УДК 004.056.5: 518

Кобозева А.А., Николаенко О.В., Ткач Д.В.
ОНПУ

НОВЫЙ ПОДХОД К ПРОБЛЕМЕ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА К АТАКЕ СЖАТИЕМ

1.Введение

Сегодняшнее общество, его жизнедеятельность немыслимы без накопления, хранения, изменения, передачи информации. В силу этого трудно переоценить важность и актуальность вопросов, связанных с ее защитой. Специфика сегодняшнего дня заключается в том, что информация характеризуется не только как ресурс, обеспечивающий деятельность общества, но и как объект труда. Действительно, в настоящее время в число защищаемых помимо военных, государственных и ведомственных, включены также секреты промышленные, коммерческие и даже личные, а сама информация все больше становиться товаром, причем одним из самых дорогих [1].

Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии. Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде, а также средств реализации этих методов. Компьютерная стеганография — самостоятельное научное направление информационной безопасности, изучающее проблемы создания компонентов скрываемой информации в открытой информационной среде, которая может быть сформирована вычислительными системами и сетями. Особенностью стеганографического подхода является то, что он не предусматривает прямого оглашения факта существования защищаемой информации. Это обстоятельство позволяет в рамках традиционно существующих информационных потоков или информационной среды решать некоторые важные задачи защиты информации ряда прикладных областей [1-4].

Стеганографирование осуществляется различными способами. Общей чертой этих способов является то, что скрываемое сообщение, или дополнительная информация (ДИ) встраивается в некоторый безобидный, не привлекающий внимание объект, или контейнер. Процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС).

К любому стеганографическому алгоритму (СА) предъявляется требование устойчивости к преднамеренным (непреднамеренным) атакам [2], при этом СА назовем *неустойчивым* согласно [4], если даже малые возмущающие воздействия – атаки, направленные на СС, могут привести к значительному или полному уничтожению встроенной в контейнер при помощи этого алгоритма секретной информации, и *устойчивым* в противном случае. Созданию устойчивых алгоритмов в современной печати уделено достаточное внимание, однако вопрос создания СА, устойчивых к атаке сжатием, являющейся чрезвычайно распространенной в силу популярности использования форматов с потерями для хранения и передачи цифровых сигналов (в частности цифровых изображений (ЦИ)), а потому часто остающейся незамеченной сторонами, непосредственно организующими секретный канал связи, остается актуальным и на сегодняшний день. Как правило, все существующие СА такого плана осуществляют погружение ДИ в частотной области контейнера в коэффициенты средней части частотного спектра и выдерживают лишь незначительное сжатие [2,5]. В силу этого

актуальным остается поиск принципиально новых путей и подходов к решению проблемы разработки СА, устойчивых к сжатию.

Поскольку процесс сжатия, осуществляемый с различными коэффициентами, приводит к различным «по силе» возмущающим воздействиям (и не обязательно малым), конкретизируем понятие СА, устойчивого к такой атаке (для определенности везде ниже в качестве ОС выступает ЦИ в градациях серого, а в качестве ДИ - бинарная последовательность, сформированная случайным образом). Во-первых, в силу специфики предметной области решаемой задачи не имеет смысла рассматривать сжатие с потенциально произвольным коэффициентом, поскольку после проведенной на СС атаки надежность восприятия этого СС не должна быть нарушена. В соответствии с [6] в настоящей работе рассматриваются варианты JPEG-сжатия ЦИ, осуществляемого в среде Photoshop с коэффициентами качества $Q \in \{8,9,10,11,12\}$ (для меньших значений Q надежность восприятия может не соблюдаться). Во-вторых, поскольку до настоящего момента нигде в открытой печати не была приведена нижняя граница числа, каким-либо образом характеризующего эффективность декодирования СА, для которой алгоритм еще можно называть устойчивым к операции сжатия (чаще всего такая оценка носит не количественный, а качественный характер), условимся считать СА устойчивым к сжатию, если объем правильно восстановленной информации (ОПИ) после атаки сжатием на СС с $Q \in \{8,9,10,11,12\}$, вычисляемый в соответствии с формулой

$$ОПИ = \frac{Количество\ бит\ секретного\ сообщения,\ восстановленных\ верно}{Общее\ количество\ бит\ в\ секретном\ сообщении} \cdot 100\%,$$

окажется не меньше 75% для наименьшего значения $Q = 8$ (такое значение для ОПИ уже рассматривалось в печати в виде порогового для оценки эффективности декодирования СА [7]). ОПИ является численной оценкой устойчивасти СА.

