УДК 004.056.5: 518: 512.624.3

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 3, pp. 248-257

ПОВЫШЕНИЕ СКРЫТОЙ ПРОПУСКНОЙ СПОСОБНОСТИ УСТОЙЧИВЫХ К СЖАТИЮ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ ДЛЯ ПРОИЗВОЛЬНЫХ ИЗОБРАЖЕНИЙ-КОНТЕЙНЕРОВ

М.А. Мельник

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: ritochek@yandex.ua

Разработан стеганографический алгоритм, устойчивый к атаке сжатием, в том числе, с малыми коэффициентами качества. В качестве контейнера используется цифровое изображение, хранимое в произвольном формате. Разработка алгоритма проведена на основе существующих аналогов, математическим базисом которых является общий подход к анализу состояния и технологии функционирования информационных систем. Основным преимуществом нового стеганоалгоритма является увеличение в 6 раз его скрытой пропускной способности, по сравнению с алгоритмами, положенными в его основу. Приведены результаты вычислительного эксперимента, подтверждающие высокую эффективность декодирования погруженной информации в условиях атаки сжатием с малыми коэффициентами качества на стеганосообщение.

Ключевые слова: стеганографический алгоритм, атака сжатием, стеганосообщение, цифровое изображение, симметричная матрица, собственные значения, собственные векторы, спектральное разложение

Введение

Задача разработки стеганографических алгоритмов, устойчивых к распространенной на сегодняшний день атаке сжатием, относящейся к атакам против встроенного сообщения, направленной на разрушение дополнительной информации, является актуальной и нерешенной до конца [1]. Решению этой задачи посвящено много современных научных изысканий, в том числе, [2–4], где автором настоящей работы на базе общего подхода к анализу состояния и технологии функционирования информационных систем [5, 6] были предложены стеганоалгоритмы, использующие в качестве контейнера, или основного сообщения (ОС), цифровые изображения (ЦИ), хранящиеся в произвольном формате, обозначаемые далее $A1$, $A2$, $A3$, устойчивые к атаке сжатием, значительно превосходящие свои современные аналоги (S_1 [7], S_2 [8], S_3 [9], S_4 [10], S_5 [11], S_6 [12], S_7 [13], S_8 [14], S_9 [15], S_{10} [16], S_{11} [17], SS_1, SS_2 [18]) по эффективности декодирования в условиях сжатия со значительными коэффициентами (табл. 1). В [2–4] и настоящей работе атака сжатием на стеганосообщение (СС), являющееся результатом стеганопреобразования, моделируется путем пересохранения СС в формат Jpeg с различными коэффициентами качества QF в общедоступном графическом редакторе IrfanView, эффективность стеганоалгоритма оценивается стандартным образом: при помощи коэффициента корреляции NC для дополнительной информации (ДИ), в качестве которой выступает случайно сформированная бинарная последовательность: $NC = \frac{1}{t}\sum_{i=1}^{t} p_i' \times \overline{p}_i'$, где $p_1, p_2, ..., p_t$;

$\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $p_i, \overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$, — соответственно погруженная и декодированная из стеганосообщения ДИ; $p_i' = 1, \overline{p}_i' = 1$, если $p_i = 1, \overline{p}_i = 1$, и $p_i' = -1, \overline{p}_i' = -1$, если $p_i = 0, \overline{p}_i = 0$, т.е. $p_i' \times \overline{p}_i' \in \{1,-1\}$.

Один из разработанных алгоритмов ($A1$) [2] основан на возмущениях максимальных сингулярных чисел (СНЧ) блоков матрицы контейнера, полученных после ее стандартного разбиения, другой ($A2$) – на sign-нечувствительности левых и правых сингулярных векторов (СНВ) блоков, соответствующих максимальным СНЧ [3], третий ($A3$), являясь комбинацией $A1$ и $A2$ [4], позволил повысить скрытую пропускную способность (СПС) [1] базовых стеганоалгоритмов, составляющую $1/64$ бит/пиксель, в три раза. Однако СПС $3/64$ бит/пиксель, достигнутая в $A3$, оставляет желание и возможность ее повышения.

