УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 362-373

РАЗРАБОТКА УСТОЙЧИВОГО К СЖАТИЮ СТЕГАНОПРЕОБРАЗОВАНИЯ ЦИФРОВОГО ИЗОБРАЖЕНИЯ НА ОСНОВЕ МЕТОДА МОДИФИКАЦИИ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА

А.А. Кобозева, Т.В. Варда, В.И. Ануфриев

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net, tomavarda@gmail.com

Стеганографическая система является составной частью любой современной комплексной системы защиты информации. Основой стеганосистемы, определяющей ее свойства, является используемый в ней стеганографический алгоритм. Работа посвящена повышению устойчивости стеганографической системы к атакам против встроенного сообщения путем разработки на основе метода модификации наименьшего значащего бита стеганографического алгоритма, устойчивого к сжатию с потерями. Обосновывается выбор области стеганопреобразования - области сингулярного разложения блоков матрицы цифрового изображения-контейнера. Из множества параметров, определяемых сингулярным разложением, процесс стеганопреобразования локализуется в максимальных сингулярных числах блоков матрицы, полученных путем ее стандартного разбиения. Выбор области для погружения дополнительной информации, в качестве которой в работе выступает бинарная последовательность, сформированная случайным образом, позволил обеспечить устойчивость разработанного стеганоалгоритма не только к сжатию с потерями, но и к другим атакам против встроенного сообщения: гауссовскому шуму, мультипликативному шуму. Показано, что эффективность разработанного алгоритма в условиях атаки сжатием сравнима с эффективностью современных аналогов, а для наиболее распространенных значений коэффициента качества, используемого при сжатии цифрового изображения (QF=70,75), превосходит их. Полученный результат является следствием выбора области изображения для стеганопреобразования (максимальные сингулярные числа блоков), которая при сжатии испытывает незначительные возмущения, по сравнению с другими составными области сингулярного разложения соответствующих матриц. Разработанный стеганографический алгоритм является полиномиальным степени 2, что делает его перспективным для использования в условиях потокового контейнера.

Ключевые слова: цифровое изображение, стеганографический алгоритм, метод модификации наименьшего значащего бита, максимальное сингулярное число блока, формат с потерями, формат без потерь.

Введение

Метод модификации наименьшего значащего бита (Least Significant Bit (LSB)) до настоящего момента стается одним из самых распространенных и широко используемых стеганографических методов [1], хотя его недостатки, главным из которых является неустойчивось к атакам против встроенного сообщения (когда погружение дополнительной информации (ДИ) происходит в пространственной области контейнера, в качестве которого в настоящей работе рассматривается цифровое изображение (ЦИ)) хорошо известны. Устранению этого недостатка уделяется значительное внимание. Так в [2] предложен метод двухэтапного декодирования, в основе которого лежит процесс, позволяющий уменьшить чувствительнось формируемого стеганосообщения (СС) к возмущающим воздействиям путем уменьшения числа обусловленности задачи декодирования.

Для повышения устойчивости LSB-метода предпринимаются попытки его использования в областях ЦИ-контейнера, отличных от пространственной, что связано с распространенным мнением о том, что стеганопреобразование (СП) в областях

преобразования, в частности, частотной области, являются более устойчивыми к атакам против встроенного сообщения (в частности к сжатию с потерями) [1]. Так в [3] разработан метод, основанный на LSB-преобразовании, использующий для погружения область дискретного преобразования Фурье (ДПФ), однако основная цель, на достижение которой направлено внимание автора, - это обеспечение при помощи разработанного метода проверки целостности передаваемой информации.

В работах [4-6] предлагаются стеганографические алгоритмы (СА), где погружение ДИ с использованием LSB-преобразования происходит в частотные коэффициенты ДПФ для блоков 2×2. В версии, представленной в [5] СА производит погружение одной буквы передаваемой информации, которая имеет 8-битное двоичного представления, в 1 блок контейнера, что очевидно не позволит для произвольного ЦИ, используемого в качестве контейнера, обеспечить надежность восприятия соответствующего СС, хотя это никак не оговорено в работе. И хотя устойчивость к возмущающим воздействиям соответствующих алгоритмов декларируется в упомянутых выше работах [4-6], вычислительные эксперименты, иллюстрирующие эффективность предлагаемых СА, проводятся на незначительном (часто меньше 10) количестве ЦИ, что ставит под сомнение объективность приведенных результатов и последующих выводов.

Таким образом задача повышения устойчивости к атакам против встроенного сообщения стеганографических методов, использующих LSB-преобразование, остается актуальной.

Цель статьи и постановка исследований

Стеганографическая система является составной частью любой современной комплексной системы защиты информации. Основой стеганосистемы, определяющей ее свойства, является используемый в ней СА [1,7].

Целью работы является повышения устойчивости стеганографической системы к атакам против встроенного сообщения путем разработки на основе LSB-преобразования стеганографического алгоритма, устойчивого к сжатию с потерями.

Для достижения цели в работе решаются следующие задачи:

- обосновать выбор области ЦИ-контейнера (пространственной, области преобразования) для осуществления СП таким образом, чтобы это давало принципиальную возможность для обеспечения устойчивости разрабатываемого СА к сжатию с потерями;
- подтвердить практически целесообразность сделанного выбора области ЦИ-контейнера для СП;
- разработать СА на основе LSB-преобразования, производимого в выбранной области контейнера;
- провести оценку, в том числе сравнительную, эффективности разработанного СА в условиях атак против встроенного сообщения.

