, целесообразность, удобства его использования в стеганографии, является то, что все СНЧ всегда вещественны и неотрицательны. Необходимо отметить, что разложение (1) определяется неоднозначно за счет неединственности СНВ. Однозначности (1) добиваются за счет дополнительных условий, накладываемых на СНВ, в частности, требования лексикографической положительности левых СНВ. В этом случае (1) называется нормальным сингулярным разложением [4,6].

Пусть результат СП блока B формально выражается возмущением его СНЧ. Тогда для соответствующего блока $\overline{B}$ СС будет иметь место равенство:

$$\overline{B} = U(\Sigma + \Delta\Sigma)V^T, \quad (2)$$

где $\Delta\Sigma = diag(\Delta\sigma_1,...,\Delta\sigma_l)$ - матрица возмущений $\Delta\sigma_i$ СНЧ σ_i, $i = \overline{1,l}$, матрицы B в процессе СП.

Для достаточного условия, упомянутого выше,

$$\Delta\Sigma = diag(\Delta\sigma_1,0,0,...,0). \tag{3}$$

С учетом (3) формула (2) будет иметь вид:

$$\overline{B} = (u_1,...,u_l)\begin{pmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma_l \end{pmatrix}(v_1,...,v_l)^T + (u_1,...,u_l)\begin{pmatrix} \Delta\sigma_1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}(v_1,...,v_l)^T. \tag{4}$$

Исходя из (4), получаем общее формальное представление стеганопреобразования в пространственной области контейнера:

$$\overline{B} = B + \Delta B.$$

где

$$\Delta B = \Delta\sigma_1 u_1 v_1^T \tag{5}$$

- матрица возмущения блока B.

Матрица ΔB (5) имеет единичный ранг, поскольку, исходя из (4), ее инерция [13] равна $(1,0,l-1)$ или $(0,1,l-1)$. Если $u_1 = (u_{11},u_{21},...,u_{l1})^T$, $v_1 = (v_{11},v_{21},...,v_{l1})^T$, то:

$$\Delta B = \begin{pmatrix} \Delta\sigma_1 u_{11}v_{11} & \Delta\sigma_1 u_{11}v_{21} & \dots & \Delta\sigma_1 u_{11}v_{l1} \\ \Delta\sigma_1 u_{21}v_{11} & \Delta\sigma_1 u_{21}v_{21} & \dots & \Delta\sigma_1 u_{21}v_{l1} \\ \dots & \dots & \dots & \dots \\ \Delta\sigma_1 u_{l1}v_{11} & \Delta\sigma_1 u_{l1}v_{21} & \dots & \Delta\sigma_1 u_{l1}v_{l1} \end{pmatrix}. \tag{6}$$

В [14] показано, что СНВ u_1, v_1 блоков матрицы ЦИ, отвечающие максимальным СНЧ, получаемые путем нормального сингулярного разложения соответствующих матриц, в подавляющем большинстве блоков изображения близки к *n*-оптимальному вектору n^O пространства R^l:

$$u_1 \approx n^O,\ v_1 \approx n^O, \tag{7}$$

при этом *n*-оптимальный вектор определяется как [4]:

$$n^O = \left(\frac{1}{\sqrt{l}}, \frac{1}{\sqrt{l}}, \ldots, \frac{1}{\sqrt{l}}\right)^T \in R^l. \tag{8}$$

С учетом (7) и (8) формула (6) приобретает вид:

$$\Delta B \approx \begin{pmatrix} \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \cdots & \frac{\Delta\sigma_1}{l} \\ \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \cdots & \frac{\Delta\sigma_1}{l} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \cdots & \frac{\Delta\sigma_1}{l} \end{pmatrix}. \tag{9}$$

Таким образом, упомянутое выше формальное достаточное условие обеспечения устойчивости стеганоалгоритма к возмущающим воздействиям, полученное первоначально в области преобразования ЦИ (области сингулярного разложения матрицы блока) [9], может быть адаптировано для использования в пространственной области путем требования коррекции в процессе СП яркости всех пикселей блока на одно и то же значение, равное $\Delta b = \frac{\Delta\sigma_1}{l}$. Основной вопрос

здесь при разработке конкретных стеганографических методов и алгоритмов будет заключаться в определении/оценке значения $\Delta\sigma_1$, выборе в соответствии с конкретными требованиями размера блока l: Δb должно обеспечивать устойчивость алгоритма к различным/конкретным возмущающим воздействиям с учетом соблюдения надежности восприятия формируемого СС.

