ФОРМАЛЬНЫЕ УСЛОВИЯ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ СТЕГАНОМЕТОДА К СЖАТИЮ И ИХ РЕАЛИЗАЦИЯ В НОВОМ СТЕГАНОАЛГОРИТМЕ

Кобозева А.А., Мельник М.А.
Одесский национальный политехнический университет, Украина

Аннотация. На основе общего подхода к анализу состояния и технологии функционирования информационных систем получены достаточные условия для формального представления стеганопреобразования как совокупности возмущений сингулярных чисел матриц, отвечающих контейнеру, обеспечивающие нечувствительность (малую чувствительность) формируемого стеганосообщения к сжатию. Полученные достаточные условия не зависят от используемой для погружения конфиденциальной информации области контейнера (пространственной или частотной) и конкретики стеганоалгоритма, определяются локализацией и относительной величиной возмущений сингулярных чисел соответствующих матриц основного сообщения, произошедших в ходе стеганопреобразования. Основными математическими инструментами являются матричный анализ и теория возмущений. В качестве контейнера рассматривается цифровое изображение. На основе полученных достаточных условий в работе разработан новый стеганографический алгоритм, основанный на возмущениях максимальных сингулярных чисел блоков матрицы контейнера. Алгоритм является устойчивым к сжатию, в том числе, с малыми коэффициентами качества. Представлены результаты вычислительного эксперимента.
Ключевые слова: стеганографический алгоритм, атака сжатием, цифровое изображение, сингулярное число, матрица.

CONDITIILE FORMALE DE ASIGURARE A STABILITĂŢII STEGANOMETODEI LA COMPRIMARE ŞI REALIZAREA LOR ÎNTR-UN STEGANOALGORITM NOU

Cobozeva A.A., Melinic M.A.
Universitatea Naţională Politehnică din Odesa, Ucraina

Rezumat. Pe baza abordării generale a analizei stării şi tehnologiei de funcţionare a sistemelor informaţionale sunt obţinute condiţiile suficiente pentru reprezentarea formală a steganotransformarii, ca agregat al perturbaţiilor numerelor singulare ale matricelor, ce răspund containerului, ce asigură insensibilitatea (sensibilitatea mică) a steganomesajului format la comprimare. Conditiile obţinute suficiente nu depind de informaţia utilizată pentru confundarea informaţiei confidenciale a ariei containerului (spaţiale sau frecvenţiale) şi de detaliile stenagoalgoritmului, şi se determină prin localizarea şi valoarea relativă a perturbaţiilor numerelor singulare ale matricelor corespunzătoare ale mesajului de bază, ce a avut loc în timpul steganotransformării. Instrumentele matematice de bază sunt analiza de matrice şi teoria perturbaţiilor. În calitate de container se consideră imaginea numerică. Pe baza condiţiilor suficiente obţinute în lucrare este elaborat un algoritm steganografic nou, bazat pe perturbaţiile numerilor maxime signulare ale bloculrilor matricei containerului. Algoritmul este stabil la comprimare, incluzând şi coeficienţi mici de calitate. Sunt prezentate rezulatele experimentului de calcul.
Cuvinte-cheie: algoritmul steganografic, atac prin comprimare, imaginea numerică, numărul singular, matrice.

FORMAL CONDITIONS OF STEGANOGRAPHIC METHOD'S SUSTAINABILITY TO COMPRESSION ATTACKS AND THEIR IMPLEMENTATION IN NEW STEGANOGRAPHIC ALGORITHM

Kobozeva A.A., Melnik M.A.
Odessa National Polytechnic University, Ukraine

Abstract. The analysis of the current development and operation of information systems provided sufficient data for definition of sufficient conditions for a formal presentation steganographic transformation as a set of perturbations of

singular values of the matrices (corresponding to the container) those ensure insensitivity (or low sensitivity) of formed steganographic message to compression attacks. The obtained sufficient conditions are independent of the confidential information that embedded to container (spatial or frequency) and specificity of stegano algorithm. The main mathematical tool is a matrix analysis. As the container is considered a digital image. New steganographic algorithm is developed and based on sufficient conditions that received in paper. The algorithm is stable to compression, including low compression rate. The results of computational experiments are presented.
Key words: steganographic algorithm, compression attacks, digital image, singular values, matrix.