В [8] на основе теории возмущений был разработан новый общий подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), адаптация которого в область стеганографии дала возможность формально рассматривать процесс СП, *а также* любую атаку на СС или ОС, как совокупность возмущений сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) специального вида соответствующей матрицы (матриц) контейнера, независимо от рассматриваемой области сигнала, конкретики алгоритма погружения или предпринятой атаки [4].

Целью настоящей работы является разработка путем дальнейшей адаптации ОПАИС в область стеганографии принципиально нового подхода к решению проблемы обеспечения максимально возможной устойчивости СА к атаке сжатием при его создании. Разрабатываемый подход позволит получить *достаточные условия* такого обеспечения.

Для достижения посталенной цели необходимо решить следующие *задачи*:

1. Поскольку результат СП формально представим в виде совокупности возмущений СНЧ и СНВ соответствующей ОС матрицы (матриц), необходимо выделить из этих определяющих параметров наименее чувствительные к операции сжатия. Для этого
2. Необходимо получить формальное представление процесса сжатия в виде совокупности определенных возмущений СНЧ (СНВ) .
3. На основе решений задач 1 и 2 в качестве апробации предлагаемого подхода разработать конкретный СА, устойчивый к атаке сжатием.

4. Провести вычислительный эксперимент, выполнить сравнение эффективностей декодирования разработанного СА и имеющихся СА, устойчивых к сжатию.

2. Формальное представление процесса сжатия в виде совокупности возмущений сингулярных спектров матриц

Общая схема сжатия (с потерями) для ЦИ, как правило, 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 [9]. По такой схеме работает один из самых распространенных на сегодняшний день стандартов сжатия – JPEG. Последний шаг восстановления ЦИ после сжатия возвращает его 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 получено после округления значений яркости до целых и введения их в границы 0...255.

Процесс квантования приводит к обнулению коэффициентов, отвечающих, как правило, высоким частотам сигнала, за счет чего и происходит сжатие. Но при достаточно большом коэффициенте сжатия возможно обнуление и среднечастотных коэффициентов, поэтому использование для погружения ДИ средней части частотного спектра, о чем говорилось выше, формирует СС, которое принципиально может выдерживать лишь незначительное сжатие.

Пусть F - $m\times n$-матрица контейнера. Для F существует нормальное сингулярное разложение [8]: $F=U\Sigma V^T$, где U, V — ортогональные матрицы размерности $m\times n$ и $n\times n$ соответственно, столбцы $u_1,...,u_n$ матрицы U, называемые левыми СНВ, лексикографически положительны [8] (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 [8] показано, что невырожденная матрица имеет единственное нормальное сингулярное разложение, если ее СНЧ попарно различны, которое может представляться также в форме внешних произведений: $F=\sum_{k=1}^{n}\sigma_k u_k v_k^T$. Матрицу

$$S_k=\sigma_k u_k v_k^T \quad (1)$$

назовем k-й составляющей изображения F.

В [10] в результате представительного вычислительного эксперимента было установлено соответствие между элементами частотного спектра ЦИ и сингулярными тройками его матрицы: k-ые составляющие (1) изображения, отвечающие тройкам с максимальными СНЧ, соответствуют, главным образом, низкочастотным составляющим сигнала; k-ые составляющие ЦИ, отвечающие тройкам с минимальными (средними по величине) СНЧ, несут в себе, в основном, высокочастотные (среднечастотные) составляющие. Такой вывод может быть получен также на основании следующих рассуждений. В соответствии с [10] энергия $E(F)$ цифрового сигнала, представлением которого является матрица F, может быть определена по формуле:

$$E(F) = \sigma_1^{\,2} + \ldots + \sigma_n^{\,2} = \sum_{u=0}^{m-1}\sum_{v=0}^{n-1} P(u,v) = \sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij}^2$$

2)

где $P(u,v)$, $u = \overline{0,m-1}$, $v = \overline{0,n-1}$, - энергетический спектр сигнала с матрицей F [9], а f_{ij} элементы F. Энергия сигнала с матрицей S_k

$$E(S_k) = \qquad\qquad \sigma_k^2 .$$

3)