Таблица 1.

Значение NC для различных стеганоалгоритмов при атаке сжатием с различными коэффициентами качества на стеганосообщение

Стегано-алгоритм	*QF*										
	10	20	25	30	40	50	60	70	75	80	90
S_1	-	-	-	0.15	-	0.28	-	0.57	-	-	1
S_2	0.15	0.34	-	0.52	-	0.52	-	0.63	-	-	0.80
S_3	0.17	0.61	-	0.79	-	0.89	-	0.97	-	-	1
S_4	0.34	0.67	-	0.82	-	0.96	-	0.97	-	-	0.99
S_5	-	-	0.63	-	0.80	0.89	-	-	-	-	-
S_6	-	-	0.801	-	0.828	0.916	-	-	-	-	-
S_7	-	-	-	-	-	-	0.70	0.95	-	0.99	0.99
S_8	-	0.85	-	-	-	0.87	-	-	-	0.90	-
S_9	-	0.84	-	-	-	0.93	-	-	-	0.97	-
S_{10}	0.86	0.95	-	0.95	0.97	0.98	0.98	0.98	-	0.98	0.99
S_{11}	0.42	0.56	-	0.80	0.95	0.95	1	1	-	1	1
SS_1	-	-	0.67	-	-	0.80	-	-	0.92	-	-
SS_2	-	-	0.7	-	-	0.91	-	-	0.95	-	-
$A1$	0.87	0.93	0.94	0.95	0.96	0.98	0.98	0.98	0.98	0.98	0.98
$A2$	0.94	0.95	0.95	0.95	0.95	0.95	0.95	0.96	0.96	0.96	0.96
$A3$	0.90	0.93	0.93	0.93	0.93	0.94	0.94	0.94	0.94	0.94	0.94

Цель статьи и постановка исследований

Целью настоящей работы является разработка полиномиального стеганоалгоритма, устойчивого к атаке сжатием, в том числе при малых коэффициентах качества, на основе алгоритмов, предложенных автором ранее ($A1$, $A2$, $A3$), для повышения СПС организуемого скрытого канала связи, по сравнению с СПС для $A1$, $A2$, $A3$.

Для достижения поставленной цели в работе решаются следующие *задачи*:

1) Увеличения СПС канала скрытой связи за счет виртуальной симметризации матриц блоков ЦИ-контейнера;

2) Оценка вычислительной сложности разработанного стеганоалгоритма.

3) Сравнительная оценка эффективности декодирования ДИ разработанным стеганоалгоритмом в условиях атаки сжатием на стеганосообщение.

Основная часть

Пусть F — $m \times n$-матрица ЦИ-контейнера. В качестве ДИ рассматривается случайно сформированная бинарная последовательность $p_1,...,p_t$, $p_i \in \{0,1\}$, $i = \overline{1,t}$. Пусть B — произвольный 8×8-блок матрицы ОС, полученный после ее стандартного разбиения [19]. Матрице B поставим в соответствии четыре симметричные матрицы B_1, B_2, B_3, B_4 по правилу, называемому далее правилом SB, наглядно представленному на рис. 1 (здесь цифрами 5,6,7 обозначены главная и части побочной диагонали B), отражая относительно главной и побочной диагоналей треугольные части, обозначенные цифрами 1,2,3,4, исходной матрицы соответственно, которые и будем рассматривать ниже как блоки контейнера. Для каждого из полученных виртуальных блоков в силу их симметричности возможно построение нормального спектрального разложения [20]:

$$B_i = U_i \Lambda_i U_i^T, \quad i = \overline{1,4}, \tag{1}$$

где

U_i, $i = \overline{1,4}$, — матрицы ортонормированных лексикографически положительных собственных векторов (СВ),

$\Lambda_i = diag\left(\lambda_1^{(i)},...,\lambda_8^{(i)}\right)$, $i = \overline{1,4}$, — матрицы собственных значений (СЗ) B_i, $i = \overline{1,4}$, соответственно.