Замечание 1. С учетом особенностей машинной арифметики, а также (7) в большинстве блоков матрицы изображения после возмущения максимальных СНЧ в соответствии с (4) точное равенство в (9) не достигается. В силу этого ключевым моментом при разработке стеганографических алгоритмов, удовлетворяющих полученному достаточному условию, может стать получение порогового значения для отклонения истинного возмущения элементов матрицы яркости блоков от $\frac{\Delta\sigma_1}{l}$.

Разработка стеганографического метода, устойчивого к возмущающим воздействиям

Пусть F, $\overline{F}$ - $m\times m-$матрицы ОС, СС соответственно, $p_1, p_2,..., p_t$ - ДИ, $p_i \in \{0,1\}, i=\overline{1,t}$. Декодированную ДИ будем обозначать: $\overline{p}_1, \overline{p}_2,..., \overline{p}_t$, где $\overline{p}_i \in \{0,1\}, i=\overline{1,t}$.

В [9] показано, что для принципиальной возможности декодирования ДИ из СС, претерпевшего возмущающие воздействия, совокупный результат возмущений блоков ОС при погружении ДИ должен превосходить возмущение, которое будет претерпевать блок СС в процессе возмущающего воздействия в канале атаки (рис.1).

Пусть предполагаемое возмущение блока $\overline{B}$ СС при атаке – это $\Delta\overline{B}$, тогда в соответствии с соотношением [12]:

$$\max_{1\le j\le l}\left|\sigma_j(\overline{B})-\sigma_j(\overline{B}+\Delta\overline{B})\right|\le\left\|\Delta\overline{B}\right\|_2,$$

где $\sigma_j(\overline{B})$, $\sigma_j(\overline{B}+\Delta\overline{B})$ - СНЧ матриц $\overline{B}$ и $\Delta\overline{B}$ соответственно, $\left\|\Delta\overline{B}\right\|_2$ - спектральная матричная норма $\Delta\overline{B}$, возмущение СНЧ σ_1 блока B при стеганопреобразовании, организуемом в области сингулярного разложения, должно быть больше, чем $\left\|\Delta\overline{B}\right\|_2$, а тогда возмущение Δb значений яркости пикселей блока B ОС при погружении ДИ в пространственной области должны удовлетворять соотношению:

$$|\Delta b| = \left|\frac{\Delta\sigma_1}{l}\right| > \frac{\left\|\Delta\overline{B}\right\|_2}{l}. \qquad (10)$$

Предположим, что оценка $\left\|\Delta\overline{B}\right\|_2$ результата предполагаемого возмущающего воздействия на блок СС известна. Основные шаги предлагаемого стеганометода следующие.

Погружение ДИ.

1. Матрица F ОС разбивается на $l\times l-$блоки. Каждый блок контейнера используется для погружения $k+1$ $(k\geq 0)$ бит ДИ.

2. (*Погружение ДИ в очередной блок контейнера*). Пусть B — очередной блок, используемый для стеганопреобразования, а $p_i,...,p_{i+k}$ — очередные биты ДИ. Погружение дополнительной информации производится за счет возмущения значений яркости пикселей блока B на Δb, удовлетворяющего (10). Количество различных вариантов корректировки яркости определяется количеством различных вариантов упорядоченных бинарных последовательностей $p_i,...,p_{i+k}$: 2^{k+1}. Результат – блок $\overline{B}$ СС $\overline{F}$.

В результате пересылки и/или хранения СС может подвергаться различным возмущающим воздействиям, после которых его матрица, в общем случае, будет отлична от $\overline{F}$ и далее обозначается $\overline{\overline{F}}$.

Декодирование ДИ

1. Матрицы F контейнера и $\overline{\overline{F}}$ возможно возмущенного СС разбиваются на $l \times l$ – блоки. Каждый блок СС используется для извлечения $k+1$ ($k \geq 0$) бит ДИ.

2. Пусть $\overline{\overline{B}}$ — очередной блок СС, из которого извлекаются биты $\overline{p}_i, ..., \overline{p}_{i+k}$ ДИ, а B - соответствующий ему блок ОС.

2.1. Определить:

$$\Delta B = \overline{\overline{B}} - B.$$

2.2. Определить по матрице ΔB значение Δb, в соответствии с которым целиком декодировать бинарная последовательность $\overline{p}_i, ..., \overline{p}_{i+k}$.

Конкретный способ реализации шагов 2 при погружении и декодировании ДИ будет определять конкретный стеганоалгоритм, один из вариантов которого предлагается ниже.

Разработка стеганографического алгоритма

Для разработанного выше стеганометода предлагается одна из возможных реализаций, где возмущающее воздействие конкретизируется атакой сжатием на стеганосообщение.