Действительно, поскольку

$$S_k = \sigma_k u_k v_k^T = \sigma_k \left(u_{1k},\ldots,u_{mk}\right)^T \left(v_{1k},\ldots,v_{nk}\right) = \sigma_k \begin{pmatrix} u_{1k}v_{1k} & u_{1k}v_{2k} & \ldots & u_{1k}v_{nk} \\ u_{2k}v_{1k} & u_{2k}v_{2k} & \ldots & u_{2k}v_{nk} \\ \ldots & \ldots & \ldots & \ldots \\ u_{mk}v_{1k} & u_{mk}v_{2k} & \ldots & u_{mk}v_{nk} \end{pmatrix}$$

то в соответствии с (2), учитывая ортогональность матриц U, V, получаем

$$E(S_k) = \sigma_k^{\,2}\left(u_{1k}^{\,2}v_{1k}^2 + \ldots + u_{1k}^2 v_{nk}^2 + u_{2k}^2 v_{1k}^2 + \ldots + u_{2k}^2 v_{nk}^2 + \ldots + u_{mk}^2 v_{1k}^2 + \ldots + u_{mk}^2 v_{nk}^2\right) =$$

$$= \sigma_k^2 (u_{1k}^2 (v_{1k}^2 + \ldots + v_{nk}^2) + \ldots + u_{mk}^2 (v_{1k}^2 + \ldots + v_{nk}^2)) = \sigma_{ki}^2 \left(u_{1k}^2 + \ldots + u_{mk}^2\right)\left(v_{1k}^2 + \ldots + v_{nk}^2\right) = \sigma_k^2 .$$

Из сопоставления формул (2) и (3) с учетом того, что наибольшие (наименьшие) значения $P(u,v)$ элементов энергетического спектра отвечают наименьшим (наибольшим) значениям u,v, вытекает упомянутое выше соответствие.

Результат сжатия в соответствии с [9] - это обнуление коэффициентов при высоких (и возможно средних) частотных составляющих в частотной области ЦИ. При использовании ОПАИС сжатие формально представимо в виде возмущения сингулярных троек, главным результатом которого, с учетом соответствия между элементами частотного спектра ЦИ и сингулярными тройками его матрицы, является обнуления наименьшим (и возможно средним) по величине СНЧ, что приведет к удалению из F k-х составляющих (1), где k имеет значения равные или близкие к n (вплоть до сравнимых с $n/2$). Это подтверждается результатами вычислительного эксперимента [11]: если для 8×8-блоков ЦИ, полученных после стандартного разбиения матрицы [9], хранящегося в формате без потерь, лишь около 3% общего числа блоков имеют нулевые СНЧ, то после квантования и ЧВ нулевые СНЧ присутствуют практически в каждом блоке. Иллюстрацией сказанному может служить блок конкретного TIF-ЦИ, сингулярный спектр которого первоначально имеет вид: 950.92, 164.12, 61.74, 17.10, 7.13, 4.10, 1.58, 0.70 . После квантования коэффициентов ДКП в процессе сжатия и ЧВ СНЧ соответственно равны: 950.68, 175.75, 53.64, 12.94, 0.71, 0.00, 0.00, 0.00.

Величина коэффициента квантования (коэффициент сжатия) отразится на количестве нулевых СНЧ в блоках: чем больше коэффициенты квантования, тем больше будет нулей в сингулярных спектрах.

Таким образом, независимо от того, *какой конкретно алгоритм используется для сжатия с потерями* ЦИ, результат этого процесса в соответствии с ОПАИС *всегда* может быть представлен в виде совокупности возмущений составляющих сингулярного спектра,

обязательной характерной чертой которой является обнуление наименьших (вплоть до средних) по значению СНЧ соответствующих матриц, что дает решение задачи 2. Как иллюстрирует приведенный выше пример, наибольшее СНЧ практически не возмутилось в процессе сжатия. Это не случайно. Сингулярные тройки, отвечающие максимальным СНЧ, соответствуют, главным образом, низкочастотным составляющим сигнала, а значит являются наименее чувствительными к сжатию, что принципиально решает задачу 1.