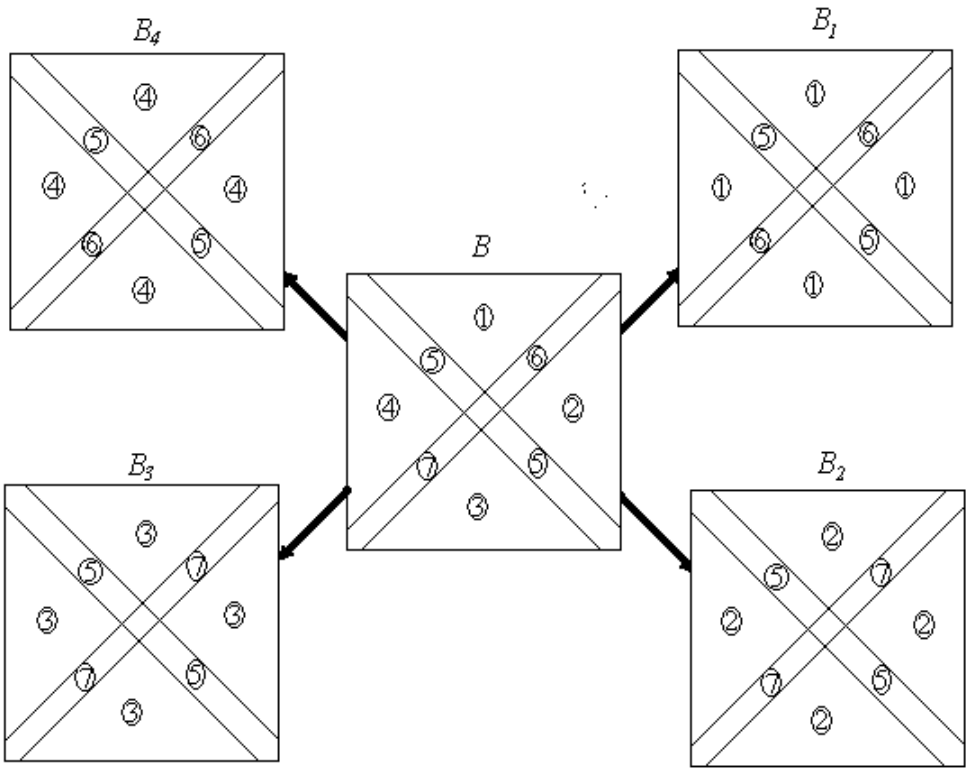

Рис. 1. Правило SB получения симметричных виртуальных блоков матрицы контейнера

По аналогии с $A3$ [4], обозначим K – пороговое значение вариации возмущений максимальных СЗ блоков (в соответствии с [2], учитывая связь между СНЧ и СЗ симметричной матрицы [20], K берется равным 200 для СЗ, как и для СНЧ несимметричных блоков в СА $A1$), $n^o = \left(\frac{1}{\sqrt{8}},...,\frac{1}{\sqrt{8}}\right)^T \in R^8$ — n-оптимальный вектор пространства R^8, обладающий максимальной sign-устойчивостью к произвольным возмущающим воздействиям [6].

Основные шаги предлагаемого стеганоалгоритма, называемого далее $A4$, следующие.

Погружение ДИ.

Шаг 1. Матрица F контейнера разбивается стандартным образом на блоки B размером 8×8. Каждый блок используется для погружения 6 бит ДИ.

Шаг 2. (*Погружение ДИ*). Пусть B — очередной блок с элементами b_{ml}, $m,l=\overline{1,8}$, используемый для стеганопреобразования.

2.1. Каждому блоку B ставятся в соответствии симметричные блоки B_i, $i=\overline{1,4}$, по правилу SB; $p_i, p_{i+1},..., p_{i+5}$ — очередные 6 бит ДИ.

2.2. Строятся нормальные спектральные разложения (1) для B_i, $i=\overline{1,4}$.

2.3.

