УДК 004.056.5

И. И. БОБОК, аспирант ОНПУ, Одесса

СТЕГАНОАНАЛИТИЧЕСКИЙ АЛГОРИТМ ДЛЯ ОСНОВНОГО СООБЩЕНИЯ, ХРАНИМОГО В ФОРМАТАХ С ПОТЕРЯМИ

Пропонується новий стеганографічний алгоритм для аналізу стеганоповідомлень, сформованих на основі контейнера, що зберігається у форматі з втратами з використанням методу модифікації найменшого біту, що є значущим.

Предлагается новый стеганоаналитический алгоритм для анализа стеганосообщений, сформированных на основе контейнера, хранимого в формате с потерями, с использованием метода модификации наименьшего значащего бита

Proposed a new steganalysis algorithm for the analysis of stegano-messages formed on the basis of the container, stored in lossy format, using the method of modifying the least significant bit

Введение. Защита информации сегодня является одним из самых важных вопросов, решаемых обществом. Комплексный системный подход к проблеме информационной безопасности предполагает создание системы защиты, необходимым звеном которой является цифровая стеганография [1].

Активизация в настоящий момент научной деятельности в области стеганографии, отчасти связанная с ограничением использования шифрования во многих странах мира, усилила актуальность вопросов, связанных с повышением эффективности стеганоанализа (СА) [2].

При всем многообразии имеющихся стеганоаналитических методов [3–6] общего подхода к проблеме СА (в смысле детектирования произведенного внедрения секретной информации или вывода об отсутствии такого внедрения) до настоящего момента не существовало.

Совсем недавно в [7, 8] был предложен принципиально новый математический подход к решению проблемы СА (МПСА), основанный на общем подходе к анализу состояния и технологии функционирования информационных систем (ОПАИС) [9], основными математическими инструментами которого являются матричный анализ и теория возмущений. Настоящая статья является очередным шагом автора на пути разработки универсального стеганоаналитического метода (на основе МПСА).

В стеганографии организация секретного канала связи осуществляется внутри открытого канала [2]: в некоторый информационный контент – контейнер, или основное сообщение (ОС), осуществляется внедрение секретной, или дополнительной, информации (ДИ) так, чтобы результат этого внедрения – стеганосообщение (СС) был зрительно (на слух) неотличим от ОС. Процесс погружения ДИ будем называть стеганопреобразованием (СП).

В настоящее время хранение и передача подавляющего большинства цифровых сигналов, в частности, цифровых изображений (ЦИ) по каналам

телекоммуникаций осуществляется в сжатом состоянии. Учитывая этот факт, в качестве контейнера будет рассматриваться цифровой сигнал, для определенности – ЦИ, хранящийся в каком-либо из форматов с потерями (КсП – контейнер с потерями).

При организации секретного канала связи на сегодняшний день очень широко используется метод модификации наименьшего значащего бита (LSB), хотя его недостатки хорошо известны [2]. Однако, кроме популярности в силу обеспечения надежности восприятия сформированного СС, простоты реализации и значительной скрытой пропускной способности [2], LSB-метод обладает очень важным в условиях решаемой автором задачи свойством: СП вызывает здесь очень незначительные возмущения контейнера. Разрабатывая СА метод для выявления результаты такого «слабого» СП, можно надеяться на его эффективную работу по выявлению результатов СП другими стеганографическими алгоритмами. Все это явилось побуждающими факторами для автора, в первую очередь, рассмотреть характерные особенности и найти способы выявления последствий работы LSB-метода.

Целью настоящей работы является разработка нового СА алгоритма для анализа СС (ОС), сформированных на основе КсП с использованием LSB-метода.

Метод модификации наименьшего значащего бита является неустойчивым к любого рода возмущающим воздействия, в частности, к операции сжатия [2]. Поэтому СС, сформированное LSB-методом на основе КсП, может быть сохранено только в формате без потерь (ФБП) (например, TIF, BMP). С учетом этого для достижения поставленной цели необходимо решить следующие задачи:

1. Выделить математические объекты, характеризующие ОС, СС, анализ которых позволит отделить ЦИ, подвергшееся операции СП, от ЦИ, не претерпевшего СП;
2. Выявить характерные признаки (качественные, количественные) для выделенных математических объектов, которые позволят отличить сжатое ЦИ, пересохраненное в ФБП, от ЦИ, которое первоначально хранится в ФБП;
3. Выявить характерные признаки для выделенных математических объектов, которые позволят отличить сформированное LSB-методом на основе КсП и сохраненное в ФБП СС от ЦИ, которое хранилось первоначально в формате с потерями (ФСП) и, не подвергаясь процессу СП, было пересохранено в ФБП;
4. На основе результатов решения задач 2 и 3, необходимо выявить характерные признаки (качественные, количественные) для выделенных математических объектов, которые позволят отличить сформированное LSB-методом на основе КсП и сохраненное в ФБП СС от ЦИ, которое первоначально хранится в ФБП.