Основная часть

Не ограничивая общности рассуждений, в качестве формального представления ЦИ рассматривается одна $n\times m$-матрица F, в качестве ДИ – сформированная случайным образом битовая последовательность: $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}, i=\overline{1,t}$.

Любое СП ЦИ-контейнера с матрицей F может быть представлено в виде [7]: $\overline{F} = F + \Delta F$, где $\overline{F}$ - матрица ЦИ-СС, ΔF - матрица возмущения контейнера в результате СП. В связи с этим, как показано в [7], результат погружения ДИ формально

может быть представлен в виде возмущений параметров, составляющих полный набор для матрицы F : совокупности сингулярных чисел (СНЧ) и/или сингулярных векторов (СНВ) матрицы (блоков матрицы) F , при этом свойства СС, СА, при помощи которого СС было получено, определяются свойствами возмутившихся в процессе СП СНЧ и/или СНВ. В связи с этим в качестве области СП целесообразно использовать область сингулярного разложения матрицы (блоков матрицы) ЦИ, непосредственно определяя и корректируя в ней должным образом требуемые свойства СА за счет корректировки возмущений полного набора параметров матрицы (блоков матрицы) при погружении ДИ. Использование СА, устойчивыми к сжатию, области сингулярного разложения соответствующих матриц уже имело место, например в [8,9]. В [8] показано, что для обеспечения нечувствительности СС к сжатию СП должно проводиться таким образом, чтобы его формальным результатом было возмущение максимальных СНЧ блоков (σ_1 и/или σ_2: $\sigma_1 \geq \sigma_2$), полученных стандартным разбиением матрицы контейнера, причем возмущения СНЧ должны превосходить возмущение, которое будет претерпевать блок при сжатии ЦИ с потерями. Наиболее часто используемыми при сжатии ЦИ коэффициентами качества QF на практике являются $QF \geq 70$. С учетом этого в [9] приводятся результаты представительного вычислительного эксперимента, целью которого было определение величин возможных возмущений матрицы 8×8-блока при сохранении ЦИ в формате Jpeg с $QF \geq 70$. Показано: в указанных условиях норма матрицы возмущения блока не превосходит 75; для обеспечения надежности восприятия формируемого СС возмущения СНЧ не должны превосходить 50, при этом устойчивость соответствующего СА будет тем больше, чем больше будут возмущения СНЧ в результате погружения ДИ.

Поскольку за основу разрабатываемого в данной работе СА взят метод LSB, то погружение бита ДИ имеет смысл проводить в 6 бит двоичного представления σ_1 или σ_2 после их округления до целого значения. Действительно, в этом случае величина возмущения СНЧ $\Delta\sigma = 2^5 = 32$, при этом значение пикового отношения «сигнал-шум», используемого для оценки визуальных искажений ЦИ, $PSNR = 39dB$, что в соответствии с [10] является приемлемым. Если же для погружения ДИ использовать 7-й бит двоичного представления σ_1 или σ_2 после их округления, то величина возмущения $\Delta\sigma = 2^6 = 64 > 50$, кроме того, значение $PSNR = 33dB$, что говорит о возможности нарушения надежности восприятия СС. Таким образом, (на данном этапе исследования) результатом локализации области для погружения бита ДИ является 6-й бит целой части σ_1 или σ_2.

В рассматриваемых условиях привлечение для СП σ_2 является нецелесообразным в силу следующей причины. Как показывает вычислительный эксперимент, значение σ_2 в блоках оригинального ЦИ-контейнера часто оказывается в окрестности $2^5 = 32$. Это приводит к тому, что при СП, использующем 6-й разряд, значение возмущенного σ_2 может оказаться меньше σ_3 ($\sigma_1 \geq \sigma_2 \geq \sigma_3$), а возможно меньше и последующих СНЧ, что приведет к изменению первоначального порядка СНЧ в блоке СС по сравнению с соответствующим блоком оригинального ЦИ. Следствием этого будет ситуация, когда декодирование бита ДИ будет происходить из СНЧ, не несущего в своем возмущении ДИ, что может привести к ошибке.

Иллюстрацией сказанному является сингулярный спектр 8×8-блока B оригинального ЦИ в формате tif: $\sigma_1 = 969.8221$, $\sigma_2 = 38.3538$, $\sigma_3 = 37.4455$, $\sigma_4 = 4.5496$, $\sigma_5 = 3.2947$, $\sigma_6 = 1.4942$, $\sigma_7 = 0.7871$, $\sigma_8 = 0.2154$, где $\sigma_2 = 38.3538$ после округления примет значение 38, двоичное представление которого: 100110. В результате погружения нуля значение $[\sigma_2]$ уменьшится на 32: новое (возмущенное) значение

$\bar{\sigma}_2 = 6$ (двоичное представление: 000110), что приведет к перестановке $\bar{\sigma}_2 = 6$ и $\sigma_3 = 37.4455$, для которого $[\sigma_3] = 37$ (двоичное представление: 100101), и при декодировании ДИ из такого блока извлечется 1. Аналогичная ситуация может иметь место и для ЦИ в формате с потерями.