В [9] экспериментально получены оценки $\left\| \Delta \overline{B} \right\|_2 \leq 72$ для случая, когда $l = 8$, а атака происходит путем пересохранения СС в формат Jpeg с различными коэффициентами качества $QF \geq 60$.

С учетом (10) положим: $\Delta b = 10$; а $l = 8$. Предлагается алгоритм, реализующий разработанный выше метод, устойчивый к сжатию при $QF \geq 60$, имеющий скрытую пропускную способность $1/64$ бит/пиксель ($k = 0$), количество различных вариантов корректировки значений яркости пикселей блока B равно: $2^{k+1} = 2$.

Основные шаги алгоритма выглядят следующим образом.

Погружение ДИ.

1. Матрица F ЦИ-контейнера разбивается на 8×8 – блоки.

2. (*Погружение ДИ – реализация двух различных вариантов корректировки значений яркости пикселей блока* B). Пусть B — очередной блок ОС, используемый для СП, а p_i — очередной бит ДИ, $\overline{B}$ - соответствующий блок стеганосообщения.

Если

$$p_i = 1$$

то

$$\overline{B} = B + \Delta b \cdot \overline{E}$$

иначе

$$\overline{B} = B - \Delta b \cdot \overline{E}$$

где $\overline{E}$ - $8 \times 8-$матрица, все элементы которой равны 1.

Декодирование ДИ

1. Матрицы F контейнера и $\overline{\overline{F}}$ возможно возмущенного СС разбиваются на $8 \times 8-$блоки. Каждый блок СС используется для извлечения 1 бита ДИ.

2. Пусть $\overline{\overline{B}}$ — очередной блок СС, из которого извлекается бит $\overline{p}_i$ ДИ, а B - соответствующий ему блок ОС.

2.1. Определить:

$$\Delta B = \overline{\overline{B}} - B.$$

2.2. Определить количества положительных k_p и отрицательных k_n элементов в матрице ΔB.

если

$$k_p > k_n,$$

то

$$\overline{p}_i = 1,$$

иначе

$$\overline{p}_i = 0\,.$$

Замечание 2. Реализация процессов СП и декодирования в предложенном стеганоалгоритме происходит в предположении, что формальным представлением ЦИ-контейнера является одна матрица. Это никак не ограничивает область применимости разработанного алгоритма: если в качестве ОС используется цветное изображение, то алгоритм, во-первых, может применяться для погружения ДИ лишь в одну из множества матриц, используемых для представления ЦИ; во-вторых, он может использоваться для каждой из матриц.

Замечание 3. При разработке стеганоалгоритма реализация двух различных вариантов корректировки значений яркости пикселей блока B при СП может быть реализована путем только увеличения/уменьшения значений яркости. В этом случае для организации эффективного декодирования ДИ значения Δb_1 и Δb_2 - двух вариантов корректировки должны удовлетворять соотношениям:

$$\begin{cases} |\Delta b_1| \geq |\Delta b|, \\ |\Delta b_1 - \Delta b_2| \geq |\Delta b| \end{cases},$$

где Δb определяется (10).

Замечание 4. Вычислительная сложность разработанного стеганоалгоритма определяется количеством блоков, на которые разбивается $m \times m$ – матрица контейнера/стеганосообщения, и составляет

$$\left[\frac{m}{8}\right]\left[\frac{m}{8}\right] = \underline{O}\left(m^2\right) \qquad (11)$$

операций, где $[\bullet]$ - операция округления аргумента до целого значения.

При тестировании работы предложенного выше алгоритма было установлено, что результаты декодирования ДИ в условиях атаки сжатием с коэффициентами качества $QF \geq 60$, направленной на СС, сравнимы с результатами работы алгоритма $A1$ [11,15], что находится в полном соответствии с разработанным при его создании теоретическим подходом.

Для проверки соблюдения надежности восприятия СС, формируемого предложенным выше стеганоалгоритмом, в среде MatLab был проведен вычислительный эксперимент, в котором было задействовано 300 ЦИ из базы NRCS [16], являющейся традиционной при тестировании алгоритмов, работающих с ЦИ.