Если $p_i = 0$,

то $\overline{\lambda}_1^{(1)} = \lambda_2^{(1)} + K\left(n+\frac{1}{4}\right)$,

где n — натуральное число здесь и ниже;

иначе $\overline{\lambda}_1^{(1)} = \lambda_2^{(1)} + K\left(n+\frac{3}{4}\right)$.

2.4.

Если $p_{i+1} = 0$,

то $\overline{\lambda}_1^{(2)} = \lambda_2^{(2)} + K\left(n+\frac{1}{4}\right)$,

иначе $\overline{\lambda}_1^{(2)} = \lambda_2^{(2)} + K\left(n+\frac{3}{4}\right)$.

2.5.

Если $p_{i+2} = 1$,

то 2.5.1 $\overline{u}_1^{(1)} = n^o$,

где $\overline{u}_1^{(1)}$ — возмущенный в ходе СП $u_1^{(1)}$;

2.5.2 Приведение СВ $u_2^{(1)},...,u_8^{(1)}$ блока B_1 к ортонормированному с $\overline{u}_1^{(1)}$ лексикографически положительному виду. Результат – $\overline{u}_2^{(1)},\ldots,\overline{u}_8^{(1)}$.

иначе 2.5.1 $\overline{u}_1^{(2)} = n^o$,

где $\overline{u}_1^{(2)}$ — возмущенный в ходе СП $u_1^{(2)}$;

2.5.2 Приведение СВ $u_2^{(2)},...,u_8^{(2)}$ блока B_2 к ортонормированному с $\overline{u}_1^{(2)}$ лексикографически положительному виду. Результат – $\overline{u}_2^{(2)},...,\overline{u}_8^{(2)}$.

2.6.

Если $p_{i+3} = 0$,

то $\overline{\lambda}_1^{(3)} = \lambda_2^{(3)} + K\left(n + \frac{1}{4}\right)$;

иначе $\overline{\lambda}_1^{(3)} = \lambda_2^{(3)} + K\left(n + \frac{3}{4}\right)$.

2.7.

Если $p_{i+4} = 0$,

то $\overline{\lambda}_1^{(4)} = \lambda_2^{(4)} + K\left(n + \frac{1}{4}\right)$;

иначе $\overline{\lambda}_1^{(4)} = \lambda_2^{(4)} + K\left(n + \frac{3}{4}\right)$.

2.8.

Если $p_{i+5} = 1$,

то 2.8.1 $\overline{u}_1^{(3)} = n^o$,

где $\overline{u}_1^{(3)}$ — возмущенный в ходе СП $u_1^{(3)}$;

2.8.2 Приведение СВ $u_2^{(3)},...,u_8^{(3)}$ блока B_3 к ортонормированному с $\overline{u}_1^{(3)}$ лексикографически положительному виду. Результат – $\overline{u}_2^{(3)},\ldots,\overline{u}_8^{(3)}$.

иначе 2.8.1 $\overline{u}_1^{(4)} = n^o$,

где $\overline{u}_1^{(4)}$ — возмущенный в ходе СП $u_1^{(4)}$;

2.8.2 Приведение СВ $u_2^{(4)},...,u_8^{(4)}$ блока B_2 к ортонормированному с $\overline{u}_1^{(2)}$ лексикографически положительному виду. Результат – $\overline{u}_2^{(4)},...,\overline{u}_8^{(4)}$.

Шаг 3. Формирование блока СС.

3.1.

Если $p_{i+2} = 1$,

то $\overline{B}_1 = \overline{U}_1 \overline{\Lambda}_1 \overline{U}_1{}^T$, $\overline{B}_2 = U_2 \overline{\Lambda}_2 U_2{}^T$,

где $\overline{U}_1 = \left(n^0, \overline{u}_2^{(1)}, \ldots, \overline{u}_8^{(1)}\right)$, $\overline{\Lambda}_1 = diag\left(\overline{\lambda}_1^{(1)},...,\lambda_8^{(1)}\right)$,

$\overline{\Lambda}_2 = diag\left(\overline{\lambda}_1^{(2)},...,\lambda_8^{(2)}\right)$;

