STEGO TRANSFORMATION OF SPATIAL DOMAIN OF COVER IMAGE ROBUST AGAINST ATTACKS ON EMBEDDED MESSAGE

[1] A. Kobozeva, [1]E. Lebedeva, [2]O. Kostyrka
[1]Odessa National Polytechnik University, Ukraine
[2]Academy of Fire Safety named after Chernobyl Heroes, Ukraine

Abstract. One of the main requirements to steganografic algorithm to be developed is robustness against disturbing influences, that is, to attacks against the embedded message. It was shown that guaranteeing the stego algorithm robustness does not depend on whether the additional information is embedded into the spatial or transformation domain of the cover image. Given the existing advantages of the spatial domain of the cover image in organization of embedding and extracting processes, a sufficient condition for ensuring robustness of such stego transformation was obtained in this work. It was shown that the amount of brightness correction related to the pixels of the cover image block is similar to the amount of correction related to the maximum singular value of the corresponding matrix of the block in case of embedding additional data that ensures robustness against attacks on the embedded message. Recommendations were obtained for selecting the size l of the cover image block used in stego transformation as one of the parameters determining the calculation error of stego message. Given the inversely correspondence between the stego capacity of the stego channel being organized and the size of the cover image block, l=8 value was recommended.
Keywords: Stego algorithm, robustness, attack against the embedded message, spatial domain, digital image.

STEGANOTRANSFORMARE A REGIUNII SPAŢIALE A IMAGINII – CONTAINER, REZISTENTĂ ÎMPOTRIVĂ ATACURILOR CONTRA MESAJULUI ÎNCORPORAT

[1]Cobozeva A.A., [1]Lebedeva E.Iu., [2]Costârca O.V.
[1]Universitatea Naţională politehnică din Odesa, Ucraina
[2]Academia securităţii antiincendiare Eroii Cernobâl, Ucraina

Rezumat. Una dintre principalele cerinţele pentru steganoalgoritmul în procesul elaborării este cerinţa de stabilitate la perturbaţii – atacurilor îndreptate împotrivă mesajului încorporat. Se demonstrează, că stabilitatea steganoalgoritmului nu depinde de faptul, în ce regiune a containerului, care este considerat ca o imagine digitală - spaţială sau de transformare (în domeniul de frecvenţă, singularitate, descompunere a matricei imaginei etc.) are loc încărcarea informaţiei suplimentare. Având în vedere avantajele existente privind domeniul spaţial de codificare şi decodificare a informaţiei, în lucrare este formulată condiţia formală necesară de obţinute a stabilităţii procedurii de steganotransformare. Se demonstrează, că corectarea luminozităţii pixelilor în blocului containerului cu aceiaşi valoare este echivalentă cu efectul de corecţie a valorii maximale a numărului de singularitate a matricei respective a blocului containerului la încărcarea informaţiei suplimentare, care garantează stabilitatea la atacurilor contra informaţiei incorporate. Se prezintă recomandări privind dimensionarea blocului containerului utilizat pentru procedura de steganotransformare în calitate de parametru care determină eroarea de calcul în procesele de steganotransformare. Ţinând cont de raportul invers proporţional dintre capacitatea neevidentă de trafic a canalului organizat steganografic şi a dimensiunii blocului containerului se recomandă utilizarea dimensiunii l=8.
Cuvinte–cheie: Algoritm steganografic, stabilitate, atacul împotriva imaginii încorporate, imagine digitală.

СТЕГАНОПРЕОБРАЗОВАНИЕ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА, УСТОЙЧИВОЕ К АТАКАМ ПРОТИВ ВСТРОЕННОГО СООБЩЕНИЯ

[1]Кобозева А.А., [1]Лебедева Е.Ю., [2]Костырка О.В.
[1]Одесский национальный политехнический университет, Украина
[2]Академия пожарной безопасности им.Героев Чернобыля, Украина

Аннотация. Одним из основных требований, предъявляемых к стеганоалгоритму при его разработке, является требование устойчивости к возмущающим воздействиям – атакам, направленным против встроенного сообщения. Показано, что обеспечение устойчивости стеганоалгоритма не зависит от того, в какой области контейнера, в качестве которого рассматривается цифровое изображение, – пространственной или преобразования (частотной, области сингулярного, спектрального разложения матрицы изображения и др.) происходит погружение дополнительной информации. Учитывая существующие преимущества пространственной области изображения для организации процессов погружения/декодирования