Традиционным при оценке искажений ЦИ при различных возмущениях является оценка $PSNR$ (пиковое отношение «сигнал-шум»), получаемая в децибелах (dB) [17]:

$$PSNR = 10 \cdot \log_{10}\left(\frac{255^2}{\frac{1}{m^2}\sum_{i,j}\left(F(i,j) - (F+\Delta F)(i,j)\right)^2} \right), \qquad (12)$$

где $F(i,j), (F+\Delta F)(i,j),\ i,j = \overline{1,m}$, — значения яркости пикселей исходного изображения с матрицей F и возмущенного с матрицей $F+\Delta F$ соответственно. Однако оценка (12) визуального искажения ЦИ в общем случае не является пригодной для оценки надежности восприятия СС в стеганографии, которая носит субъективный характер [17,18]. Поскольку основной задачей любого стеганоалгоритма является сохранение в секрете наличия тайного канала передачи информации, достигаемое, в том числе, и за счет обеспечения надежности восприятия стегосообщения, в систему стеганографической передачи данных включается человек, что вносит дополнительные, непреодоленные до настоящего момента трудности в процесс математической формализации обеспечения

рассматриваемого требования, хотя работа в этом направлении ведется очень активно, с привлечением обширного математического аппарата [18,19]. В силу этого степень обеспечения надежности восприятия СС в работе оценивается двумя способами: путем субъективного ранжирования; при помощи $PSNR$.

Субъективным ранжированием было установлено соблюдение надежности восприятия СС, сформированных разработанным алгоритмом для 97% ЦИ, подвергнутых тестированию (в качестве ДИ использовалась случайно сформированная бинарная последовательность). Типичные результаты приведены на рис.2, где погружение ДИ проводилось в синюю матрицу цветного ЦИ (формат RGB). Для тестируемых ЦИ $PSNR \approx 35\,dB$, что рассматривается в литературных источниках как значение, характеризующее приемлемое качество ЦИ.

а б

Рис.2. Результат стеганопреобразования изображения разработанным алгоритмом: контейнер (а); стеганосообщение (б)

Таким образом, разработанный стеганографический алгоритм, осуществляя погружение ДИ в пространственной области контейнера, удовлетворяет выдвинутым к нему требованиям: он является устойчивым, обеспечивает

надежность восприятия формируемого стеганосообщения, является полиномиальным степени 2 (см. (11)).

Анализ внутреннего параллелизма разработанного стеганографического алгоритма

Одной из возможных форм записи алгоритмов, удобной для анализа на наличие у них внутреннего параллелизма, является их представление в виде графов, в частности, графов информационной зависимости реализации алгоритма [20,21], которые ниже для удобства называются графами алгоритмов.

Множеству операций алгоритма, реально выполняемых при заданных входных данных, ставится во взаимно однозначное соответствие множество вершин графа. Если аргумент одной операции является результатом выполнения другой операции, то соответствующие вершины образуют ребро, направленное из той вершины, откуда берется результат. Необходимо отметить, что в целях уменьшения размеров графа алгоритма, упрощения процедуры его анализа часто вершина графа отвечает не одной, а множеству выполняемых операций алгоритма, называясь при этом макровершиной.

Граф алгоритма $G(V,E)$, где V — множество вершин графа, а E — множество его ребер, определяет все множество возможных реализаций алгоритма, показывая, как при этих реализациях происходит распространение информации.

Реализация алгоритма порождает определенное разбиение его операций на группы, которые выполняются последовательно, а операции внутри каждой группы могут выполняться параллельно (одновременно). Разбиение операций алгоритма порождает соответствующее разбиение вершин графа алгоритма (называемое топологической сортировкой, или параллельной формой) и наоборот.

Для анализа внутреннего параллелизма разработанного стеганографического алгоритма построим его граф. Следуя логике работы алгоритма, а также для удобства исследования рассмотрим отдельно графы, отвечающие логическим составным частям алгоритма: процессу погружения ДИ и ее декодирования. Самые общие виды таких графов – макрографы [20,21] представлены на рис.3, где макровершины, являющиеся результатами гомоморфных сверток [20] подграфов, отвечающих операциям обработки отдельных блоков $B_1, B_2, ..., B_n$ при СП и $\overline{=}{B}_1, \overline{=}{B}_2, ..., \overline{=}{B}_n$ при извлечении ДИ из возможно возмущенного СС, где $n = \left[\frac{m}{8}\right]\left[\frac{m}{8}\right]$, принадлежат одному ярусу топологической сортировки [20,21] (на рис.3 эти ярусы выделены штриховой линией), т.е. являются информационно независимыми, а значит могут выполняться одновременно, или параллельно. Таким образом, уже на этапе анализа макрографов можно утверждать, что разработанный стеганоалгоритм обладает внутренним параллелизмом как в части СП, так и в части декодирования ДИ. Однако, поскольку в общем случае топологическая сортировка макрографа (являющегося результатом гомоморфной свертки графа алгоритма) порождает лишь обобщенную топологическую сортировку [20,21] исходного графа алгоритма, рассмотрим подграфы исходного графа, отвечающие макровершинам макрографа, подробно с целью выявления внутреннего параллелизма и в этих частях алгоритма.