1. Введение

Для современного общества проблема информационного обеспечения всех сфер деятельности: образования, строительства, медицины, финансов, энергетики и т.д. по своей значимости и актуальности превосходит проблему дальнейшей индустриализации производства, которая до недавнего времени считалась одной из центральных. Общество вступило в период своего развития, который по всеобщему мнению можно назвать информационным [1, 2]. В случае развертывания масштабируемой автоматизированной системы коммерческого учета электропотребления возникает необходимость безопасной передачи данных по открытым каналам связи, что требует решения вопросов информационной безопасности, которая структурируется в совершенно разных, но связанных между собой аспектах. Широкомасштабное использование вычислительной техники и телекоммуникационных систем, переход к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационных систем, к их высокой уязвимости [2, 3].

В современных условиях массового распространения средств электронной вычислительной техники, расширяющимися возможностями несанкционированных действий над информацией, необходимостью защиты не только государственной и военной, но и промышленной, коммерческой, финансовой тайн, защита информации в современных системах передачи данных как беспроводных, так и с использованием электрических сетей становится все более актуальной и сложной проблемой. Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем, электрических сетей, используемых в современных системах передачи данных, постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. Такое влияние образуется непредусмотренными связями, которые приводят к образованию электрических каналов утечки информации, что нельзя не учитывать при разработке информационной системы любой наполненности и направленности [3].

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке многочисленных методов, предназначенных для обеспечения безопасной передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Стеганографические методы, наряду с криптографическими, занимают важное место среди методов защиты информации [4-7]. Но если в криптографии наличие шифрованного сообщения само по себе привлекает внимание противников, то стеганография не предусматривает прямого оглашения факта существования защищаемой информации. Это обстоятельство позволяет в рамках традиционно существующих информационных потоков или информационной среды решать важные задачи защиты информации ряда прикладных областей [5,8-10].

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 [11]. 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 [3,11], при этом СА назовем *неустойчивым* согласно [2], если даже малые возмущающие воздействия – атаки, направленные на СС, могут привести к значительному или полному уничтожению встроенной в контейнер при помощи этого алгоритма конфиденциальной информации, и *устойчивым* в противном случае.

Проблеме создания устойчивых алгоритмов в современной печати уделено много внимания, однако вопрос создания СА, устойчивых к атаке сжатием, которая является чрезвычайно распространенной благодаря популярности использования форматов с потерями для хранения и передачи цифровых сигналов (в частности цифровых изображений (ЦИ), которые далее рассматриваются в качестве ОС), остается актуальным и на сегодняшний день. Как правило, все существующие СА такого плана осуществляют погружение ДИ в частотной области контейнера и, при условии обеспечения надежности восприятия СС, выдерживают лишь незначительное сжатие [11-13]. До настоящего момента не формализованы в целом и не унифицированы требования к СА, гарантированно обеспечивающие его устойчивость к атаке сжатием, не сформулированы достаточные (необходимые) условия наличия такой устойчивости.

Таким образом, *актуальным* остается поиск новых путей и подходов к принципиальному решению проблемы обеспечения и разработки СА, устойчивых к сжатию.

2. Цель исследования и постановка задачи

Цель настоящей работы – повышение эффективности процесса разработки стеганоалгоритмов, устойчивых к атаке сжатием, в том числе, при значительных коэффициентах сжатия, путем получения и использования формальных условий обеспечения нечувствительности (малой чувствительности) формируемого ими СС к возмущающим воздействиям.

В соответствии с общим подходом к анализу состояния и технологии функционирования информационных систем, разработанного одним из авторов настоящей статьи ранее в [2], основываясь на теории возмущений [14-18] и матричном анализе, результат процесса СП, независимо от способа и области погружения ДИ, можно представить как совокупность возмущений сингулярных чисел (СНЧ) и/или сингулярных векторов (СНВ) соответствующих контейнеру матриц (матрицы).