информации, в работе получено формальное достаточное условие обеспечения устойчивости такого стеганопреобразования. Показано, что коррекция яркости пикселей блока контейнера на одно и то же значение аналогична коррекции максимального сингулярного числа соответствующей матрицы блока при погружении дополнительной информации, которая гарантирует устойчивость к атакам против встроенного сообщения. Получены рекомендации по выбору размера блока l контейнера, задействованного в стеганопреобразовании, как одного из параметров, определяющих величину вычислительной погрешности в стеганосообщении. С учетом обратно пропорционального соответствия между величинами скрытой пропускной способности организуемого стеганографичекого канала связи и размером блока рекомендовано l=8.

Ключевые слова: Стеганографический алгоритм, устойчивость, атака против встроенного сообщения, пространственная область, цифровое изображение.

1. Введение

Стремительный рост арсенала технических средств и систем, предназначенных для приема, передачи, обработки и хранения информации, происходящий сегодня повсеместно в учреждениях и организациях всех форм собственности, обусловлен стремительно нарастающим потоком информации, вызванным научно-техническим прогрессом. Физические процессы, происходящие в таких технических устройствах при их функционировании, создают в окружающем пространстве побочные электромагнитные, акустические и другие излучения, которые в той или иной степени связаны с обработкой информации [1]. Подобные излучения могут использоваться злоумышленниками, пытающимися получить доступ к секретной или конфиденциальной информации. Физические явления, лежащие в основе появления излучений, имеют различный характер, тем не менее, в общем виде утечка информации за счет излучений может рассматриваться как непреднамеренная передача секретной информации по некоторой «побочной системе связи». В силу этого необходимым является обеспечение дополнительной защищенности информации в условиях ее возможной утечки, для чего эффективными являются стеганографические методы [1-6].

В настоящий момент стеганография переживает этап своего бурного развития, связанный с многими объективными и субъективными причинами, среди которых ограничение и даже запрет на законодательном уровне в некоторых странах мира использования криптографии. В процессе стеганографирования конфиденциальная информация после предварительного кодирования, результатом которого является дополнительная информация (ДИ), погружается в контейнер, или основное сообщение (ОС), в качестве которого в работе рассматривается цифровое изображение (ЦИ), результатом чего является стеганосообщение (СС). СС открыто пересылается по каналу связи.

При разработке новых и усовершенствовании существующих стеганографических алгоритмов остро встают вопросы обеспечения ими различных требований, среди которых одним из основных является требование устойчивости алгоритма к различным возмущающим воздействиям – атакам, направленным против встроенного сообщения. К таким воздействиям относятся, в частности, наложение различных шумов на СС, фильтрация, сжатие СС с потерями и др. [4,7,8].

На протяжении долгого времени считалось, что для обеспечения помехоустойчивости стеганографических алгоритмов предпочтительной для погружения ДИ является область преобразования изображения [4,5,8-10], в частности, частотная область. В результате современных научных изысканий было показано, что обеспечение устойчивости стеганоалгоритма не зависит напрямую от того, в какой области контейнера

– пространственной или преобразования происходит процесс погружения ДИ [2,3], который будем называть стеганопреобразованием (СП). Любые изменения, происходящие при погружении ДИ в любой области контейнера (пространственной, области преобразования) однозначно отражаются в виде определенных изменений в других областях (преобразования, пространственной), приводящих к тем же результатам, касающимся устойчивости СП. При этом пространственная область обладает рядом преимуществ при организации СП, в частности, процесс погружения/декодирования ДИ в пространственной области ЦИ имеет меньшую вычислительную сложность, приводит к меньшему накоплению вычислительной погрешности за счет отсутствия дополнительной обработки контейнера, стеганосообщения.

Таким образом, пространственная область изображения-контейнера при разработке стеганоалгоритмов, устойчивых к возмущающим воздействиям, на сегодняшний день незаслуженно «отодвинута на второй план». Среди причин этого отсутствие до настоящего момента формальных достаточных условий обеспечения такой устойчивости для СП в пространственной области ЦИ; более простая реализации существующих достаточных условий в областях преобразования при организации погружения ДИ.