3. Стеганографический алгоритм относительной замены сингулярных чисел

Любое СП в соответствии с ОПАИС определяется совокупностью возмущений СНЧ (СНВ) матрицы контейнера F (или каких-то ее подматриц). Учитывая, что рассматриваемая в работе задача связана с процессом сжатия, осуществление которого предполагает предварительное разбиение матрицы ЦИ на 8×8-блоки, результат СП формализуем в виде совокупностей СНЧ (СНВ) всех блоков [4]. Для достижения цели работы необходимо выделить из СНЧ (СНВ) 8×8-блоков такие, возмущения которых в ходе СП обеспечат нечувствительность получаемого в результате СС к возмущающему воздействию – сжатию. В соответствии с полученным выше решением задачи 1 очевидно, что погружение ДИ надо производить так, чтобы результатом СП было возмущение наибольших по значению СНЧ. Однако, изменение величины максимального СНЧ в блоках всего на 5%-8%, возмущение которого в ходе СП *очевидно является наиболее желаемым*, как показывает вычислительный эксперимент, приводит к появлению явных артефактов на изображении, т.е. нарушает одно из наиболее важных требований к любому СА – требование обеспечения алгоритмом надежности восприятия формируемого им СС [4]. Такой же порядок относительного изменения второго по величине СНЧ не приводит к возникновению видимых артефактов. Типичный пример приведен на рис.1.

Таким образом, имеет место следующее утверждение, являющееся достаточным условием обеспечения максимально возможной устойчивости СА к сжатию.

Утверждение 1. Для обеспечения принципиально максимально возможной устойчивости СА к сжатию с одновременным обеспечением большой вероятности надежности восприятия формируемого СС *достаточно* производить погружение ДИ таким образом, чтобы формальным результатом СП было возмущение второго (и возможно третьего) по значению СНЧ в сингулярных спектрах 8×8-блоков матрицы контейнера. Если же СП формально выразится в возмущении средних и наименьших по значению СНЧ, то (при большой вероятности обеспечения надежности восприятия СС) устойчивость такого СА к сжатию может быть обеспечена только для сжатия с малыми коэффициентами (исключая $Q=8$).

На основе полученных заключений, в качестве примера СА, построенного в соответствии с утверждением 1, может выступать следующий.

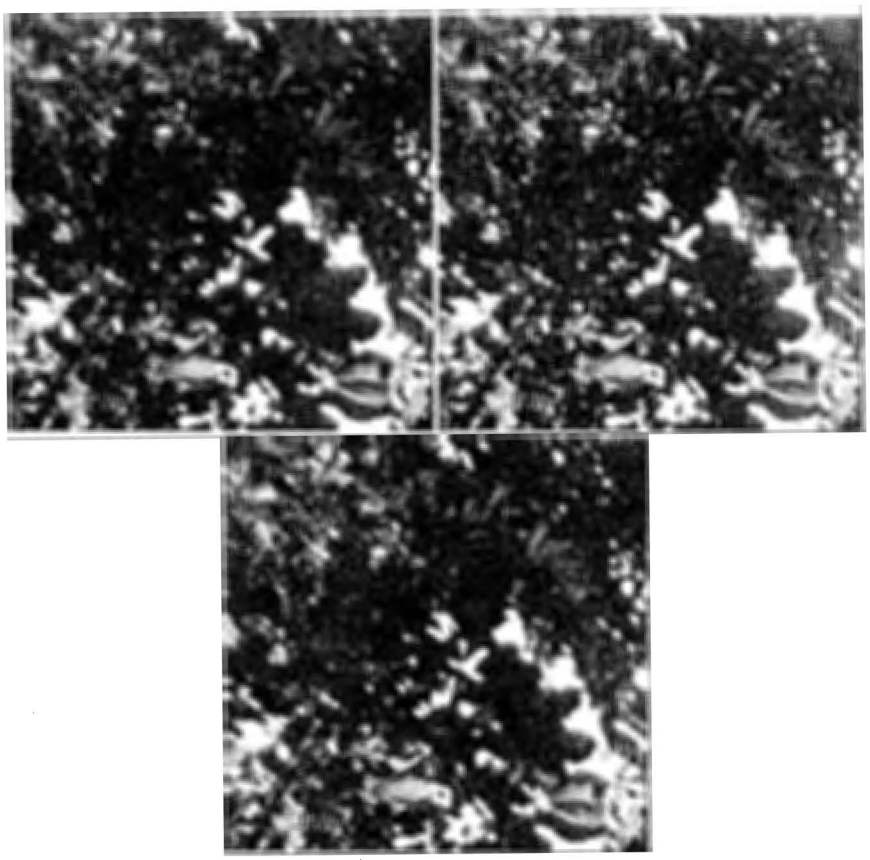

Рис.1. Результат возмущения СНЧ блоков матрицы ЦИ: а- исходное ЦИ; б – возмущению подвергнуто максимальное СНЧ блока; в - возмущению подвергнуто второе по величине СНЧ блока

Основные шаги процесса СП:

Шаг 1. Матрицу F ЦИ-контейнера размерами $n \times m$ разбить стандартным образом на 8×8-блоки $F_{ij}^{(B)}$, $i = 1,...,\left[\frac{n}{8}\right]$, $j = 1,...,\left[\frac{m}{8}\right]$.