Поскольку как этап погружения, так и этап извлечения ДИ содержит условные операторы, то разработанному стеганоалгоритму будет отвечать семейство «похожих» графов [20,21]. Для каждого отдельно взятого блока $B_i, i = \overline{1,n}$, с элементами $b_{kp}{}^{(i)}, k, p = \overline{1,8}$, при погружении ДИ (результат – блок $\overline{B}_i, i = \overline{1,n}$, с элементами $\bar{b}_{kp}{}^{(i)}, k, p = \overline{1,8}$) это семейство состоит из двух графов – подграфов графа алгоритма (рис.4(а,б)). В этом случае вместо того, чтобы отдельно исследовать топологические сортировки каждого из графов семейства, анализируется топологическая сортировка их объединения (рис.4(в)), поскольку

любая топологическая сортировка графа-объединения порождает топологическую сортировку каждого графа семейства [20].

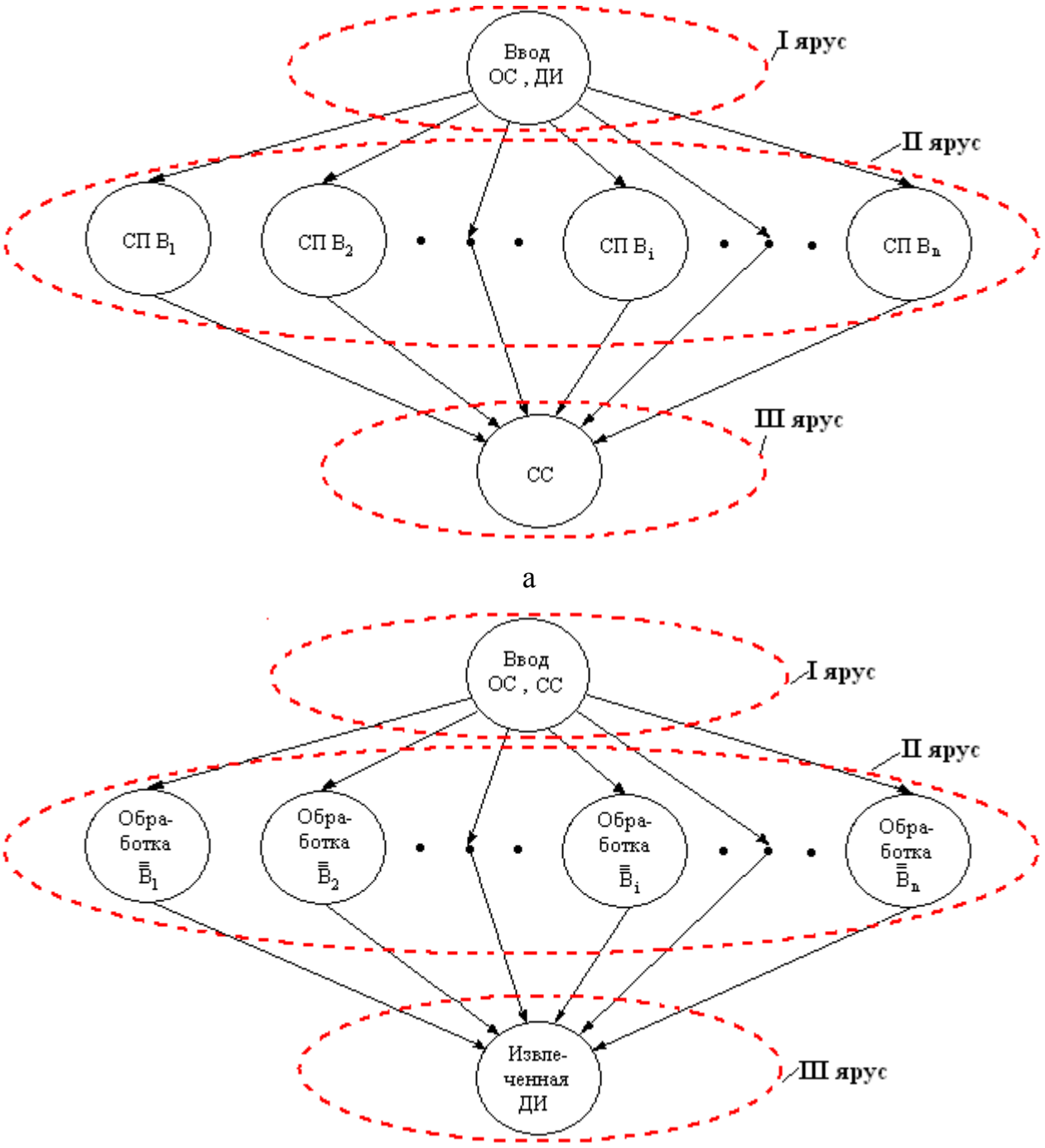
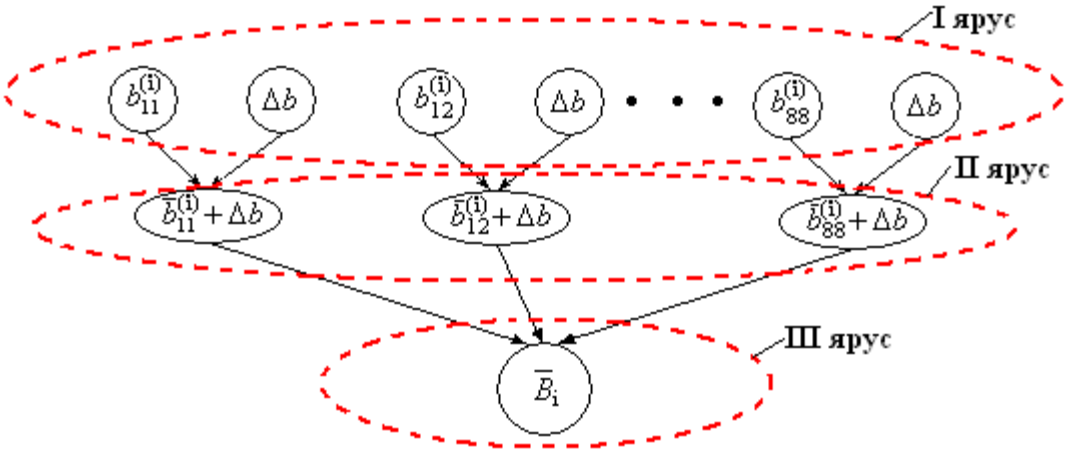
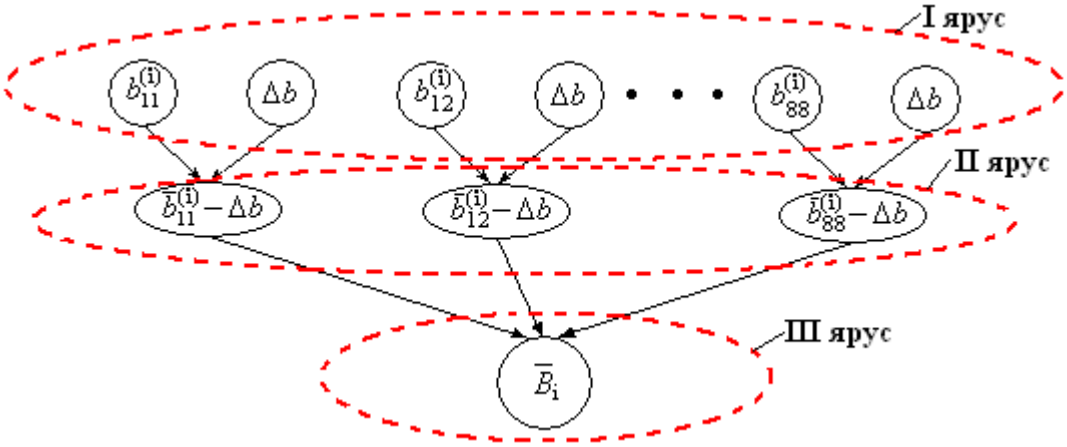