Все это оставляет *актуальной* задачу разработки эффективных в условиях активных атакующих действий СП в пространственной области контейнера-изображения.

2. Цель исследования и постановка задач

Целью работы является разработка теоретических основ обеспечения устойчивости стеганографических алгоритмов к возмущающим воздействиям – атакам против встроенного сообщения в пространственной области изображения-контейнера.

Для достижения цели необходимо решить *задачи*:

1. Получить соответствия между формальными представлениями устойчивых стеганопреобразований в области преобразования изображения и пространственной области;
2. Разработать формальное достаточное условие обеспечения устойчивости стеганоалгоритма к возмущающим воздействиям при организации стеганопреобразования в пространственной области контейнера-изображения;
3. Получить рекомендации по выбору размера блока контейнера, задействованного в стеганопреобразовании, как одного из определяющих вычислительную погрешность параметров в формируемом стеганосообщении.

Достижение поставленной цели позволит разработать на основе полученного формального достаточного условия обладающие приемлемой вычислительной сложностью стеганометоды и реализующие их алгоритмы, устойчивые к возмущающим воздействиям, работающие в пространственной области контейнера.

3. Основная часть

Достаточные условия обеспечения устойчивости к возмущающим воздействиям стеганометодов и алгоритмов уже обсуждались в открытой печати [2-4]. Однако эти условия реализовывались в областях преобразования матрицы контейнера. Так в [3] было доказано, что для обеспечения устойчивости к сжатию СП достаточно проводить таким образом, чтобы его формальным представлением была совокупность S возмущений максимальных сингулярных чисел (СНЧ) блоков матрицы контейнера. Полученное

достаточное условие обеспечивает устойчивость и к другим атакам против встроенного сообщения, а с учетом той математической базы, которая была положена в его основу, – общий подход к анализу состояния и технологии функционирования информационных систем [2,3], упомянутое достаточное условие рассматривается для возмущающих воздействий, независимо от их конкретики. Практической реализацией этого достаточного условия явились устойчивые к атакам против встроенного сообщения стеганометод и реализующий его алгоритм $A1$, разработанный в [3], где погружение ДИ, представляющей из себя случайно сформированную бинарную последовательность, проводилось путем возмущения максимальных СНЧ блоков матрицы ЦИ-контейнера, полученных в результате ее стандартного разбиения.

В силу однозначности нормального сингулярного разложения [3], дискретного преобразования Фурье, однозначного определения матрицы ЦИ в пространственной области своими элементами существует взаимнооднозначное соответствие между изменениями параметров, определяющих ЦИ, в разных областях преобразования, а также соответствие между изменениями параметров в области преобразования и параметров в пространственной области изображения. Основываясь на этом, найдем соответствие между возмущением максимального СНЧ блока матрицы контейнера, гарантирующего при СП его устойчивость к атакам против встроенного сообщения, и возмущениями яркости пикселей блока.

Пусть B - $l \times l$ – блок марицы изображения-контейнера. Для B существует сингулярное разложение [2,3]:

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

где U,V - ортогональные $l \times l$ – матрицы, столбцы которых u_i, v_i, $i = \overline{1,l}$, - левые и правые сингулярные векторы (СНВ) B соответственно, $\Sigma = diag(\sigma_1,...,\sigma_l)$, $\sigma_1 \geq ... \geq \sigma_l \geq 0$ - СНЧ.

Пусть процесс СП для блока формально выражается в возмущении его сингулярных чисел. Тогда его результатом будет блок $\overline{B}$ СС, отвечающий с учетом (1) матричному выражению:

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

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

Возмущение наибольшего СНЧ блока B с учетом (2) формально выразится следующим образом:

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

$$+(u_1,\ldots u_l)\begin{pmatrix}\Delta\sigma_1 & 0 & \ldots & 0\\ 0 & 0 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & \ldots & 0\end{pmatrix}(v_1,\ldots,y_l)^T, \qquad (3)$$

то есть

$$\overline{B} = B + \Delta\sigma_1 u_1 v_1^T .$$

Таким образом, отображением формулы (3) в пространственной области будет соотношение:

$$\overline{B} = B + \Delta B . \qquad (4)$$

где $\Delta B = \Delta\sigma_1 u_1 v_1^T$ - матрица возмущения блока B.