Для практического подтверждения нецелесообразности использования в процессе СП σ_2 был проведен вычислительный эксперимент, в котором было задействовано 150 ЦИ размером 400×400 пикселей в формате без потерь (Tif) из базы [11] (множество M_1). В ходе эксперимента в каждый 8×8-блок каждого ЦИ из M_1 биты ДИ погружались двумя способами: в 6 бит результата округления до целого значения максимального СНЧ σ_1 блока; в 6 бит $[\sigma_2]$. Затем каждое из полученных СС сохранялось в формате Jpeg с QF=75. После чего проводилось декодирование ДИ. В результате ошибки при декодировании при первом способе погружения составили 8.9%, при втором, как и ожидалось, их количество оказалось больше – 11.7%.

Таким образом, в результате проведенных исследований выбрана область для погружения ДИ: 6-й бит результата округления до целого значения максимального СНЧ блока (σ_1) матрицы ЦИ-контейнера. Для оценки эффективности такого СП в случае разбиения матрицы на блоки размером 8×8 пикселей был проведен вычислительный эксперимент, в котором были задействованы ЦИ из множества M_1 (формат Tif), а также 150 ЦИ из базы NRCS [12] в формате Jpeg (множество M_2). После погружения ДИ СС сохранялось без потерь (Tif), а также с потерями (формат Jpeg с $QF \in \{75,85\}$). Результаты приведены в таблице 1.

Таблица 1.

Количество ошибок при декодировании ДИ в случае СП, использующего 6-й бит $[\sigma_1]$ 8×8-блоков матрицы ЦИ-контейнера (%)

Множество ЦИ	Формат, в котором сохраняется СС		
	Tif	Jpeg	
		QF=75	QF=85
M_1	0.20	8.9	4.3
M_2	0.18	7.9	4.0
Среднее значение по эксперименту	0.19	8.4	4.1

Из полученных результатов вытекает, что точность декодирования в рассмотренном СП выше для СС, полученных из ЦИ-контейнеров, которые хранятся в формате с потерями. Такой результат является абсолютно закономерным и имеет место в силу следующих причин. Главным результатом сжатия ЦИ с потерями является обнуление высокочастотной (возможно и среднечастотной) составляющей сигнала вследствие квантования с последующим округлением коэффициентов дискретного косинусного преобразования (ДКП) 8×8-блоков матрицы ЦИ [13]. Если ЦИ уже хранится в формате с потерями, то такой процесс хотя бы один раз оно уже претерпело, некоторые коэффициенты ДКП уже приняли нулевые значения, поэтому при повторном квантовании для таких коэффициентов значительных изменений не будет (изменения в пределах погрешностей округлений). Низкочастотные коэффициенты для ЦИ в формате без потерь и соответствующего ему ЦИ в формате с потерями отличаются незначительно, поэтому повторное квантование для ЦИ, первоначально хранившегося в формате с потерями, не может отразится значительно на них (также, как и на высокочастотных). Иллюстрация этого факта представлена на рисунке 1.

$$B_{DCT}=\begin{pmatrix}149.5000 & -17.2649 & 1.0196 & -2.1528 & -0.2500 & 1.1688 & -0.1517 & 0.2181\\ 7.7334 & -0.7444 & -3.6987 & 1.4329 & -0.8460 & 0.5169 & -0.0827 & -0.3988\\ -7.2489 & 1.7312 & -3.0910 & 0.4673 & 0.8843 & -0.1619 & -0.1768 & 0.2182\\ -1.6610 & 0.4212 & 0.7930 & -0.4865 & -1.5214 & 0.4675 & 0.4821 & -0.3341\\ 0.7500 & 0.2390 & 0.2310 & -0.7247 & 0.5000 & 0.0914 & -0.0957 & -0.1855\\ 2.1931 & -0.1659 & -0.8928 & 0.3211 & 0.4610 & -0.1599 & -0.1718 & -0.2859\\ -0.5152 & 0.2485 & -0.1768 & 0.3843 & 0.1749 & -0.4952 & 0.0910 & 0.0780\\ 0.0126 & 0.4548 & 0.6083 & 0.1902 & 0.3634 & 0.9329 & 0.0693 & -0.6091\end{pmatrix}$$

а

$$B_{DCT}^{(Jpg)}=\begin{pmatrix}152.0000 & -17.8625 & 0 & -0.5773 & 0 & -0.8323 & 0 & 0.3941\\ 12.0828 & 0 & -6.8493 & 0 & -0.7097 & 0 & 0.2566 & 0\\ 0 & -0.8974 & 0 & -0.0901 & 0 & -0.4531 & 0 & -0.5115\\ 0.5995 & 0 & 0.1877 & 0 & -0.0286 & 0 & 0.1549 & 0\\ 0 & -0.0585 & 0 & -0.0461 & 0 & 0.5190 & 0 & -0.9875\\ -0.4285 & 0 & -0.0373 & 0 & -0.1436 & 0 & 0.0361 & 0\\ 0 & 0.1591 & 0 & 0.4127 & 0 & 0.1130 & 0 & -0.1063\\ -0.4623 & 0 & -0.5584 & 0 & 0.4742 & 0 & 0.3841 & 0\end{pmatrix}$$