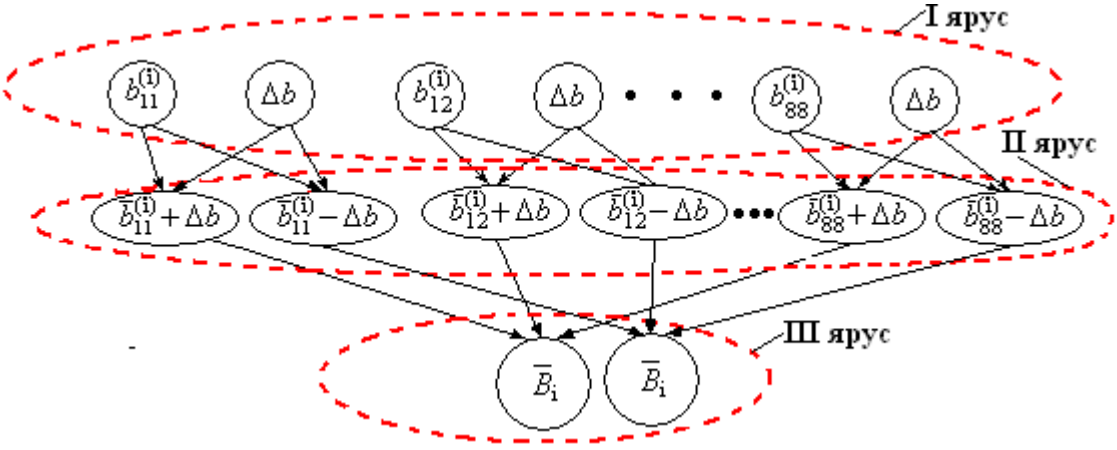
Рис.3. Параллельная форма макрографов составных частей разработанного стеганоалгоритма: а – процесс СП; б – процесс извлечения ДИ из СС