Соотношение (4) дает общее формальное представление процесса СП в пространственной области контейнера [2].

В [11] показано, что СНВ u_1, v_1 блоков матрицы ЦИ, отвечающие максимальным СНЧ, в случае нормального сингулярного разложения [2], которое дополнительно требует лексикографическую положительность левых СНВ, в подавляющем большинстве блоков изображения близки к *n*-оптимальному вектору n^O пространства R^l:

$$u_1 \approx n^O,\ v_1 \approx n^O, \qquad (5)$$

при этом *n*-оптимальный вектор имеет вид:

$$n^O = \left(\frac{1}{\sqrt{l}},\frac{1}{\sqrt{l}},\ldots,\frac{1}{\sqrt{l}}\right)^T \in R^l . \qquad (6)$$

Рассмотрим подробно матрицу ΔB, фигурирующую в (4), имеющую единичный ранг. Если $u_1 = (u_{11},u_{21},\ldots,u_{l1})^T$, $v_1 = (v_{11},v_{21},\ldots,v_{l1})^T$, то эта матрица представляется следующим образом:

$$\Delta B = \Delta\sigma_1 u_1 v_1^T = \Delta\sigma_1 \begin{pmatrix}u_{11}\\ u_{21}\\ \ldots\\ u_{l1}\end{pmatrix}(v_{11},v_{21},\ldots,v_{l1}) = \begin{pmatrix}\Delta\sigma_1 u_{11}v_{11} & \Delta\sigma_1 u_{11}v_{21} & \ldots & \Delta\sigma_1 u_{11}v_{l1}\\ \Delta\sigma_1 u_{21}v_{11} & \Delta\sigma_1 u_{21}v_{21} & \ldots & \Delta\sigma_1 u_{21}v_{l1}\\ \ldots & \ldots & \ldots & \ldots\\ \Delta\sigma_1 u_{l1}v_{11} & \Delta\sigma_1 u_{l1}v_{21} & \ldots & \Delta\sigma_1 u_{l1}v_{l1}\end{pmatrix}. \qquad (7)$$

С учетом (5) и (6) формула (7) может быть записана в виде:

$$\Delta B = \begin{pmatrix} \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \cdots & \frac{\Delta\sigma_1}{l} \\ \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \cdots & \frac{\Delta\sigma_1}{l} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \cdots & \frac{\Delta\sigma_1}{l} \end{pmatrix}. \quad (8)$$

Таким образом, устойчивое СП, которое первоначально было разработано в области сингулярного разложения матрицы [3], может быть реализовано в пространственной области ЦИ-контейнера путем коррекции яркости всех пикселей очередного блока, задействованного в процессе погружения ДИ, на одно и то же значение, равное

$$\Delta b = \frac{\Delta\sigma_1}{l}. \quad (9)$$

Замечание 1. Говоря о проблемах информационной безопасности в целом, необходимо отметить, что соответствие процессов (3)-(4) может рассматриваться и в обратном порядке: коррекция яркости пикселей, проводимая в пространственной области в качестве обработки ЦИ, может быть реализована путем коррекции максимального сингулярного числа соответствующей матрицы. Полученный математический результат может быть использован для решения других, не менее важных задач информационной безопасности: выявления результатов (несанкционированного) изменения изображения, локализации областей нарушения его целостности [12]. Решение упомянутых задач обеспечивается пассивными методами защиты информации и является очень важным в современных условиях повсеместного распространения различных программных комплексов, графических редакторов (Adobe Photoshop, GIMP и др.), используемых для фальсификаций цифровых контентов.

Основной вопрос при разработке конкретных стеганографических методов и алгоритмов, основанных на организации СП в соответствии с (4), (8), будет заключаться в определении/выборе значений $\Delta\sigma_1, l$, обеспечивающих устойчивость алгоритмов к различным возмущающим воздействиям с учетом соблюдения надежности восприятия формируемого СС. Величина блока l при организации СП важна также с учетом возможности возникновения/накопления вычислительной погрешности при формировании СС, которая, в свою очередь, может оказать негативное влияние на эффективность декодирования ДИ в разрабатываемых алгоритмах.