Шаг 2 (погружение ДИ). Для каждого блока $F_{ij}^{(B)}$, $i = 1,...,\left[\frac{n}{8}\right]$, $j = 1,...,\left[\frac{m}{8}\right]$:

2.1. Построить сингулярное разложение $F_{ij}^{(B)} = U_{ij}^{(B)} \Sigma_{ij}^{(B)} \left(V_{ij}^{(B)}\right)^T$, где $\Sigma_{ij}^{(B)} = diag(\sigma_1, \sigma_2, \sigma_3, ..., \sigma_8)$;

2.2. Пусть b - очередной погружаемый бит секретного сообщения. Оценить разность $\sigma_2 - \sigma_3$. Встраиванию $b = 0$ соответствует $\sigma_2 - \sigma_3 \geq 50$ (при невыполнении полагаем новое возмущенное значение второго по величине СНЧ $\overline{\sigma}_2 = \sigma_3 + 50$), $b = 1$ соответствует $\sigma_2 - \sigma_3 \leq 10$ (при невыполнении полагаем $\overline{\sigma}_2 = \sigma_3 + 10$).

2.3. Построить очередной блок СС с матрицей $\overline{F}_{ij}^{(B)}$:

$\overline{F}_{ij}^{(B)} = U_{ij}^{(B)} \overline{\Sigma}_{ij}^{(B)} \left(V_{ij}^{(B)}\right)^T$, где $\overline{\Sigma}_{ij}^{(B)} = diag(\sigma_1, \overline{\sigma}_2, \sigma_3, ..., \sigma_8)$.

Основные шаги процесса декодирования ДИ:

Шаг 1. Матрицу $\overline{F}$ СС размерами $n \times m$ разбить стандартным образом на 8×8-блоки $\overline{F}_{ij}^{(B)}$, $i = 1,...,\left[\frac{n}{8}\right]$, $j = 1,...,\left[\frac{m}{8}\right]$.

Шаг 2 (декодирование ДИ). Для каждого блока $\overline{F}_{ij}^{(B)}$, $i = 1,...,\left[\frac{n}{8}\right]$, $j = 1,...,\left[\frac{m}{8}\right]$:

2.1. Построить сингулярное разложение $\overline{F}_{ij}^{(B)} = \overline{U}_{ij}^{(B)} \overline{\Sigma}_{ij}^{(B)} \left(\overline{V}_{ij}^{(B)}\right)^T$, где $\overline{\Sigma}_{ij}^{(B)} = diag(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, ..., \overline{\sigma}_8)$;

2.2. Оценить разность $\overline{\sigma}_2 - \overline{\sigma}_3$: если $\overline{\sigma}_2 - \overline{\sigma}_3 > 30$, то извлекаемый бит ДИ $b = 0$, иначе $b = 1$.

4. Результаты вычислительных экспериментов

Для апробации нового СА, названного *алгоритмом относительной замены сингулярных чисел* (АЗСНЧ) в среде Matlab был проведен вычислительный эксперимент, в котором в качестве ОС участвовало более 300 ЦИ в форматах Tif и Jpeg (Jpeg-ОС были получены путем пересохранения Tif-ЦИ в Photoshop с разными коэффициентами качества Q). После встраивания секретной информации СС сохранялись в формате Jpeg с потерями в Photoshop с коэффициентами качества $Q = 8,9,10,11,12$. Результаты декодирования ДИ приведены в таблице 1.

Таким образом, разработанный на основе ОПАИС новый АЗСНЧ является устойчивым к атаке сжатием при сохранении надежности восприятия получаемого СС. Для относительной оценки эффективности его работы было проведено сравнения работы АЗСНЧ с одним из наиболее широко распространенных СА, которые считаются устойчивыми к атаке сжатием - методом Кахо и Жао (МКЖ), или методом относительной замены величин коэффициентов дискретного косинусного преобразования (ДКП) [5]. МКЖ производит внедрение в коэффициенты ДКП средней части частотного спектра 8×8-блоков путем их взаимного изменения. Коэффициенты ДКП, выбранные для внедрения ДИ, задаются своими координатами в 8×8-массиве - $(i_1, j_1), (i_2, j_2)$ (рекомендуемые в [5] для внедрения ДИ коэффициенты (5,4) и (4,5)). Вычислительный эксперимент, в котором участвовало более 200 ЦИ в формате TIF, проводился в среде Matlab. После СП полученное СС сохранялось в Photoshop с $Q = 8,9,10,11,12$. Результаты эксперимента представлены в табл.2.