б

$$B_{DCT}^{(Jpg,Jpg)}=\begin{pmatrix}153.0000 & -16.9310 & 0.2310 & 0.2005 & -0.2500 & -0.1258 & -0.0957 & -0.1448\\ 11.8402 & 0.6858 & -5.8537 & 0.2635 & -0.3204 & 0.4675 & -0.1097 & 0.6667\\ 0.5576 & -0.1361 & -0.4268 & 0.0982 & -0.0396 & 0.1470 & 0.0732 & -0.1532\\ -0.1880 & -0.4548 & -0.2222 & -0.2254 & -0.1125 & 0.3797 & -0.0843 & -0.1409\\ -0.2500 & 0.1815 & -0.0957 & -0.1327 & 0.5000 & -0.0264 & -0.2310 & -0.2716\\ 0.0977 & -0.0056 & 0.2107 & 0.0262 & 0.0752 & 0.3718 & -0.0424 & 0.3988\\ 0.0396 & -0.0345 & -0.4268 & 0.4036 & 0.5576 & -0.4823 & -0.0732 & -0.1734\\ -0.0162 & 0.3132 & -0.1938 & -0.3211 & 0.0637 & -0.5901 & -0.2859 & 0.1678\end{pmatrix}$$

в

Рис. 1. Матрицы коэффициентов ДКП соответствующих 8×8-блоков: а – ЦИ в формате Tif; б – ЦИ, пересохраненного из формата Tif в Jpeg с QF=75; в - ЦИ, пересохраненного из формата Jpeg с QF=75 в Jpeg с QF=80

Таким образом, возмущения, которые претерпевает ЦИ в формате без потерь при сохранении в формат с потерями, значительнее, чем при пересохранении с потерями соответствующего ЦИ, которое уже первоначально было сохранено с потерями. Практическим подтверждением этого служат результаты вычислительного эксперимента, представленные на рисунке 2, где кривая, отвечающая ЦИ множества M_1 (формат без потерь), находится выше всех других кривых, отражающих зависимость среднего значения нормы матрицы возмущения ЦИ при сохранении в формат Jpeg для ЦИ, первоначально хранящихся с потерями.

Следствием вышесказанного является то, что в большинстве случаев возмущения, которые претерпевает максимальное СНЧ блока («несущее» ДИ) при сохранении ЦИ в формат с потерями, больше для изображения, которое первоначально хранилось без потерь, по сравнению с возмущениями в случае, когда исходное уже хранилось с потерями. Иллюстрация типичной картины возмущений максимального СНЧ представлена на рисунке 3. Из исходного ЦИ, хранимого в формате Tif, случайным образом был выделен 8×8-блок B (рис.3(а)), матрица которого представлена на рисунке 3(б). Для B было найдено максимальное СНЧ σ_1. ЦИ пересохранялось в формат Jpeg с коэффициентами качества $QF\in\{65,70,75,80,85,90\}$, после чего из каждого полученного ЦИ были извлечены блоки, отвечающие B, для удобства обозначаемые далее B_{65}, B_{70}, B_{75}, B_{80}, B_{85}, B_{90}, где нижний индекс отвечает коэффициенту QF, с которым было сохранено соответствующее изображение. Для каждого B_i, $i\in\{65,70,75,80,85,90\}$, вычислялось максимальное СНЧ $\sigma_1^{(i)}$, после чего определялись абсолютные значения возмущения σ_1 при пересохранении ЦИ с потерями: $\left|\sigma_1-\sigma_1^{(i)}\right|$, $i\in\{65,70,75,80,85,90\}$. Отражением описанного процесса является

ломаная 1 на рисунке 3(в). Далее ЦИ (рис.3(а)) дополнительно пересохранялось в Jpeg с $QF \in \{67,78,96\}$ (коэффициенты качества намеренно выбраны так, чтобы отличаться от используемых в процессе анализа возмущений максимального СНЧ блока).

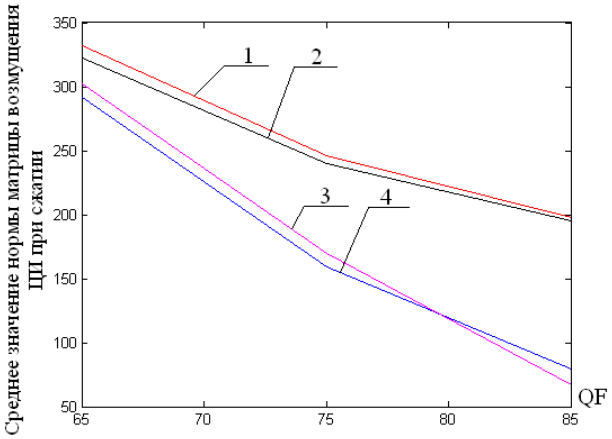


Рис. 2. Зависимость среднего значения по эксперименту нормы матрицы возмущения ЦИ при его пересохранении в формат Jpeg от используемого коэффициента качества QF: 1 – для ЦИ в формате без потерь (множество M_1); 2 - для ЦИ в формате с потерями (множество M_2); 3 – множество ЦИ в формате Jpeg (QF=67), полученных путем пересохранения с потерями изображений из множества M_1; 4 – множество ЦИ в формате Jpeg (QF=78), полученных путем пересохранения с потерями ЦИ из множества M_1