а



б



в

Рис.4. Параллельные формы пографов, отвечающих СП блока $B_i, i=\overline{1,n}$: а,б – графов, составляющих семейство «похожих» графов; в – графа-объединения семейства «похожих» графов

Такой способ анализа алгоритма является предпочтительным, поскольку для конкретных входных данных можно даже не знать, с каким конкретно графом из семейства «похожих» графов придется иметь дело.

При декодировании ДИ для определения количества положительных и отрицательных элементов в матрице ΔB при стандартной организации процесса накопления сумм k_p и k_n будет использовано в общем случае 64 условных оператора (по количеству элементов в $8\times8-$блоке), что уже на этой стадии построения той части графа алгоритма, которая отвечает за обработку 1 блока матрицы СС, приведет к семейству из 2^{64} «похожих» графов. Для получения топологической сортировки каждого из них имеет смысл сразу рассмотреть объединение семейства (рис.5).

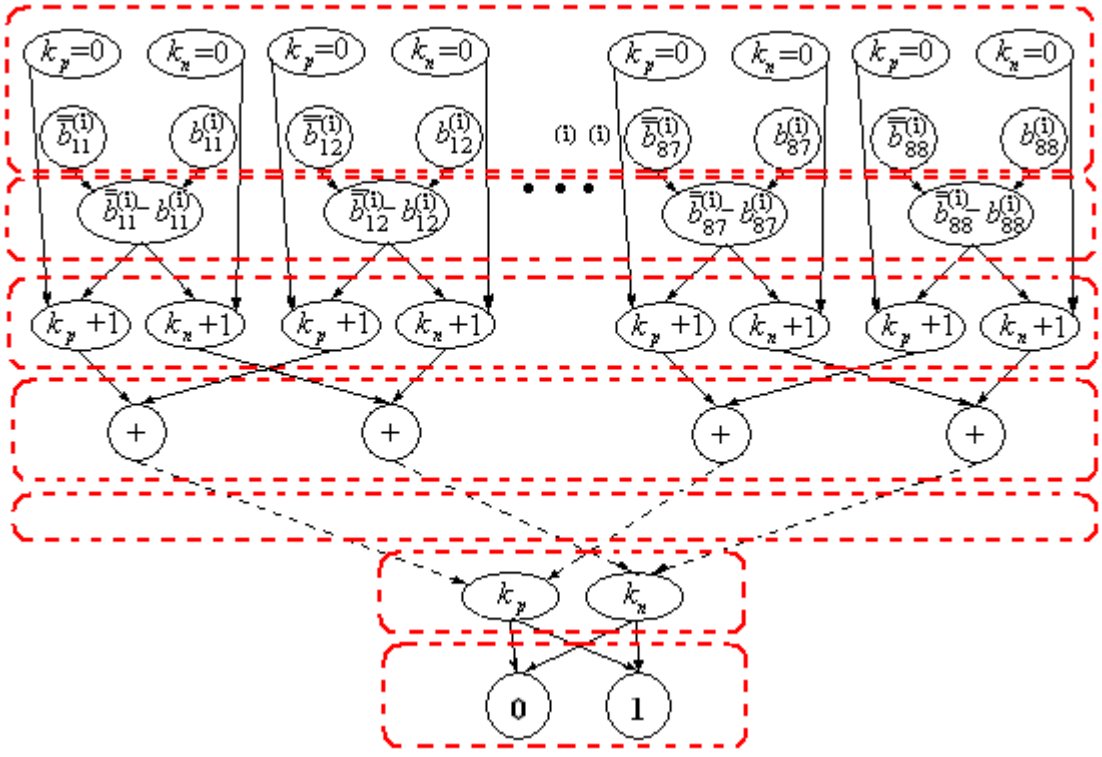


Рис.5. Топологическая сортировка объединения «похожих» подграфов, отвечающих процессу декодирования ДИ из одного блока $\overline{\overline{B}}_i$ возможно возмущенного СС

Таким образом, анализ подграфов графа разработанного стеганоалгоритма, отвечающих обработке отдельных блоков матрицы контейнера/стеганосообщения, осуществляемой при погружении/декодировании ДИ, выявил наличие внутреннего параллелизма и в этих частях алгоритма.