Сравнивнение результатов, приведенных в табл.1,2, говорит в пользу практического подтверждения выдвинутого ранее теоретического тезиса о том, что существующие СА, осуществляющие СП в частотной области контейнера в коэффициенты средней части частотного спектра, оказываются несостоятельными при сравнительно малом Q ($Q = 8$), где значительно надежнее выглядит АЗСНЧ (при этом для $Q = 9,10,11,12$ ОПИ в обоих алгоритмах сравнимы между собой). Заметим, что относительная замена коэффициентов (2,3), (3,2), которые являются низкочастотными, не может рассматриваться в качестве варианта МКЖ, т.к. приводит к нарушению надежности восприятия СС.

Таблица 1

Результаты декодирования секретной информации в алгоритме относительной замены сингулярных чисел

Q	ОПИ (%)		
	Tif-OC	Jpeg-OC $Q=12$	Jpeg-OC $Q=11$
8	82,0480	81,7065	82,9027
9	88,5894	88,4076	89,5593
10	94,1694	94,0241	95,2328
11	97,2369	97,0568	97,4091
12	98,1358	98,3027	98,4114

Проанализируем результаты СП, произведенного МКЖ, с точки зрения их представления в виде совокупности возмущений СНЧ блоков матрицы контейнера и соответствия их утверждению 1. В табл.3 для примера приведены типичные результаты для одного и того же блока тестируемого ЦИ. Эти результаты полностью соответствуют утверждению 1. Так МКЖ, использующий для СП коэффициенты ДКП с индексами (4,5) и (5,4) не мог оказаться устойчивым к сжатию, что и было получено ранее при тестировании его работы (табл.2), т.к. такое СП практически не возмутило наибольшие СНЧ. В соответствии с результатами табл.3 и утверждением 1, устойчивым к сжатию должен оказаться МКЖ, использующий коэффициенты ДКП с индексами (2,3) и (3,2), что полностью отвечает результатам его работы на практике (табл.2).

Таблица 2

Результаты декодирования секретной информации в методе Кахо и Жао

$(i_1, j_1), (i_2, j_2)$	Q	ОПИ (%)	Обеспечение надежности восприятия СС
(5,4), (4,5)	8	54.6339	+
	9	91.7782	+
	10	99.1146	+
	11	99.9362	+
	12	99.9947	+
(3,4), (4,3)	8	71.3798	+
	9	94.9230	+
	10	99.0976	+
	11	99.9126	+
	12	99.9782	+
(2,3), (3,2)	8	98.0660	-
	9	99.7319	-
	10	99.8848	-
	11	99.9132	-
	12	99.9392	-

Таблица 3

Возмущения СНЧ ЦИ, хранимого в формате TIF, при СП методом Кахо и Жао (СС после СП сохраняется без потерь)

(i_1, j_1), (i_2, j_2)	Характер восстановления ЦИ при обратном ДКП	Относительные погрешности СНЧ в порядке, отвечающем $\sigma_1, \sigma_2, ..., \sigma_8$ (%)
(5,4), (4,5)	ЧВ	0.0000 0.0899 3.7185 32.0837 93.2585 0.0623 265.5867 82.1709
	ПВ	0.0000 0.0362 3.3645 27.8843 97.7085 0.0402 258.8111 93.8611
(3,4), (4,3)	ЧВ	0.0000 0.3338 14.9730 0.5167 17.2428 3.2857 125.4383 62.1174
	ПВ	0.0000 0.4575 14.7477 0.4936 11.3472 1.9157 148.5082 62.6708
(2,3), (3,2)	ЧВ	0.0013 11.4289 3.2428 1.3678 8.1935 12.7950 0.2274 24.0782
	ПВ	0.0013 11.4957 2.8944 1.5089 2.2150 13.7399 7.9410 25.0259

5. Заключение

В работе предложен новый подход к проблеме обеспечения СА устойчивости к атаке сжатием при его разработке, основанный на ОПАИС, позволивший получить достаточное условие обеспечения принципиально максимально возможной устойчивости СА к сжатию с одновременным обеспечением большой вероятности надежности восприятия формируемого СС, что никогда не делалось ранее. Перспективность и обоснованность предложенного подхода подтверждается результатами тестирования разработанного на его основе нового стеганографического алгоритма АЗСНЧ.