Для следующего этапа эксперимента были использованы пять ЦИ в формате Jpeg с $QF \in \{67,75,78,90,96\}$, обозначаемые далее $I^{(i)}$, $i \in \{67,75,78,90,96\}$. Эти ЦИ рассматривались как исходные. Из каждого выделялся блок, отвечающий B: B_i с максимальным СНЧ $\sigma_1^{(i)}$, $i \in \{67,75,78,90,96\}$. Далее для каждого ЦИ $I^{(i)}$ выполнялись следующие операции. Изображение $I^{(i)}$ пересохранялось в формат Jpeg с $QF \in \{65,70,75,80,85,90\}$. Для каждого вновь полученного ЦИ выделялся интересующий блок, отвечающий B, для которого находилось максимальное СНЧ. После чего находились абсолютные значения возмущений $\sigma_1^{(i)}$ в результате пересохранения ЦИ $I^{(i)}$ с потерями с $QF \in \{65,70,75,80,85,90\}$. Графики зависимости этих возмущений от QF для изображений $I^{(i)}$, $i \in \{67,75,78,90,96\}$, представлены на рис.3(в) (ломаные 2-6). Исходя из представленных результатов очевидно, что для приведенного примера возмущения, которые претерпевает максимальное СНЧ блока при пересохранении в формат с потерями ЦИ, первоначально хранимого без потерь, больше, чем в случае, когда пересохранению подвергаются ЦИ, уже хранимые с потерями, что в общем случае, объясняет меньшее количество ошибок при декодировании ДИ в случае, когда в качестве контейнера выбирались ЦИ в формате с потерями (табл.1).

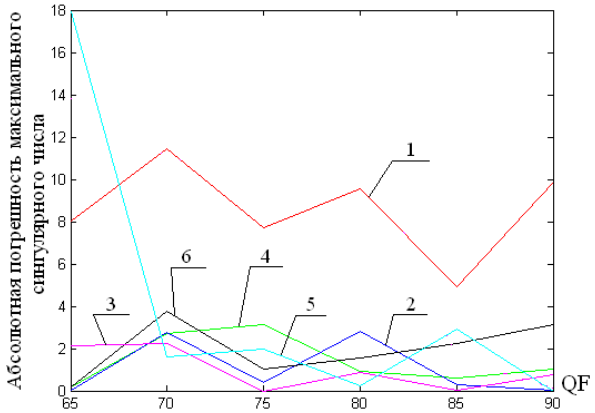
С учетом всего вышесказанного очевидно, что эффективность СП, использующего для погружения ДИ максимальное СНЧ 8×8-блока контейнера, будет выше для контейнеров в форматах с потерями. Данный факт не может рассматриваться как такой, который ограничивает область применимости обсуждаемого СП, поскольку, во-первых, различия в эффективности, как подтверждается вычислительным экспериментом, не являются критическими, а, во-вторых, в настоящий момент наибольшее распространение получили именно форматы с потерями для хранения и пересылки ЦИ, поэтому очевидным является факт большей вероятности использования в качестве контейнера ЦИ в форматах с потерями.

а

B =

34	37	41	39	39	40	41	41
34	36	38	39	39	40	41	41
33	35	36	37	39	40	41	41
33	34	35	37	39	41	41	42
33	34	35	37	37	39	40	41
32	33	34	36	37	37	38	39
33	33	34	35	35	36	37	38
33	33	33	34	35	37	38	39

б



в

Рис. 3. Иллюстрация характера возмущений максимального СНЧ блока при сжатии ЦИ с потерями: а – ЦИ в формате Tif с указанием рассматриваемого блока; б – матрица анализируемого блока ЦИ; в – графики зависимости абсолютной погрешности максимального СНЧ анализируемого блока от величины коэффициента качества QF, использованного при сохранении изображения в формат Jpeg: 1 – для исходного ЦИ (формат Tif); 2 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=67; 3 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=75; 4 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=78; 5 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=90; 6 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=96

Проведенные исследования являются основой для разработки нового СА. Для обеспечения значительной устойчивости СП к атакам против встроенного сообщения (сжатия СС с потерями), в предлагаемом СА, основные шаги которого приведены ниже, погружение одного бита ДИ проводится трижды. Для того, чтобы в этом случае избежать уменьшения пропускной способности скрытого канала связи, предлагается использовать для СП блоки, получаемые в результате стандартного разбиения 8×8-блока.

Погружение ДИ.

Шаг 1. Матрицу F разбить стандартным образом на блоки размером 8×8 пикселей.

Шаг 2. Пусть B очередной блок матрицы ЦИ-контейнера, используемый в процессе СП и определяемый в соответствии с секретным ключом, а p_i – очередной бит ДИ.

2.1. Блок B разбить стандартным образом на 4×4-блоки, три из которых ($B^{(1)}, B^{(2)}, B^{(3)}$) в соответствии с секретным ключом использовать для погружения бита p_i ДИ.

2.2. В каждый из трех выбранных блоков погрузить p_i:

2.2.1. Для матрицы каждого блока $B^{(j)}$, $j=1,2,3$, определить максимальное СНЧ $\sigma_1\left(B^{(j)}\right)$ путем ее сингулярного разложения [7]: $B^{(j)}=U^{(j)}\Sigma^{(j)}V^{(j)T}$, где $U^{(j)},V^{(j)}$ - ортогональные матрицы левых и правых сингулярных векторов $B^{(j)}$, а $\Sigma^{(j)}$ - диагональная матрица, на диагонали которой находятся СНЧ: $\sigma_1\left(B^{(j)}\right)\geq ...\geq\sigma_8\left(B^{(j)}\right)\geq 0$.