иначе $\overline{B}_1 = U_1 \overline{\Lambda}_1 U_1{}^T$, $\overline{B}_2 = \overline{U}_2 \overline{\Lambda}_2 \overline{U}_2{}^T$,

где $\overline{U}_2 = \left(n^0, \overline{u}_2^{(2)}, \ldots, \overline{u}_8^{(2)}\right)$, $\overline{\Lambda}_1 = diag\left(\overline{\lambda}_1^{(1)}, \lambda_2^{(1)},...,\lambda_8^{(1)}\right)$,

$\overline{\Lambda}_2 = diag\left(\overline{\lambda}_1^{(2)}, \lambda_2^{(2)},...,\lambda_8^{(2)}\right)$.

3.2.

Если $p_{i+5} = 1$,

то $\overline{B}_3 = \overline{U}_3 \overline{\Lambda}_3 \overline{U}_3{}^T$, $\overline{B}_4 = U_4 \overline{\Lambda}_4 U_4{}^T$,

где $\overline{U}_3 = \left(n^0, \overline{u}_2^{(3)}, \ldots, \overline{u}_8^{(3)}\right)$, $\overline{\Lambda}_3 = diag\left(\overline{\lambda}_1^{(3)},...,\lambda_8^{(3)}\right)$,

$\overline{\Lambda}_4 = diag\left(\overline{\lambda}_1^{(4)},...,\lambda_8^{(4)}\right)$;

иначе $\overline{B}_3 = U_3 \overline{\Lambda}_3 U_3{}^T$, $\overline{B}_4 = \overline{U}_4 \overline{\Lambda}_4 \overline{U}_4{}^T$,

где $\overline{U}_4 = \left(n^0, \overline{u}_2^{(4)}, \ldots, \overline{u}_8^{(4)}\right)$, $\overline{\Lambda}_3 = diag\left(\overline{\lambda}_1^{(3)},...,\lambda_8^{(3)}\right)$,

$\overline{\Lambda}_4 = diag\left(\overline{\lambda}_1^{(4)},...,\lambda_8^{(4)}\right)$.

3.3. Элементы матриц $\overline{B}_i$, $i = 1,2,3,4,$ обозначим соответственно $\overline{b}_{ml}^{(i)}$, $m,l = \overline{1,8}$. Блок $\overline{B}$ СС будет иметь вид:

$$\overline{B} = \begin{pmatrix} b_{11} & \overline{b}_{12}^{(1)} & \overline{b}_{13}^{(1)} & \overline{b}_{14}^{(1)} & \overline{b}_{15}^{(1)} & \overline{b}_{16}^{(1)} & \overline{b}_{17}^{(1)} & b_{18} \\ \overline{b}_{21}^{(4)} & b_{22} & \overline{b}_{23}^{(1)} & \overline{b}_{24}^{(1)} & \overline{b}_{25}^{(1)} & \overline{b}_{26}^{(1)} & b_{27} & \overline{b}_{28}^{(2)} \\ \overline{b}_{31}^{(4)} & \overline{b}_{32}^{(4)} & b_{33} & \overline{b}_{34}^{(1)} & \overline{b}_{35}^{(1)} & b_{36} & \overline{b}_{37}^{(2)} & \overline{b}_{38}^{(2)} \\ \overline{b}_{41}^{(4)} & \overline{b}_{42}^{(4)} & \overline{b}_{43}^{(4)} & b_{44} & b_{45} & \overline{b}_{46}^{(2)} & \overline{b}_{47}^{(2)} & \overline{b}_{48}^{(2)} \\ \overline{b}_{51}^{(4)} & \overline{b}_{52}^{(4)} & \overline{b}_{53}^{(4)} & b_{54} & b_{55} & \overline{b}_{56}^{(2)} & \overline{b}_{57}^{(2)} & \overline{b}_{58}^{(2)} \\ \overline{b}_{61}^{(4)} & \overline{b}_{62}^{(4)} & b_{63} & \overline{b}_{64}^{(3)} & \overline{b}_{65}^{(3)} & b_{66} & \overline{b}_{67}^{(2)} & \overline{b}_{68}^{(2)} \\ \overline{b}_{71}^{(4)} & b_{72} & \overline{b}_{73}^{(3)} & \overline{b}_{74}^{(3)} & \overline{b}_{75}^{(3)} & \overline{b}_{76}^{(3)} & b_{77} & \overline{b}_{78}^{(2)} \\ b_{81} & \overline{b}_{82}^{(3)} & \overline{b}_{83}^{(3)} & \overline{b}_{84}^{(3)} & \overline{b}_{85}^{(3)} & \overline{b}_{86}^{(3)} & \overline{b}_{87}^{(3)} & b_{88} \end{pmatrix}. \quad (2)$$