Основная часть. Общая схема сжатия (с потерями) для ЦИ, которая использована в наиболее распространенных на сегодня стандартах, в частности, JPEG, состоит из трех основных шагов: отображение в частотную область после предварительного стандартного разбиения матрицы изображения на 8×8-блоки, квантование полученных частотных коэффициентов, энтропийное кодирование. Восстановление включает в себя шаги, обратные к перечисленным выше, в обратном порядке [10].

Независимо от конкретики непосредственной реализации сжатия отметим, что в силу специфики человеческого зрения сжатие происходит таким образом, что его результат приводит к исключению из сигнала его высокочастотных (а возможно, и среднечастотных) составляющих за счет обнуления соответствующих коэффициентов. В силу этого матрицы одного ЦИ в ФБП и в ФСП (обозначим эти матрицы F_T и F_J соответственно) различны. Кроме того, матрица изображения, сохраненного в ФБП первоначально и сохраненного в ФБП после сжатия (обозначим последнюю $F_{J\to T}$) качественно отличаются друг от друга по своим характеристикам, в частности, они кардинально по-разному реагируют на пересохранение ЦИ в ФСП. Действительно, F_T отвечает представлению сигнала, у которого все частотные коэффициенты в «первозданном» невозмущенном виде, в то время, как $F_{J\to T}$ соответствует представлению сигнала, у которого уже «отсутствуют» высокочастотные (возможно, среднечастотные) составляющие – коэффициенты при них если ненулевые, то малые (сравнимы с погрешностями округлений). Сжатие для F_T – первое (матрицу результата обозначим $F_{T\to J}$), свойства $F_{T\to J}$ аналогичны F_J. С учетом того, что сжатие происходит с достаточно высоким качеством (такое предположение делается в силу требования сохранения надежности восприятия СС), ожидаемым результатом является незначительное возмущение значений яркости большинства пикселей изображения. Для $F_{J\to T}$ очередное сжатие является вторым (матрицу результата обозначим $F_{J\to T\to J}$), причем его характеристики с большой вероятностью не будут совпадать с характеристиками первого сжатия, в силу чего результат возмущений значений яркости пикселей $F_{J\to T}$ при переходе к $F_{J\to T\to J}$ в общем случае принципиально предсказать невозможно. Ясно лишь, что эти возмущения должны быть значительнее, чем при переходе от F_T к $F_{T\to J}$.

Обозначим: $R = abs\left(F_T - F_{T\to J}\right)$ ($\overline{R} = abs\left(F_{J\to T} - F_{J\to T\to J}\right)$) — матрицу абсолютных значений разностей элементов F_T и $F_{T\to J}$ ($F_{J\to T}$ и $F_{J\to T\to J}$). Пусть $M(A)$ – значение, которое встречается среди элементов произвольной матрицы A с максимальной частотой, $\max(A)$ – максимальное значение среди эле-

ментов матрицы A. На основании проведенных рассуждений можно предположить, что $\max(R) < \max(\overline{R})$; $M(R) < M(\overline{R})$.

Для практической проверки выдвинутого предположения в среде Matlab был проведен вычислительный эксперимент, в котором участвовало около 800 ЦИ размером 1024×1024 пикселей. С учетом поставленных задач в качестве предмета исследования были выбраны гистограммы значений матриц R, $\overline{R}$.

Не ограничивая общности рассуждений, для определенности при проведении вычислительных экспериментов на этой стадии в качестве ФБП использовался TIF, а как ФСП – JPEG, основанный на дискретном косинусном преобразовании (хотя в силу вышесказанного мог быть использован любой другой ФСП, что будет подробно рассмотрено ниже).

На первом этапе эксперимента устанавливались характерные особенности возмущений элементов матрицы изображения при переходе от F_T к $F_{T \to J}$. В результате вычислительного эксперимента было получено, что для различных ЦИ

$$\max(R) \in \{7,8,9,\ldots,32\}, \tag{1}$$

$$M(R) \le 1. \tag{2}$$

Во второй части вычислительного эксперимента устанавливались характерные особенности возмущений элементов матрицы изображения при переходе от $F_{J \to T}$ к $F_{J \to T \to J}$. В результате вычислительного эксперимента было установлено, что

$$\max(\overline{R}) \in \{36,37,\ldots,47\} \tag{3}$$

для разных ЦИ. Для всех протестированных ЦИ $M(\overline{R}) > 1$, что соответствует выдвинутому предположению и, с учетом соотношений (1) и (2) позволяет различить ЦИ, первоначально сохраненные в ФБП, и ЦИ, пересохраненные в ФБП после сжатия.