Пусть F - матрица монохромного ЦИ-контейнера, имеет размеры $n \times n$. Общая схема сжатия (с потерями) состоит из трех основных шагов: отображение в частотную область после предварительного разбиения матрицы изображения на 8×8 – блоки, квантование полученных коэффициентов, энтропийное кодирование. Обозначим B матрицу отдельного блока. Учитывая, что

- СНЧ B являются хорошо обусловленными [2],

- любые возмущения СНЧ проявятся абсолютно одинаково для матриц блоков ЦИ как в пространственной, так и в частотной области, что обеспечивает независимость от анализируемой области изображения (пространственной, частотной) формализации процесса СП в виде совокупности возмущений СНЧ блоков [19]

ниже будем рассматривать результат СП как совокупность возмущений СНЧ блоков матрицы контейнера. В связи с этим для достижения посталенной цели в работе решаются следующие *задачи*:

1. Получить достаточные условия для формального представления СП как совокупности возмущений СНЧ матриц, отвечающих контейнеру, обеспечивающих нечувствительность (малую чувствительность) формируемого СС к сжатию;
2. Разработать новый устойчивый по отношению к сжатию стеганоалгоритм, удовлетвряющий полученным достаточным условиям нечувствительности СС.

Тестирование разработанного СА будет проводиться путем вычислительного эксперимента в среде Matlab, при этом атака сжатием будет моделироваться путем пересохранения СС в Adobe Photoshop в формат Jpeg с различными коэффициентами качества Q. Будем говорить, что сжатие ЦИ проводится со значительным коэффициентом (или низким коэффициентом качества), если $Q \le 7$.

3. Основная часть

СНЧ B являются хорошо обусловленными в соответствии с соотношением [20]: $\max\limits_{1\le j\le 8}\left|\sigma_j(B)-\sigma_j(B+\Delta B)\right| \le \left\|\Delta B\right\|_2$, где ΔB - матрица возмущающего воздействия (в частности, матрица возмущения блока B при сжатии), $\left\|\bullet\right\|_2$ - спектральная матричная норма [20], $\sigma_j(B), \sigma_j(B+\Delta B),\ j=\overline{1,8}$, - СНЧ матриц B и $B+\Delta B$ соответственно. Характер поведения наименьших СНЧ блоков изображений с потерями качественно отличается от характера СНЧ с теми же номерами для блоков изображений без потерь: скорость их изменения (например, оцениваемая угловым коэффициентом линейной аппроксимации графика зависимости значения СНЧ от его номера) значительно меньше аналогичного параметра для TIF-блока [19].

Из вышесказанного и [19] вытекает ряд выводов, значимых для решения поставленных задач:

- возмущения различных СНЧ в ходе сжатия, анализ которых можно проводить как в частотной, так и в пространственной области изображения, сравнимы друг с другом и с величиной возмущающего воздействия (если учитывать оценку сверху), поэтому, при формальном представлении результата процесса СП в виде совокупности возмущений СНЧ для принципиальной возможности декодирования конфиденциальной информации совокупный результат возмущений при погружении ДИ должен превосходить возмущение, которое будет претерпевать блок СС в процессе сжатия.
- Наименьшие СНЧ не имеет смысла задействовать при организации процесса СП, т.к. после сжатия независимо от того, как возмущались эти СНЧ при погружении ДИ, они станут сравнимы друг с другом и с нулем, а погруженная в них информация с большой вероятностью будет утеряна.
- СНЧ нечувствительны к малым возмущениям (сжатию с высоким качеством). Однако, если сжатие будет происходить с низким качеством, что приведет к увеличению

$\|\Delta B\|_2$, возмущения в процессе сжатия СНЧ также увеличатся, а это значит, что при СП потребуется увеличение возмущения СНЧ, которые являются формальным представлением этого СП, чтобы «перекрыть» «разрушающее действие» сжатия. Однако в результате такого «перекрытия» возможно возникновение двух отрицательных последствий: во-первых, нарушение надежности восприятия СС; во-вторых, нарушение первоначального порядка СНЧ блоков: $\sigma_1 \geq ... \geq \sigma_8$. Данная ситуация может значительно затруднить (или даже сделать невозможным) процесс декодирования ДИ в случае, когда процесс СП формализован в виде совокупности возмущений СНЧ. Чтобы избежать нарушения первоначального порядка СНЧ, процесс СП (с учетом возможности сжатия СС с малыми коэффициентами качества) достаточно проводить таким образом, чтобы требуемые для «перекрытия сжатия» значительные возмущения претерпевали только максимальные СНЧ блоков σ_1 (и возможно σ_2): за счет величин их значений и значений их отделенностей [20] изменение их взаимного порядка после СП можно легко избежать. Так для σ_1 никаких ограничений вообще не выдвигается, а возмущение σ_2 желательно проводить в сторону увеличения его значения. Допустимая величина возмущений максимальных СНЧ, происходящих в результате погружения ДИ, должна быть установлена с учетом требования соблюдения надежности восприятия формируемого СС.