Замечание 2. С учетом особенностей машинной арифметики, а также соотношений (5) в большинстве блоков матрицы изображения после операции (3) точное равенство в (8) достигаться не будет, хотя отклонение будет незначительным.

Для практической оценки величины отклонения в среде Matlab был проведен вычислительный эксперимент, в котором было задействовано 200 ЦИ разных форматов (с потерями, без потерь), в градациях серого, цветные (цветовая схема RGB; в этом случае анализу подвергалась синяя составляющая изображения). В ходе эксперимента матрица ЦИ разбивалась на $l \times l -$блоки B ($l \in \{4,8,16\}$), для каждого из которых строилось

разложение (1), после чего σ_1 возмущалось на $\Delta\sigma_1$ ($\Delta\sigma_1 \in \{60,80,100\}$) (одинаковое для всех блоков); после возмущения СНЧ блок $\overline{B}$ восстанавливался в соответствии с (3). Когда описанная операция была проведена со всеми блоками ЦИ, оно переводилось в формат *uint8*, обеспечивающий введение значений яркости пикселей во множество $\{0,1,2,\ldots,255\}$, после чего в пространственной области ЦИ определялось значение среднего возмущения яркости пикселей по всему ЦИ, которое сравнивалось с ожидаемым (9). Иллюстрацией типичных результатов эксперимента является гистограмма полученных средних значений для случая $l=8$, $\Delta\sigma_1=80$, приведенная на рис.1. Среднее значение Δb по всем ЦИ здесь составило 9.65 (при ожидаемом 10), что отвечает относительной погрешности 3.5%. При этом средние значения Δb для большинства изображений, принимавших участие в эксперименте, оказались близкими к 10 (см.рис.1).

Замечание 3. При фиксированном $\Delta\sigma_1$ относительная погрешность получаемого по формуле (9) Δb будет увеличиваться с уменьшением l.

Действительно, чем меньше l, тем больше значение Δb коррекции яркости пикселей, тем больше вероятность того, что результат такой коррекции (как в случае осветления, так и в случае затемнения) приведет к выходу новых значений за пределы множества $\{0,1,\ldots,255\}$, т.е. к дополнительному росту вычислительной погрешности (и, как следствие, к росту вероятности возникновения ошибок при декодировании ДИ в стеганоалгоритме, основанном на (4), (8)).