Литература

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. — 272с.*
3. *Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. — К.: Арий, 2008. — 344с.*
4. *Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А.Кобозєва, І.О.Мачалін, В.О.Хорошко. - К.: Вид. ДУІКТ, 2010. – 316 с.*
5. *Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: МК — Пресс, 2006.*
6. *Кобозева А.А. Метод выявления результатов размытия цифрового изображения / А.А.Кобозева, В.В.Зорило // Сучасна спеціальна техніка. – 2010. - №3(22). – С.52-63.*
7. *Bergman C. Unitary embedding for data hiding with the SVD / C.Bergman, J.Davidson // Security, steganography and watermarking of multimedia contents VII, SPIE. — 2005. — Vol.5681. — P.619—630.*
8. *Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А.Хорошко. - К.: Изд.ГУИКТ, 2009. – 251 с.*
9. *Гонсалес Р. Цифровая обработка изображений / Р.Гонсалес, Р.Вудс; пер. с англ. под ред. П.А.Чочиа. — М.: Техносфера, 2005. — 1072 с.*
10. *Кобозева А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / А.А.Кобозева // Искусственный интеллект. — 2007. — №4. — С.531—538.*

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.

Рецензент: Хорошко В.О.
Поступила 24.11.2011

УДК 621.391+519.2

Попов А.А.
Национал. унив. обороны Украины

ИНВАРИАНТЫ ГРУПП ОТОБРАЖЕНИЙ СЛУЧАЙНЫХ СИГНАЛОВ (СООБЩЕНИЙ) В ПРИЛОЖЕНИИ К СТАТИСТИЧЕСКОМУ АНАЛИЗУ КРИПТОАЛГОРИТМОВ

Разработка любого криптоалгоритма предусматривает оценку его стойкости к практически разнообразным попыткам криптоанализа. Как известно, далеко не все разрабатываемые криптографические средства обеспечивают обещанный уровень защиты [1]. Криптографические средства защиты информации характеризуются тем, что для них не существует простых и однозначных тестов, позволяющих убедиться в надежной защите информации. Задача определения эффективности криптографических средств и методов защиты зачастую более трудоемкая, чем их разработка. Анализ разработанного криптоалгоритма является новой, прежде всего научной, а не инженерной задачей.

Фундаментальное допущение криптоанализа, сформулированное А. Керкгоффом (Kerckhoffs A.) [2], состоит в том, что секретность сообщения полностью зависит от ключа, т.е. весь криптоалгоритм, кроме значения ключа, известен противнику. Если статистически выявляемые закономерности каким-либо образом проявляются в зашифрованном тексте, у криптоаналитиков появляется возможность определить ключ криптоалгоритма (его составляющие) либо же сузить множество вероятных ключей. К. Шенноном введено понятие идеального шифра [3], т.е., такого, который полностью устраняет в криптограмме все статистические закономерности открытого текста.

Метод *разностного анализа, описанный в работах* [4], [5] сочетает в себе обобщение идеи общей линейной структуры с применением вероятностно-статистических методов исследования. Однако разностный анализ основан на использовании неравновероятности в распределении значений разности двух криптограмм, полученных из пары открытых текстов, имеющих некоторую фиксированную разность, и если все возможные значения разностей двух криптограмм будут появляться с близкими (в идеале – с равными) вероятностями, то метод разностного анализа не сможет работать эффективно.

Подобно разностному анализу, линейный криптоанализ [6] является обобщенным методом, сочетающим в себе поиск линейных статистических аналогов для уравнений криптоалгоритмов, статистический анализ имеющихся открытых и зашифрованных текстов, использующий также методы согласования и перебора. Этот метод эксплуатирует статистические линейные соотношения между отдельными координатами векторов открытого текста, соответствующего шифртекста и ключа и использует эти соотношения для определения статистическими методами отдельных координат ключевого вектора. На сегодняшний день метод линейного криптоанализа позволил получить наиболее сильные результаты по раскрытию ряда итерационных систем блочного шифрования.