2.2.2. Для каждого блока $B^{(j)}$, $j=1,2,3$, заменить 6-й бит $\left[\sigma_1\left(B^{(j)}\right)\right]$ на p_i. Результат – $\overline{\sigma}_1\left(B^{(j)}\right)$.

2.2.3. Для матрицы каждого блока $B^{(j)}$, $j=1,2,3$, сформировать соответствующий блок $\overline{B}^{(j)}$ СС: $\overline{B}^{(j)}=U^{(j)}\overline{\Sigma}^{(j)}V^{(j)T}$, где диагональ матрицы $\overline{\Sigma}^{(j)}$: $diag\left(\overline{\Sigma}^{(j)}\right)=\left(\overline{\sigma}_1\left(B^{(j)}\right),\sigma_2\left(B^{(j)}\right),...,\sigma_8\left(B^{(j)}\right)\right)^T$.

2.3. Сформировать 8×8-блок $\overline{B}$ СС, заменив $B^{(1)},B^{(2)},B^{(3)}$ на $\overline{B}^{(1)},\overline{B}^{(2)},\overline{B}^{(3)}$ соответственно.

Шаг 3.

Если СП не завершено

то переход на шаг 2

иначе матрица ЦИ-стеганосообщения – $\overline{F}$.

Декодирование ДИ.

Пусть $\overline{\overline{F}}$ - матрица ЦИ-СС, которая, в общем случае, может быть отлична от $\overline{F}$ в результате атак против встроенного сообщения (в частности, сжатия СС с потерями).

Шаг 1. Матрицу $\overline{\overline{F}}$ ЦИ-СС разбить стандартным образом на блоки размером 8×8 пикселей.

Шаг 2. Пусть $\overline{\overline{B}}$ очередной блок матрицы ЦИ-СС, который использовался в процессе СП.

2.1. Блок $\overline{\overline{B}}$ разбить стандартным образом на 4×4-блоки, три из которых ($\overline{\overline{B}}^{(1)},\overline{\overline{B}}^{(2)},\overline{\overline{B}}^{(3)}$) выбрать в соответствии с секретным ключом для декодирования очередного бита $\overline{p}_i$ ДИ.

2.2. Декодирование очередного бита $\overline{p}_i$ ДИ:

2.2.1. Для матрицы блока $\overline{\overline{B}}^{(j)}$, $j=1,2,3$, определить максимальное СНЧ $\sigma_1\left(\overline{\overline{B}}^{(j)}\right)$.

2.2.2. Для каждого блока $\overline{\overline{B}}^{(j)}$, $j=1,2,3$, извлечь 6-й бит $\overline{p}_i^{(j)}$ из $\left[\sigma_1\left(\overline{\overline{B}}^{(j)}\right)\right]$.

2.2.3. Значение $\overline{p}_i$ определить в зависимости о того, каких значений среди $\overline{p}_i^{(j)}$, $j=1,2,3$, было больше. Для этого найти сумму $S=\sum_{j=1}^{3}\overline{p}_i^{(j)}$.

Если $S>1$, *то* $\overline{p}_i=1$,

иначе $\overline{p}_i=0$.

Шаг 3.

Если декодирование ДИ не завершено

то переход на шаг 2.

Поскольку для СП используется максимальное СНЧ блока, которое вместе с соответствующими ему СНВ отвечает, главным образом, низкочастотной составляющей соответствующего сигнала, а сжатие возмущает, главным образом,

высокочастотную (и среднечастотную) составляющие, то такой способ погружения ДИ должен обеспечить большую устойчивость к сжатию, чем в тех СА, в которых для СП задействуются среднечастотные коэффициенты, являющиеся определенным компромиссом между требованиями устойчивости алгоритма к сжатию и обеспечения надежности восприятия сответствующего СС [1,7].

Для оценки эффективности разработанного СА был проведен вычислительный эксперимент, в ходе которого декодирование ДИ производилось из СС в условиях его сохранения без потерь, а также в формате Jpeg с различными коэффициентами качества. Результаты эксперимента, в котором были задействованы изображения из множеств M_1, M_2. представлены в табл.2.

Теоретические основы разработанного СА позволили обеспечить его устойчивость не только к атаке сжатием, но и к другим атакам против встроенного сообщения. В табл.3 представлены результаты эксперимента в условиях наложения на стегансообщение гауссовского, мультипликативного шума. Параметры шумов выбирались таким образом, чтобы обеспечить значение $PSNR > 37dB$.

Таблица 2.

Количество ошибок при декодировании ДИ разработанным СА в условиях сохранения СС без/с потерями (%)

Множество ЦИ	Формат, в котором сохраняется СС					
	Tif	Jpeg				
		QF=60	QF=70	QF=75	QF=80	QF=85
M_1	0.0044	4.7	3.6	2.8	2.0	1.6
M_2	0.004	3.6	2.4	1.8	1.1	0.9
Среднее значение	0.004	4.1	2.9	2.3	1.5	1.3

Таблица 3.