Проверим принципиальную возможность проведения возмущения максимальных СНЧ блоков так, чтобы «перекрыть сжатие» и не нарушить надежность восприятия результирующего ЦИ. Для этого оценим возмущения блока ЦИ при сжатии. Для получения оценки среднего возмущения, которое претерпевает блок матрицы ЦИ, хранимого без потерь, при сжатии с различным качеством в среде Matlab был проведен вычислительный эксперимент, в котором участвовало более 200 ЦИ размера 2000×2000 пикселей формата TIF. В ходе эксперимента эти изображения пересохранялись в среде Photoshop с различными коэффициентами качества Q. Было установлено, что при снижении Q величина возмущающего воздействия на блок при сжатии ЦИ возрастает. Так, например, при сжатии с $Q = 10$ чаще всего блок B ЦИ претерпевает возмущение ΔB, спектральная норма матрицы которого $\|\Delta B\|_2$ порядка 10, при этом максимальное возмущение $\|\Delta B\|_2 \approx 40$, что наблюдается для подавляющего большинства протестированных ЦИ. Если же $Q = 7$, то максимальное возмущение блока матрицы ЦИ достигает $\|\Delta B\|_2 \approx 75$. На рис.1 представлены типичные гистограммы для значений норм матриц возмущения блоков для конкретных ЦИ.

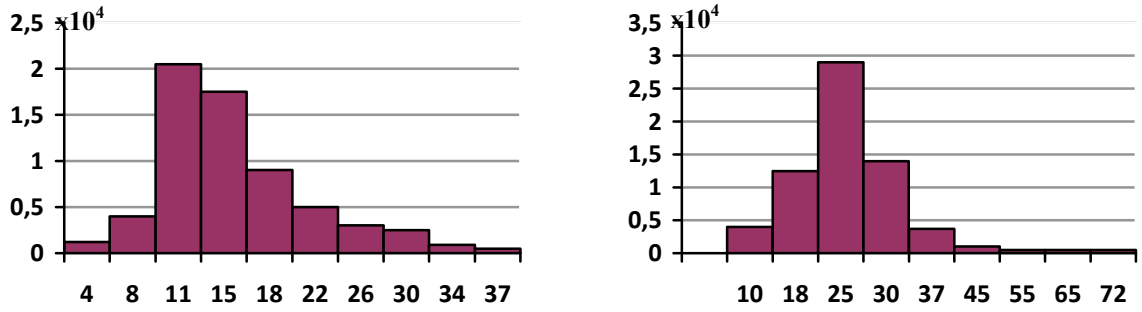
Как показывает вычислительный эксперимент, отделенность $svdgap(1, B)$ максимального СНЧ σ_1 матрицы B, определяемая как [20] $svdgap(1, B) = \min_{i \neq 1} |\sigma_1 - \sigma_i|$, для блока исходного ЦИ, хранимого без потерь, в подавляющем большинстве случаев будет *значительно* больше максимального значения нормы матрицы возмущения блока при сжатии. Исходя из результатов возможных возмущений при сжатии, процесс СП для существования принципиальной возможности осуществления декодирования ДИ может быть формализован как совокупность возмущений максимальных СНЧ блоков σ_1, превосходящих наибольшее значение $\|\Delta B\|_2$, если это не приведет к нарушению надежности восприятия СС, что проверялось путем проведения вычислительного эксперимента с 200 ЦИ в среде Matlab. В результате при возмущении максимального СНЧ

σ_1 каждого блока ЦИ в градациях серого на $\Delta\sigma_1 = \sigma_1(B) - \sigma_1(B + \Delta B)$, где $|\Delta\sigma_1| = 75$, нарушение надежности восприятия получаемого изображения, устанавливаемое путем субъективного ранжирования, могло как иметь, так и не иметь места. Кроме того, если подвергать возмущению максимальные СНЧ только одной из трех матриц цветов цветного ЦИ, то здесь даже вариант $|\Delta\sigma_1| > 75$ визуально может быть не выявлен. Таким образом, значительные возмущения максимальных СНЧ блоков *возможно* проводить так, чтобы это не вызывало нарушения надежности восприятия результирующего ЦИ.