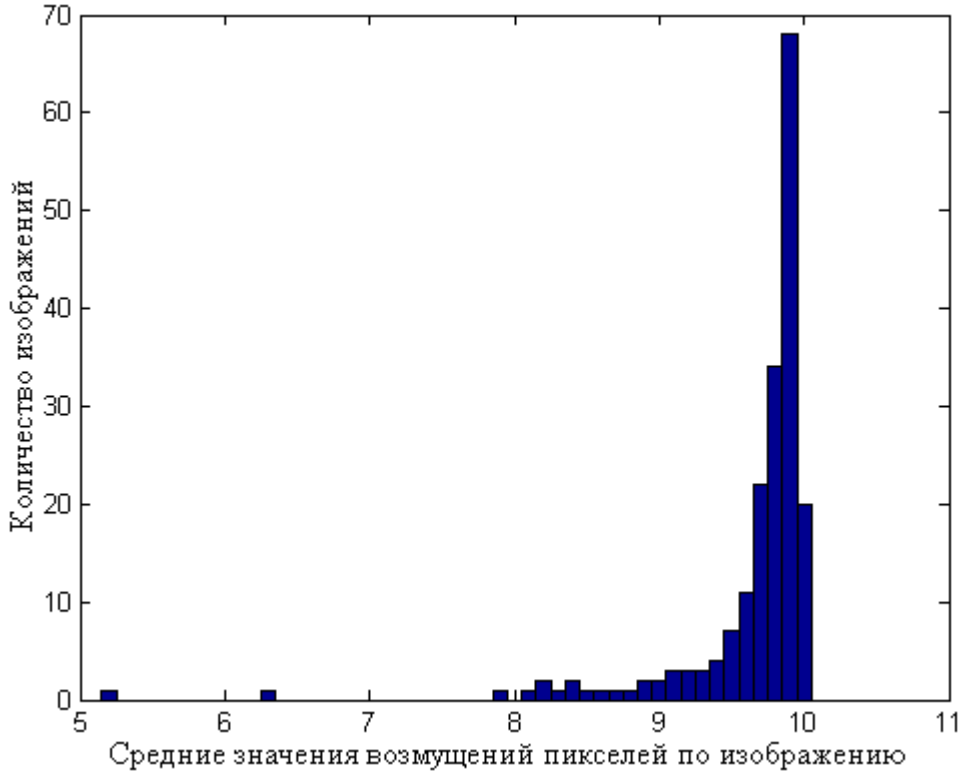

Рис.1. Гистограмма средних по изображению значений возмущений яркости пикселей ($l=8$, $\Delta\sigma_1=80$)

Практическим подтверждением истинности замечания 3 является монотонное убывание относительной погрешности среднего по эксперименту значения Δb с ростом размера блока l, установленное в результате описанного выше эксперимента, иллюстрацией чего является график, приведенный на рис.2 для $\Delta\sigma_1 = 80$. Заметим, что если при переходе от $l = 16$ к $l = 8$ относительная погрешность среднего значения Δb возрастает незначительно, то при переходе от $l = 8$ к $l = 4$ рост существенный, что говорит о преимуществах использования в процессе СП, основанного на (4), (8), блоков размера 8×8 над блоками 4×4. Преимущество 8×8-блоков по сравнению с блоками размера 16×16 вытекает из уменьшения в 4 раза скрытой пропускной способности [4] организуемого стеганографического канала связи в случае использования последних при СП. Таким образом, наиболее приемлемым размером блока матрицы контейнера для организации СП в соответствии с (4), (8) является $l = 8$.

Совокупные результаты проведенного эксперимента говорят о принципиальной возможности практического использования (8) при организации устойчивого к атакам против встроенного сообщения СП, основанного на (4).

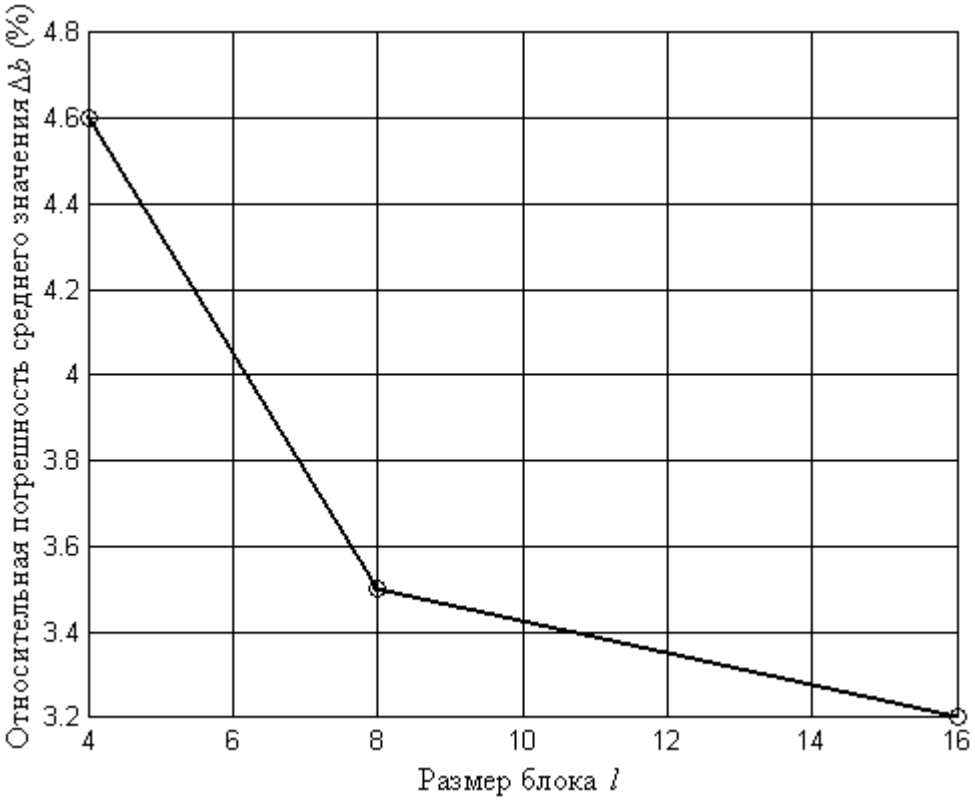

Рис.2.Зависимость относительной погрешности среднего по эксперименту значения Δb от размера блока изображения

В [11] показано, что для 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.