Количество ошибок при декодировании ДИ разработанным СА в условиях наложения на СС шума (%)

Множество ЦИ	Шум, накладываемый на СС	
	Гауссовский (нулевое матожидание, D=0.0001); $PSNR = 40dB$	Мультипликативный (D=0.0005); $PSNR = 38dB$
M_1	2.2	2.3
M_2	1.7	3.2
Среднее значение	1.9	2.8

Для сравнительной оценки эффективности разработанного СА, который ниже обозначается *SA,* были использованы следующие современные аналоги, позиционируемые в открытой печати как устойчивые к сжатию: S_1 [14], S_2 [15], S_3 [10] (Метод Коха и Жао, где использованы коэффициенты ДКП (4,5), (5,4)), S_4 [16], S_5 [17], S_6 [18] (использующий амплитудную модуляцию), S_7 [18] (использующий фазовую модуляцию), S_8 [19]. В качестве количественной оценки устойчивости СА к возмущающим воздействиям использовался коэффициент корреляции *NC* для декодированной ДИ, который определяется в соответствии с формулой [20]:

$NC = \sum_{i=1}^{t} p_i' \times \overline{p}_i' \Big/ t$, где $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}, i = \overline{1,t}$ — ДИ, погруженная в контейнер; $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $\overline{p}_i \in \{0,1\}, i = \overline{1,t}$ — декодированная ДИ; $p_i' = 1, \overline{p}_i' = 1$, если $p_i = 1, \overline{p}_i = 1$; $p_i' = -1, \overline{p}_i' = -1$, если $p_i = 0, \overline{p}_i = 0$. Результаты представлены в табл. 4.

Из приведенных результатов очевидно, что разработанный СА по эффективности сравним с современными аналогами в условиях атаки сжатием, а при самых распространеных значениях коэффициента качества QF=75, QF=70 опережает аналоги по эффективности. При этом для QF=75 эффективность повышена по сравнению с лучшим из рассмотренных аналогов (S_7) на 0.5%.

Таблица 4.

Значение NC для различных СА при атаке сжатием на СС с различными коэффициентами качества QF

Стеганоалгоритм	QF (при сохранении СС в формате Jpeg)			
	60	70	75	80
S_1	-	0.57	-	-
S_2	-	0.63	-	-
S_3	0.5316	0.9002	-	0.9846
S_4	-	-	-	0.89
S_5	-	-	-	0.97
S_6	-	-	0.92	-
S_7	-	-	0.95	-
S_8	0.94	0.94	0.94	0.94
SA	0.9168	0.9405	0.954	0.9702

Выводы

В работе на основе метода модификации наименьшего значащего бита разработан СА, устойчивый к атаке сжатием. Вычислительная сложность алгоритма определяется количеством блоков при разбиении матрицы ЦИ и для изображения размером $n \times n$ пикселей составляет $\underline{O}(n^2)$ операций, что делает его перспективным при использовании потокового контейнера. Эффективность разработанного СА в условиях атаки сжатием сравнима с эффективностью современных аналогов, а для наиболее распространенных значений коэффициента качества, используемого при сжатии ЦИ ($QF \in \{70,75\}$), превосходит их. Полученный результат является следствием выбора области ЦИ для СП: максимальных СНЧ 4×4-блоков матрицы изображения, которые в совокупности с соответствующими их сингулярными векторами, отвечают, главным образом, низкочастотной составляющей сигнала, тогда как при сжатии наиболее сильно страдают высокочастотные (среднечастотные) составляющие.

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2009. – 272 с.

2. Кобозева, А.А. Метод повышения устойчивости стеганографических методов к возмущающим воздействиям / А.А.Кобозева // Захист інформації. – 2007. – №1. – С. 53-60.
3. Kozina M.O. Discrete Fourier transform as a basis for steganography method / M.O. Kozina // Праці Одеського політехнічного університету. – 2014. – No. 2(44). – С. 118-126.
4. Ghoshal, N. A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT) / N. Ghoshal, J.K. Mandal // Malaysian Journal of Computer Science. – 2008. – Vol. 21, No. 1. – Pp. 24-32.
5. Ghoshal, N. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT) / N. Ghoshal , J.K. Mandal // Proceedings of ICCS. – 2010. – Pp. 144-150.
6. Ghoshal, N. A Bit Level Image Authentication. Secrete Message Transmission Technique / N.Ghoshal, J. K. Mandal // Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition. – 2008. - Vol. 51, No. 4. - Pp. 1-13.
7. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. – К.: ГУИКТ, 2009. – 251 с.
8. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию/ А.А. Кобозева, М.А. Мельник // Сучасна спеціальна техніка. – 2012. – №4(31). – С. 60-69.
9. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. – 2012. – №2(8). – С. 99-106.
10. Конахович Г.В. Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
11. Hsu Y.F. Detecting image splicing using geometry invariants and camera characteristics consistency / Y.F. Hsu, S.F. Chang // Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'06). – Toronto, 2006. – Pp. 549-552.
12. NRCS Photo Gallery // United States Department of Agriculture. Washington, USA. Mode of access: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).
13. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. – М.: Техносфера, 2006. – 1070 с.
14. Wang, S.H. Wavelet tree quantization for copyright protection watermarking / S.H. Wang, Y.P. Lin // IEEE Transactions on Image Processing. – 2004. – Vol. 13, No. 2. – Pp. 154-165.
15. Li, E. An integer wavelet based multiple logo-watermarking scheme / E. Li, H. Liang, X. Niu // Proceedings of the IEEE WCICA. – 2006. – Pp. 10256-10260.
16. Lu, W. Robust digital image watermarking based on subsampling / W. Lu, H. Lu, F.L. Chung // Applied Mathematics and Computation. – 2006. – Vol. 181, No. 2. – Pp. 886-893.
17. Nasir, I. Subsampling-based image watermarking in compressed DCT domain / I. Nasir // The Tenth IASTED International Conference on Signal and Image Processing (SIP 2008). – Kailua-Kona, Hawaii, USA, 2008. – Pp. 339-344.
18. Колесников, М.В. Метод скрытой передачи данных в оптическом канале видеокамеры [Электронный ресурс] / М.В. Колесников // Инженерный вестник. – М.: ФГБОУ ВПО «МГТУ им. Н.Э. Баумана», 2013. – № 2. – Режим доступа: http://engbul.bmstu.ru/doc/543251.html.
19. Мельник М.А. Повышение устойчивости стеганографической системы к атаке сжатием. – Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. – Одесский национальный политехнический университет, Одесса, 2013. – Режим доступа: http://library.opu.ua/upload/files/library/bezpeka/M_482.pdf.
20. Lin, W.H. A blind watermarking method using maximum wavelet coefficient quantization / W.H. Lin, Y.R. Wang, S.J. Horng // Expert Systems with Applications. – 2009. – No.36. – Pp. 11509-11516.