Из приведенных результатов вытекает, что существует принципиальная возможность организации процесса СП таким образом, чтобы его формальным представлением были значительные возмущения максимальных СНЧ σ_1 блоков матрицы ЦИ.

Вывод. Для обеспечения устойчивости СМ (СА) к сжатию СП *достаточно* проводить таким образом, чтобы его формальным представлением была совокупность S возмущений СНЧ блоков, удовлетворяющая следующим условиям:

- если для сжатия СС предполагается использование высоких (возможно, средних) коэффициентов качества, то S не должна содержать возмущений наименьших СНЧ блоков матрицы контейнера;
- если для СС предполагается использование сжатия с низким коэффициентом качества, то S должна содержать возмущения только максимальных СНЧ блоков матрицы контейнера.
-



а б

Рис.1. Гистограммы значений спектральной нормы матрицы возмущения блока для ЦИ : а – $Q = 10$; б – $Q = 7$

На основе полученных теоретических выводов разработан новый стеганографический алгоритм. В качестве ОС может выступать как цветное ЦИ, так и изображение в градациях серого. Для цветного ЦИ погружение ДИ будет производиться в одну из матриц R, G или B (две другие остаются в первоначальном виде для обеспечения бóльшей вероятности соблюдения надежности восприятия получаемого СС, хотя также могут быть использованы в процессе СП). В качестве ДИ рассматривается сформированная случайным образом последовательность $p_1, p_2, ..., p_t$, где $p_i \in \{0,1\}$, $i = 1,2,...t$.

Обозначим через K пороговое значение вариации возмущений максимальных СНЧ блоков, смысл которого будет объяснен ниже. Тогда основные шаги предлагаемого алгоритма выглядят следующим образом.

Погружение ДИ.

Шаг 1. Матрица F контейнера разбивается стандартным образом на блоки B размером 8×8. Каждый блок используется для погружения 1 бита ДИ.

Шаг 2. (*Погружение бита ДИ*). Пусть B - очередной блок, используемый для СП, а p_i - очередной бит ДИ.

2.2. Строится сингулярное разложение [20] $B = U\Sigma V^T$, где U, V - ортогональные 8×8-матрицы СНВ, $\Sigma = diag(\sigma_1, \sigma_2, ..., \sigma_8)$ - матрица СНЧ;

2.3. ***Если*** $p_i = 0$

то $\overline{\sigma}_1 = \sigma_2 + K\left(n + \frac{1}{4}\right)$, где n - натуральное число;

иначе $\overline{\sigma}_1 = \sigma_2 + K\left(n + \frac{3}{4}\right)$, где n - натуральное число.

Шаг 3. (*Формирование блока СС* $\overline{F}$). $\overline{B} = U\overline{\Sigma}V^T$, где $\overline{\Sigma} = diag\left(\overline{\sigma}_1, \sigma_2, ..., \sigma_8\right)$.

Декодирование ДИ.

Шаг 1. Матрица $\overline{F}$ СС разбивается стандартным образом на блоки $\overline{B}$ размером 8×8. Каждый блок используется для декодирования 1 бита ДИ.

Шаг 2. (*Декодирование бита ДИ*). Пусть $\overline{B}$ - очередной блок, из которого извлекается бит $\overline{p}_i$ ДИ.

2.2. Строится сингулярное разложение $\overline{B} = \overline{U}\overline{\Sigma}\overline{V}^T$, где $\overline{\Sigma} = diag\left(\overline{\sigma}_1, \overline{\sigma}_2, ..., \overline{\sigma}_8\right)$;

2.3. ***Если*** $\mathrm{mod}\left(\left[\overline{\sigma}_1 - \overline{\sigma}_2\right], K\right) < \frac{K}{2}$, где $[\bullet]$ - целая часть аргумента

то $\overline{p}_i = 0$;

иначе $\overline{p}_i = 1$.