Пусть предполагаемое возмущение блока $\overline{B}$ СС при атаке – это $\Delta\overline{B}$, тогда в соответствии с соотношением [3]:

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

где $\sigma_j(\overline{B})$, $\sigma_j(\overline{B}+\Delta\overline{B})$ - СНЧ матриц $\overline{B}$ и $\overline{B}+\Delta\overline{B}$ соответственно, $\left\|\Delta\overline{B}\right\|_2$ - спектральная матричная норма $\Delta\overline{B}$, каждое СНЧ блока, в том числе и σ_1, возмутится на величину, меньшую либо равную $\left\|\Delta\overline{B}\right\|_2$. Тогда в соответствии с вышесказанным возмущение СНЧ σ_1 блока B при СП, организуемом в области сингулярного разложения, должно быть больше, чем $\left\|\Delta\overline{B}\right\|_2$, откуда вытекает, что возмущение Δb значений яркости пикселей блока B ОС при погружении ДИ в пространственной области для обеспечения устойчивости к атаке, количественной оценкой которой является $\left\|\Delta\overline{B}\right\|_2$, должно удовлетворять соотношению:

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

Таким образом, из всего вышесказанного вытекает истинность следующего утверждения.

Утверждение 1 (*достаточное условие устойчивости стеганоалгоритма к возмущающим воздействиям, реализуемое в пространственной области ЦИ-контейнера*). Для того, чтобы стеганографический алгоритм был устойчивым к атаке против встроенного сообщения, результат которой на блок $\overline{B}$ стеганосообщения оценивается как $\left\|\Delta\overline{B}\right\|_2$, достаточно, чтобы организуемое в пространственной области ЦИ-контейнера СП формально представлялось для $l\times l-$блока B ОС, задействованного в СП, в виде возмущения яркости пикселей на величину Δb, для которой имеет место соотношение (10).

Обеспечение устойчивости стеганоалгоритма к конкретным возмущающим воздействиям будет определяться конкретным выбором значения Δb, для чего необходима оценка величины $\left\|\Delta\overline{B}\right\|_2$.

В настоящий момент передача информации, в том числе ЦИ, по каналам коммуникаций происходит, как правило, в сжатом виде. Поэтому сама передача ЦИ в форматах без потерь, в большей или меньшей мере, привлекает к себе внимание. Это говорит о том, что СС еще на стадии его формирования для увеличения вероятности нераскрытия стеганографического канала связи имеет смысл сохранять в формате с потерями (например, Jpeg), т.е. для СП сегодня целесообразно *всегда* использовать стеганоалгоритмы, устойчивые к сжатию.

В [3] была получена оценка величины возмущающего воздействия стандартного $8\times8-$блока при сжатии ЦИ (формат Jpeg) с коэффициентами качества $QF\ge60$:

$\left\|\Delta\bar{B}\right\|_2 < 72$. Использование этого результата с учетом (10) определяет значение $\Delta b = 9$, которое гарантирует высокую устойчивость стеганоалгоритма, построенного на основе полученного достаточного условия, к сжатию для $QF \geq 60$, разработка которого и является сейчас основной задачей авторов.

4. Выводы

В работе получены следующие результаты:

- на основе матричного анализа и теории возмущений получено формальное достаточное условие обеспечения устойчивости стеганоалгоритма к атакам против встроенного сообщения при организации стеганопреобразования в пространственной области контейнера-изображения;
- получены рекомендации по выбору размера блока контейнера, задействованного в стеганопреобразовании, как одного из параметров, определяющих величину вычислительной погрешности в стеганосообщении. Для уменьшения накопления вычислительной погрешности при формировании стеганосообщения в соответствии с полученным достаточным условием устойчивости стеганоалгоритма, а также с учетом обратно пропорционального соответствия между величинами скрытой пропускной способности организуемого стеганографичекого канала связи и размером блока l рекомендовано $l = 8$.