Пусть КсП подвергается СП методом наименьшего значащего бита, при этом стеганопуть [2] формируется случайным образом. Результат работы LSB-метода в соответствии с [11] в матричном виде будем представлять как возмущение ΔF матрицы контейнера F_J, т.е.

$$\overline{F}_J = F_J + \Delta F, \tag{4}$$

где $\overline{F}_J$ – матрица СС, при этом матрица возмущения ΔF имеет элементы, значения которых принадлежат множеству $\{-1,0,1\}$. При погружении ДИ в

дальнейшем будем учитывать лишь те ее биты, которые вызывают возмущение соответствующих пикселей ОС. Так, будем говорить, что объем погруженной информации (ОПИ) составляет, например, 10%, если при погружении этой ДИ десятая часть общего числа пикселей контейнера претерпела возмущения. СС сохраняется в ФБП (результирующая матрица – $\overline{F}_{J\to T}$). Как показал проведенный вычислительный эксперимент, в котором ОПИ изменялся от 10% до 50% с шагом 10%, полученные СС $\overline{F}_{J\to T}$ ведут себя аналогично $F_{J\to T}$: после последующего пересохранения СС в ФСП (результирующую матрицу обозначим $\overline{F}_{J\to T\to J}$), гистограммы значений элементов матриц $\overline{\overline{R}} = abs\left(\overline{F}_{J\to T} - \overline{F}_{J\to T\to J}\right)$ качественно практически не отличаются от гистограмм матриц $\overline{R}$, а также между собой, несмотря на различие в ОПИ. Теоретически такой результат был ожидаемым: возмущение матрицы ОС F_J за счет СП, которое изменит значения яркости определенной части пикселей лишь на 1, является незначительным. В представлении сигнала ОС F_J коэффициенты при высоких (и возможно некоторых средних) частотах 8×8-блоков матрицы были малы (сравнимы с нулем), что, учитывая связь между частотным спектром произвольной матрицы и ее сингулярными тройками [12], приводит к сравнимости с нулем наименьших сингулярных чисел блоков матрицы. СНЧ произвольной матрицы являются нечувствительными к возмущающим воздействиям, или хорошо обусловленными [9], что приведет к их незначительному возмущению при СП, т.е. оставит их значения сравнимыми с нулем, что, в свою очередь, оставит сравнимыми с нулем коэффициенты при высоких (и возможно некоторых средних) частотах блоков матрицы $\overline{F}_J$, а значит и $\overline{F}_{J\to T}$. Потому при пересохранении в ФСП $\overline{F}_{J\to T}$ качественно ведет себя практически также, как ЦИ, представлением которого является матрица $F_{J\to T}$.

В соответствии с ОПАИС о состоянии и изменении состояния КсП в связи с его СП можно судить по характерным свойствам сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) соответствующей матрицы ЦИ. В связи с тем, что реакция СНВ на возмущающие воздействия различна, а в некоторых случаях – непредсказуема [9], анализ состояния контейнера (или СС) целесообразности свести к анализу только СНЧ.

Рассмотрим более подробно процесс восстановлении ЦИ после сжатия (с потерями). Последний шаг восстановления возвращает ЦИ из частотной в пространственную область. При этом коэффициенты получаемой матрицы будут иметь вещественные значения, которые могут выходить за границы множества $[0,255]$. Результат восстановления на этой стадии назовем частичным (ЧВ). Окончательное, или полное, восстановление (ПВ) ЦИ будет полу-

чено после округления значений яркости до целых и введения их в границы 0...255.