Рассмотрим подробно пороговое значение вариации возмущений максимальных СНЧ K. Исходя из приведенных выше результатов, значительную устойчивость предложенного алгоритма можно было бы ожидать в случае $K \geq 300$. Тогда остатки от деления $\sigma_1 - \sigma_2$, например, для $K = 300$, могут принимать значения из множества $\{0,1,2,...,299\}$. При погружении $p_i = 0$ СНЧ σ_1 очередного блока становится таким, что остаток от деления $\sigma_1 - \sigma_2$ на K равен 75, для $p_i = 1$ упомянутый остаток будет равен 225 (рис.2). Исходя из возможного максимального возмущения σ_1 при сжатии с $Q \geq 7$ ($\max\|\Delta B\|_2 \approx 75$) и конкретики алгоритма декодирования ДИ, сжатие с $Q \geq 7$ с большой вероятностью не сможет вывести значение СНЧ σ_1 за пределы «зоны», отвечающей погруженному биту ДИ (рис.2).

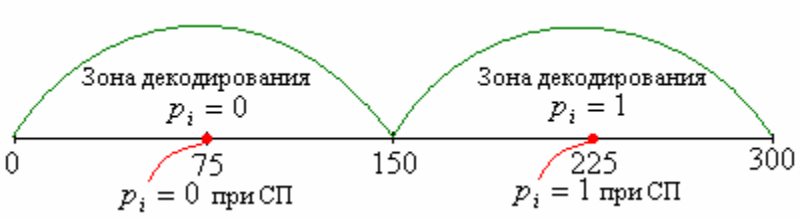


Рис.2. Иллюстрация процессов погружения и декодирования ДИ при $K = 300$

Однако, как показывает вычислительный эксперимент, значение $K = 300$, используемое в процессе СП, не всегда обеспечивало надежность восприятия СС, которая устанавливалась путем субъективного ранжирования. Заметим, что хотя максимальное значение возмущения блока рассматривалось как $\|\Delta B\|_2 \approx 75$, полученное для $Q = 7$, не имеет смысла выяснять максимальное значение $\|\Delta B\|_2$ для $Q < 7$: очевидно, что в этих случаях $\|\Delta B\|_2 > 75$, однако увеличение значения K в силу вышесказанного не представляется возможным.

Уменьшение K до 250 также не обеспечило надежность восприятия СС.

В вычислительном эксперименте, проведенном в среде Matlab для более, чем 400 ЦИ-контейнеров, хранимых как в формате с потерями (Jpeg), так и в формате без потерь (Tif), бралось значение $K = 200$. В этом случае нарушение надежности восприятия отмечено не было. Сформированные СС первоначально сохранялись в формате без потерь, а затем пересохранялись в Adobe Photoshop в формат Jpeg с различными коэффициентами качества, после чего происходило декодирование ДИ. Результаты экспериментов приведены в таблице 1. Объем восстановленной при декодировании ДИ P вычислялся в соответствии с формулой: $P = \dfrac{t - \sum_{i=1}^{t} p_i \oplus \overline{p}_i}{t} \cdot 100\%$, где $\oplus$ - операция логического исключающего ИЛИ, $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $\overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$, - декодированное из СС секретное сообщение.

Таблица 1. Зависимость объема восстановленной при декодировании ДИ от значения коэффициента качества Q

Формат хранения ЦИ-ОС	Среднее значение P при различных значениях коэффициента качества Q, используемого при сжатии СС (%)		
	$Q = 12$	$Q = 7$	$Q = 3$
Tif	98.97	98.07	92.13
Jpeg	98.54	98.11	91.06

Как видно из результатов эксперимента, эффективность предложенного алгоритма не зависит от формата хранения ОС, а объем восстановленной при декодировании ДИ говорит об устойчивости алгоритма к сжатию даже с малым коэффициенте качества $Q = 3$.

4. Заключение

В работе на основе матричного анализа и теории возмущений получены достаточные условия для формального представления стеганопреобразования как совокупности возмущений сингулярных чисел матриц блоков, отвечающих контейнеру, обеспечивающие нечувствительность (малую чувствительность) формируемого стеганосообщения к сжатию с одновременным обеспечением большой вероятности надежности его восприятия. Полученные достаточные условия не зависят от используемой для погружения секретной информации области контейнера (пространственной или частотной) и конкретики стеганоалгоритма, и определяются лишь локализацией и относительной величиной возмущений сингулярных чисел соответствующих матриц основного сообщения, произошедших в ходе стеганопреобразования.

На основе полученных достаточных условий представлен новый СА, устойчивый к сжатию даже с малыми коэффициентами качества: для $Q = 3$ среднее значение объема восстановленной информации составило $\approx 91.5\%$, что является практическим подтверждением полученных теоретических выводов.