Заключение

На основании достаточного условия устойчивости стеганоалгоритма к возмущающим воздействиям, работающего в области сингулярного разложения матрицы контейнера, получено условие обеспечения такой устойчивости при организации стеганопреобразования в пространственной области контейнера-изображения: для решения поставленной задачи стеганопреобразование достаточно проводить путем корректировки яркости пикселей блоков матрицы контейнера на одно конкретно выбранное значение Δb. Конкретные значения величины Δb (с учетом необходимости соблюдения надежности восприятия стеганосообщение) позволят обеспечить устойчивость соответствующих стеганоалгоритмов к различным возмущающим воздействиям.

На основе полученного формального достаточного условия разработан новый стеганометод и реализующий его полиномиальный (степени 2) стеганоалгоритм, устойчивый к атаке сжатием, организующий стеганопреобразование в пространственной области контейнера-изображения.

Установлено, что разработанный стеганографический алгоритм обладает внутренним параллелизмом, что дает принципиальную возможность для значительного уменьшения временных затрат на его работу при реализации этого алгоритма в многопроцессорной вычислительной системе.

Литература

1. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
3. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008 — . — Т.2: Информационная безопасность. — 2008. — 344 с.
4. Кобозєва, А.А. Аналіз захищеності інформаційних систем [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напр. «Інформаційна безпека» та «Системні науки та кібернетика» / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко ; М-во трансп. та зв'язку України, Держ. ун-т інформ.-комунікац. технологій. — К. : ДУІКТ, 2010. — 316 с.
5. Бобок, И.И. Детектирование наличия возмущений матрицы цифрового изображения как составная часть стеганоанализа / И.И. Бобок // Вісник Східноукр-го нац-го ун-ту ім. В. Даля. — 2011. — №7(161). – С. 32–41.
6. Кобозєва, А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснований на теорії збурень / А.А. Кобозєва // Інформаційні технології та комп'ютерна інженерія. — 2008. — № 1(11). — С. 164–171.
7. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. — 2007. — № 4. — С. 531–538.
8. Костырка О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В.Костырка // Інформатика та математичні методи в моделюванні. – 2013. – Т.3, №3. – С.220-227.

9. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию / А.А. Кобозева, М.А. Мельник // Сучасна спеціальна техніка. — 2012. — № 4(31). — С. 60–69.
10. Кобозева, А.А. Методика оценки основных параметров произвольного стеганоалгоритма / А.А. Кобозева, М.А. Мельник // Збірник матеріалів V Міжнародної науково-практичної конференції «Проблеми і перспективи розвитку ІТ-індустрії». Харків, 25–26 квітня 2013. — Харків : ХНЕУ, 2013. — Вип. 3(110), Том 2. — С. 201.
11. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. — 2012. — № 2(8). — С. 99–106.
12. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
13. Бахвалов, Н.С. Численные методы [Текст] : учебное пособие для студ. физико-математических спец. вузов; Рекомендовано МО РФ / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — 6-е изд. — М. : БИНОМ. Лаборатория знаний, 2008. — 636 с.
14. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А. Кобозева, М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2012. — Вип. 38. — С. 193–203.
15. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию и их реализация в новом стеганоалгоритме *[Електронний ресурс]* / А.А. Кобозева, М.А. Мельник // Проблемы региональной энергетики. — Кишинеу, 2013. — № 1(21). — С. 93–102. — Режим доступу: http://ieasm.webart.md/data/m71_2_237.pdf
16. NRCS Photo Gallery: *[Електронний ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).

17. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
18. Кобозева, А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник НТУ «ХПИ». — 2007. — № 18. — С. 81–93.
19. Winkler, S. A perceptual distortion metric for digital color images / S. Winkler // Proceedings of the 5th IEEE International Conference on Image Processing (ICIP'98), October 1998, Chicago, USA. — 1998. — Vol. 3. — PP. 399–403.
20. Воеводин В.В. Математические основы параллельных вычислений. – М.: Изд-во Моск. ун-та, 1991. –345 с.
21. Воеводин В.В. Параллельные вычисления. Воеводин В.В., Воеводин Вл. В. – СПб.: БХВ-Петербург, 2002. –608 с.

Авторы:

Кобозева Алла Анатольевна – д.т.н., проф., зав.каф.информатики и управления защитой информационных систем Одесского национального политехнического университета

Бобок Иван Игоревич – к.т.н., ст.преп. каф.информатики и управления защитой информационных систем Одесского национального политехнического университета

Костырка Олеся Викторовна – аспирант Академии пожарной безопасности им.Героев Чернобыля