РОЗРОБКА СТІЙКОГО ДО СТИСКУ СТЕГАНОПЕРЕТВОРЕННЯ ЦИФРОВОГО ЗОБРАЖЕННЯ НА ОСНОВІ МЕТОДУ МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА

А.А. Кобозєва, Т.В. Варда, В.І. Ануфрієв

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net, tomavarda@gmail.com

Стеганографічна система є складовою частиною будь-якої сучасної комплексної системи захисту інформації. Основою стеганосистеми, що визначає її властивості, є використовуваний у ній стеганографічний алгоритм. Робота присвячена підвищенню

стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки на основі методу модифікації найменшого значущого біта стеганографічного алгоритму, стійкого до стиску із втратами. Обґрунтовується вибір області стеганоперетворення - області сингулярного розкладання блоків матриці цифрового зображення-контейнера. З множини параметрів, що визначаються сингулярним розкладанням, процес стеганоперетворення локалізується в максимальних сингулярних числах блоків матриці, отриманих шляхом її стандартної розбивки. Вибір області для вбудови додаткової інформації, у якості якої в роботі виступає бінарна послідовність, сформована випадковим чином, дозволив забезпечити стійкість розробленого стеганоалгоритму не тільки до стиску із втратами, але й до інших атак проти вбудованого повідомлення: гауссівського шуму, мультиплікативного шуму. Показано, що ефективність розробленого алгоритму в умовах атаки стиском порівнянна з ефективністю сучасних аналогів, а для найпоширеніших значень коефіцієнта якості, використовуваного при стиску цифрового зображення (QF=70,75), перевищує їх. Отриманий результат є наслідком вибору області зображення для стеганоперетворення (максимальні сингулярні числа блоків), яка при стиску зазнає незначні збурення, у порівнянні з іншими складовими області сингулярного розкладання відповідних матриць. Розроблений стеганографічний алгоритм є поліноміальним ступеня 2, що робить його перспективним для використання в умовах потокового контейнера.

Ключові слова: цифрове зображення, стеганографічний алгоритм, метод модифікації найменшого значущого біта, максимальне сингулярне число блоку, формат із втратами, формат без втрат.

DEVELOPMENT OF A COMPRESSION-RESISTANT STEGANO-TRANSFORMATION OF A DIGITAL IMAGE BASED ON THE METHOD OF MODIFICATION OF THE LEAST SIGNIFICANT BIT

A.A. Koboseva, T.B. Varda, V.I. Anufriev

Odesa National Polytechnic University,
1 Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net, tomavarda@gmail.com

The steganographic system is an integral part of any modern complex information security system. The basis of the steganosystem, which determines its properties, is the steganographic algorithm used in it. The selection of the stegano-transformation domain based on the domain of singular value decomposition of the matrix blocks of the digital cover image. The stegano-transformation process uses, from the set of singular value decomposition parameters, the largest singular values of matrix blocks, obtained by standard partitioning. The choice of the area for immersion of additional information, which is a randomly generated binary sequence, allowed to provide resistance of the developed steganoalgorithm not only to lossy compression, but also to other attacks against the built-in message: Gaussian noise, multiplicative noise. It is shown that the efficiency of the developed algorithm under the conditions of compression attack is comparable with the efficiency of modern analogs, and for the most common values of the quality factor used in the compression of DI (QF = 70, 75), exceeds them. The obtained result is a consequence of the choice of the DI domain for stegano-transformation (the largest singular values of blocks), which experiences insignificant perturbations in compression in comparison with other components of the singular value decomposition of corresponding matrices. The developed steganographic algorithm is a polynomial degree 2 algorithm, which makes it promising for use in the conditions of the stream container.

Keywords: digital image, steganographic algorithm, method of modification of the least significant bit, maximum singular number of block, lossy format, lossless format.