Литература

[1] Куприянов А.И. Основы защиты информации / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов. — М.: Издательский центр «Академия», 2006. — 256 с.

[2] Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А.Хорошко. - К.: Изд.ГУИКТ, 2009. – 251 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] Cachin C. An Information-Theoretic Model for Steganography / C.Cachin // Information and Computation. — 2004. — Vol. 192, № 1. —p.41—56.

[5] Fridrich J. Lossless Data Embedding—New Paradigm in DigitalWatermarking / J.Fridrich, M.Goljan,R.Du // EURASIP Journal on Applied Signal Processing/ - 2002. – V.2. – PP. 185–196

[6] Lu C.-S. Media Hash-Dependent Image Watermarking Resilient Against Both Geometric Attacks and Estimation Attacks Based on False Positive-Oriented Detection / C.-S. Lu, S.-W. Sun, C.-Y. Hsu, P.-C. Chang // IEEE Transactions on Multimedia. – 2006. - Vol. 8. - NO. 4. – pp. 668-685.

[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] Pevny, T. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography / T. Pevny, T. Filler, P. Bas // Information Hiding. Lecture Notes in Computer Science. — 2010. — Vol.6387. — pp. 161–177.

[9] Li, B. A Survey on Image Steganography and Steganalysis / B. Li, J. He, *et al.* // Journal of Information Hiding and Multimedia Signal Processing. — 2011. — Vol.2, No.2. — PP.142–172.

[10] Natarajan, V. Universal Steganalysis Using Contourlet Transform / V. Natarajan, R. Anitha // Proceedings of the Second International Conference on Computer Science, Engineering & Applications (ICCSEA 2012), May 25-27, 2012, New Delhi, India. — 2012. — Vol.2. — PP. 727–735.

[11] Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ / А.В.Аграновский, А.В.Балакин, В.Г.Грибунин, С.А.Сапожников. – М.: Вузовская книга, 2009. – 220 с.

[12] Прохожев Н.Н. Влияние внешних воздействий на DC-коэффициент матрицы дискретно-косинусного преобразования в полутоновых изображениях / Н.Н.Прохожев, О.В.Михайличенко, А.Г.Коробейников // Научно-технический вестник Санкт-

Петербургского государственного университета информационных технологий, механики и оптики. – 2008. - №56. – С.57-62.
[13] Шумейко А.А. Использование квантования Ллойда-Макса для внедрения цифровых водяных знаков / А.А.Шумейко, А.И.Пасько, Т.Н. Тищенко // Інформаційна безпека. –2010. –№2.– С. 101-107.
[14] Маслов В.П. Асимптотические методы и теория возмущений / Маслов В.П. — М.: Наука. Гл.ред.физ.-мат.лит., 1988. — 312 с.
[15] Kato T. Scattering theory and perturbation of continuous spectra / T.Kato // Actes du Congres Int. de Math., Gauthier-Villars, Paris. — 1970. — P.135—140.
[16] Eisenstat S. Relative perturbation techniques for singular value problems / S.Eisenstat, I.Ipsen // Numer.Anal. —1995. — Vol.32. — P.1972—1988.
[17] Stewart G.W. Matrix Perturbation Theory / G.W.Stewart, J.-G.Sun. — New York: Academic Press, 1990. — 376 p.
[18] Higham N.J. Accuracy and Stability of Numerical Algorithms / N.J.Higham. — SIAM, Philadelphia, PA,1996. — 680 p.
[19] Бобок И.И. Метод детектирования стеганосообщения, сформированного посредством модификации наименьшего значащего бита / И.И.Бобок, А.А.Кобозева // Інформаційна безпека. – 2011. - №1(5). – С.56-63.
[20] Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х.Д.Икрамова. — М.: Мир, 2001. — 430 с.

Сведения об авторах

Кобозева Алла Анатольевна – д.т.н., проф., зав. каф. информатики и управления защитой информационных систем Одесского национального политехнического университета. Область научных интересов: математические методы защиты информации, численные методы, матричный анализ, дискретная математика. E-mail: alla_kobozeva@ukr.net

Мельник Маргарита Александровна – ст. препод. каф. информационной безопасности Одесского национального политехнического университета. Область научных интересов: методы защиты информации, стеганография, стеганоанализ.
E-mail: RITOCHEK@yandex.ua