Квантование коэффициентов является необратимой процедурой и приводит к некоторым закономерным особенностям СНЧ 8×8-блоков, полученных после предварительного стандартного разбиения матрицы ЦИ. Везде ниже полагаем, что СНЧ упорядочены по убыванию, т.е. $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_8 \geq 0$. Для $n\times m$-матрицы F назовем матрицей нулевых СНЧ блоков (МНСЧБ) $\left[\frac{n}{8}\right]\times\left[\frac{m}{8}\right]$-матрицу (где $[\bullet]$ – целая часть аргумента), каждый элемент которой равен количеству нулей в сингулярном спектре одноименного блока F. Для ЦИ, хранимого в ФБП, в среднем более 97% элементов МНСЧБ равны 0 [11], при ЧВ квантованного ЦИ у соответствующей МНСЧБ в среднем менее 5% являются нулевыми [11]. При ПВ подавляющее большинство нулевых СНЧ блоков матрицы частично восстановленного ЦИ станут ненулями, что сделает МНСЧБ для ПВ ЦИ подобной МНСЧБ ЦИ, хранимого в ФБП, но значения этих наименьших СНЧ первого будут сравнимы с погрешностью округления и друг с другом, что не характерно для блоков ЦИ, хранимого в ФБП [11]. Кроме того, характер поведения наименьших СНЧ ПВ изображений (бывших нулями при ЧВ) качественно отличается от характера СНЧ с теми же номерами для блоков изображений, хранимых без потерь: скорость их изменения значительно меньше. Это дает возможность предвидеть качественные изменения свойств СНЧ КсП в ходе СП: с увеличением ОПИ характер поведения СНЧ блоков СС, должен все больше «напоминать» характер СНЧ для ЦИ, хранимого в ФБП, в частности, ожидаемым является увеличение скорости изменения наименьших СНЧ с ростом ОПИ, что подтверждается результатами вычислительного эксперимента: для подавляющего большинства блоков ЦИ абсолютное значение углового коэффициента прямой, интерполирующей σ_7, σ_8, после СП даже с минимальным рассматриваемым ОПИ, равным 10%, возрастает. Результатом этого будет увеличение количества блоков матрицы СС, в которых скорость изменения наименьших СНЧ будет больше некоторого числового порога k, по сравнению с ОС. Для оценки этого порога в качестве предмета исследования рассматривались гистограммы значений скорости изменения минимальных СНЧ (ГМСЧ) блоков ОС и СС, полученных LSB-методом с разными ОПИ, результат работы которого представлялся в соответствии с (4). В ходе эксперимента, в котором участвовало 450 ЦИ, было установлено, что, как и ожидалось, аргумент, в котором достигается максимум гистограммы, монотонно увеличивается с увеличением ОПИ, при этом для исходного КсП пик ГМСЧ достигается в аргументе, меньшем 0.5. Такая картина наблюдается для большинства протестированных ЦИ, поэтому для предлагаемого СА алгоритма, основные шаги которого представлены ниже, в качестве порогового значения используется $k = 0.5$.

Стеганоаналитический алгоритм детектирования секретного сообщения, погруженного LSB-методом в КсП (h – шаг ГМСЧ)

Шаг 1. Тестируемое ЦИ в ФБП с матрицей F_{test} пересохранить в ФСП. Полученное в результате изображение с матрицей $F_{test \to J}$.

Шаг 2. Построить матрицу $R_{test} = abs\left(F_{test} - F_{test \to J}\right)$.

Шаг 3. Построить гистограмму значений элементов R_{test}. Определить $M\left(R_{test}\right)$ и $\max\left(R_{test}\right)$

Если $M\left(R_{test}\right) < 2 \,\&\, \max\left(R_{test}\right) < 33$

то F_{test} не может отвечать СС, построенному на основании КсП

иначе

Шаг 3.1. Построить ГМСЧ для F_{test}

Шаг 3.2. Определить номер N столбца ГМСЧ, в котором достигается максимум

Если $N < \dfrac{k}{h}$

то F_{test} отвечает ЦИ, не подвергшемуся СП

иначе F_{test} отвечает СС

Для апробации разработанного алгоритма в среде Matlab был проведен вычислительный эксперимент для более 800 различных изображений, первоначально хранимых в различных форматах с потерями, в качестве которых использовались JPEG (основанный на дискретном косинусном преобразовании), JPEG2000 (основанный на вейвлет-преобразовании) [10], сжатие, основанное на использовании аппроксимаций блоков ранга r матрицы изображения (МАБ), не являющееся стандартом, но часто используемое при решении различных прикладных задач [13, 14], каждое из которых подвергалось в процессе эксперимента СП с различными ОПИ. Использование бóльшего количества вариантов ФСП для КсП вызывает значительные затруднения в силу отсутствия их стандартов в свободном доступе.

Пересохранение в ФСП на шаге 1 разработанного алгоритма для определенности и единообразия везде проводилось в JPEG в среде Adobe Photoshop с коэффициентом качества $Q = 10$. Результаты тестирования работы алгоритма представлены в таблице ниже.