Таким образом, в работе разработан теоретический базис для стеганометодов и алгоритмов, устойчивых к атакам против встроенного сообщения, осуществляющих стеганопреобразование в пространственной области контейнера-изображения.

Литература

[1] Horoshko, V.A. Metody I sredstva zaschity informatsii [Text]: nauchnoe izdanie / V.A. Horoshko, A.A. Chekatkov; Red. Iu.S. Kovtaniuc. — K.: IUNIOR, 2003. — 505 c. (in Russian)

[2] Kobozeva, A.A. Teoria vozmuschenii kak osnova obschego podhoda k otsenke chiuvstvitelinosti steganosoobschenii / A.A. Kobozeva, E.V. Naromanova // Informatika ta matematichny metody v modliuvanny. — 2012. — Том 2, Nr.3. — С.254–267. (in Russian)

[3] Kobozeva, A.A. Formalinye uslovia obespechenia ustoichivosti steganometoda k sjatiu i ih realizatsia v novom steganoalgoritme *[Electrony resurs]* / A.A. Kobozrva, M.A. Melinik // Problemy regionalnoy energhetiki. — Kishinau, 2013. — № 1(21). — С. 93–102. — Regim dostupu: http://ieasm.webart.md/data/m71_2_237.pdf (in Russian)

[4] Gribunin, V.G. Tsifrovaia steganografia [Text] : monografia / V.G. Gribunin, I.N. Okov, I.V. Turinsev. — M. : SOLON-Press, 2002. — 272 c. (in Russian)

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

[6] Podilchuk, C.I. Digital Watermarking: Algorithms and Applications / C.I. Podilchuk, E.J. Delp // IEEE Signal Processing Magazine. — 2001. — Vol.18, Iss. 4. — PP. 33–46.

[7] Nasir, I.A. A Robust Color Image Watermarking Scheme Based on Image Normalization / I.A. Nasir, A.B. Abdurrman // Proceeding of the World Congress on Engineering. — 2013 Vol III, WCE 2013, July 3-5, London, U.K.

[8] Perwej Y. Copyright protection of digital images using robust watermarking based on joint DLT and DWT / Y. Perwej, F. Perwej, A. Perwej // International Journal of Scientific & Engineering Research. — 2012. — Vol. 3, Iss. 6. — PP. 1–9.
[9] Fan, C.-H. A robust watermarking technique resistant Jpeg compression / C.-H. Fan, H.-Y. Huang, W.-H. Hsu // Journal of Information Science and Engineering. — 2011. — Vol. 27, Iss. 1. — PP. 163–180.
[10] Suhail, M.A. Digital watermarking based DCT and JPEG model / M.A. Suhail, M.S. Obaidat // IEEE Transactions on Instrumentation and Measurement. — 2003. — Vol. 52, Iss. 5. — PP. 1640–1647.
[11] Kobozeva, A.A. Nechuvstvitelinosti steganosoobschenia k sjatiu i formalinye dostatochnye uslovia ee obespechenia / A.A. Kobozrva, M.A. Melinik // Zbirnik naukovih pratsi Viiskovogo institutu Kievsikogo natsionalinogo univrsitetu ім. T. Shevchenka. – 2012. — Vip. 38. — C. 193–203. (in Russian)
[12] Kobozeva, A.A. Osnovy metoda vyiavlenia klonirovanyh uchastkov izobrajenia, podvergnutyh korrektsii iarkosti / A.A. Kobozeva, E.Iu.Levebeva // Suchasna spetsialina tehnika. – 2013. - №3. – C.13-20. (in Russian)

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

Лебедева Елена Юрьевна – ст. препод. каф. информатики и управления защитой информационных систем Одесского национального политехнического университета. Область научных интересов: методы защиты информации, методы обработки изображений.

Костырка Олеся Викторовна – аспирант Академии пожарной безопасности им.Героев Чернобыля (г.Черкассы). Область научных интересов: методы защиты информации, стеганография.