При организации вычислительного эксперимента для получения КсП в формате JPEG2000 ЦИ в ФБП были пересохранены в JPEG2000 в Adobe Photoshop с коэффициентами качества $Q = 8$, $Q = 9$ (такие коэффициенты были выбраны как качественные аналоги коэффициента $Q = 10$ для JPEG,

основанном на дискретном косинусном преобразовании. Аналогия устанавливалась путем субъективного ранжирования). Аналогичным образом выбирался ранг аппроксимации в МАБ.

Результаты работы стеганоаналитического алгоритма для различных форматов с потерями, используемых для хранения контейнера

ФСП, использованные для КсП	Количество выявленных СС относительно общего количества СС (%)				Количество выявленных ОС относительно общего количества ОС (%)
	ОПИ				
	30%	40%	50%	>50%	
JPEG	69	91	98	≥98	97
JPEG2000 ($Q = 8$)	67	92	96	≥96	98
JPEG2000 ($Q = 9$)	70	92	98	≥98	98
МАБ ($r = 4$)	90	95	99	≥99	99.5
МАБ ($r = 5$)	90	94	98	≥98	99.5

Поскольку, как правило, при использовании LSB-метода на практике ОПИ достаточно большой (50%–100%) [2], то полученные в ходе эксперимента результаты говорят о высокой эффективности разработанного стеганоаналитического алгоритма в условиях применения LSB-метода к КсП.

Заметим, что несколько бóльшая эффективность разработанного СА алгоритма в случае МАБ очевидно объясняется тем, что здесь сжатие осуществлялось непосредственно за счет обнуления наименьших СНЧ блоков матрицы ЦИ, которые затем и анализировались в процессе СА.

Заключение. На основе МПСА в работе разработан эффективный в условиях применения LSB-алгоритма СА алгоритм для КсП. Проделанный анализ и полученные результаты позволяют надеяться на успешную адаптацию данного алгоритма для детектирования работы стеганографических методов, отличных от LSB, на что и направлены в настоящий момент усилия автора.

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.** *G. Gul, F. Kurugollu*. SVD-Based Universal Spatial Domain Image Steganalysis / IEEE Transactions on Information Forensics and Security. – 2010. – Vol. 5, No. 2. – P. 349–353. **4.** *G. Gul, A. E. Dirik, I. Avcibas.* Steganalytic features for JPEG compression based perturbed quantization / IEEE Signal

Process. Lett. – 2007. – Vol. 14, No. 3. – P. 205–208. **5.** *S. Lyu, H. Farid*. Detecting hidden messages using higher-order statistics and support vector machines / Lecture Notes in Computer Science. New York. – 2002.– Vol. 2578. – P. 340–354. ***6.*** *I. Avcibas, M. Kharrazi, N. Memon*, and etc. Image steganalysis with binary similarity measures / EURASIP J. Appl. Signal Process. – 2005. – Vol.7. – pp. 2749–2757. **7.** *Бобок И. И., Кобозева А. А.* Стеганоанализ как частный случай анализа информационной системы / Сучасна спеціальна техніка. – 2011. – № 2. – С. 21–34. **8.** *Бобок И. И., Кобозева А. А.* Общий стеганоаналитический подход, основанный на матричном анализе / Вісник Національного технічного ун-ту «ХПІ». Збірник наукових праць. Тематичний випуск «Системний аналіз, управління та інформаційні технології». – 2011. – № 35. – С. 12–20. **9.** *Кобозева А. А.* Анализ информационной безопасности / *А. А. Кобозева, В. А. Хорошко*. – К. : ГУИКТ, 2009. – 251 с. **10.** *Гонсалес Р.* Цифровая обработка изображений / *Р. Гонсалес, Р. Вудс*; пер. с англ. под ред. *П. А. Чочиа*. – М. : Техносфера, 2005. – 1072 с. **11.** *Кобозєва А. А.* Аналіз захищеності інформаційних систем / *А. А. Кобозєва, І. О. Мачалін, В. О. Хорошко*. – К. : ДУІКТ, 2010. – 316 с. ***12.*** *Кобозева А. А.* Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / Искусственный интеллект. – 2007. – № 4. – С. 531–538. **13.** *Деммель Дж.* Вычислительная линейная алгебра / *Дж. Деммель*; пер.с англ. *Х. Д. Икрамова*. – М. : Мир, 2001. – 430 с. **14.** *Каханер Д.* Численные методы и программное обеспечение / *Д. Каханер, К. Моулер, С. Нэш*; пер. с англ. *Х. Д. Икрамова*. – М. : Мир, 2001. – 575 с.

Надійшла до редколегії 26.12.2011