Декодирование ДИ.

Шаг 1. Матрица $\overline{F}$ СС разбивается стандартным образом на блоки $\overline{B}$ размером 8×8. Каждый блок используется для декодирования 6 бит ДИ.

Шаг 2. (*Декодирование ДИ*). Пусть $\overline{B}$ — очередной блок, из которого извлекаются биты $\overline{p}_i, \overline{p}_{i+1}, ..., \overline{p}_{i+5}$ ДИ.

2.1. Каждому блоку $\overline{B}$ ставятся в соответствии симметричные блоки $\overline{B}_i$, $i = \overline{1,4}$, в соответствии с правилом SB.

2.2. Строятся нормальные спектральные разложения вида (1).

$$\overline{B}_i = \overline{U}_i \overline{\Lambda}_i \overline{U}_i{}^T, \quad i = \overline{1,4}.$$

2.3.

Если $\mathrm{mod}\left(\left[\overline{\lambda}_1^{(1)} - \overline{\lambda}_2^{(1)}\right], K\right) < \dfrac{K}{2}$,

где $[\bullet]$ — целая часть аргумента;

то $\overline{p}_i = 0$;

иначе $\overline{p}_i = 1$.

2.4.

Если $\mathrm{mod}\left(\left[\overline{\lambda}_1^{(2)} - \overline{\lambda}_2^{(2)}\right], K\right) < \dfrac{K}{2}$;

то $\overline{p}_{i+1} = 0$;

иначе $\overline{p}_{i+1} = 1$.

2.5. Найти UN_1 и UN_1 — углы между векторами $\overline{u}_1^{(1)}$ и n^o, $\overline{u}_1^{(2)}$ и n^o соответственно.

Если $UN_1 < UN_2$;

то $\overline{p}_{i+2} = 1$;

иначе $\overline{p}_{i+2} = 0$.

2.6.

Если $\mathrm{mod}\left(\left[\overline{\lambda}_1^{(3)} - \overline{\lambda}_2^{(3)}\right], K\right) < \dfrac{K}{2}$;

то $\overline{p}_{i+3} = 0$;

иначе $\overline{p}_{i+3} = 1$.

2.7.

Если $\mathrm{mod}\left(\left[\overline{\lambda}_1^{(4)} - \overline{\lambda}_2^{(4)}\right], K\right) < \frac{K}{2}$;

то $\overline{p}_{i+4} = 0$;

иначе $\overline{p}_{i+4} = 1$.

2.8. Найти UN_3 и UN_4 - углы между векторами $\overline{u}_1^{(3)}$ и n^o, $\overline{u}_1^{(4)}$ и n^o соответственно.

Если $UN_3 < UN_4$;

то $\overline{p}_{i+5} = 1$;

иначе $\overline{p}_{i+5} = 0$.

Замечание 1. Вычислительная сложность разработанного стеганоалгоритма $A4$ определяется количеством блоков матрицы F ЦИ-контейнера, получаемых в результате ее стандартного разбиения, и в случае, когда матрица имеет размеры $n \times n$ пикселей, будет оцениваться как $\underline{O}\left(n^2\right)$ операций.

Замечание 2. В алгоритме $A4$ в качестве виртуальных блоков матрицы контейнера используются симметричные блоки. Это требование не является обязательным, т.е. матрице блока B не обязательно ставить в соответствие блоки B_1, B_2, B_3, B_4 по правилу, отраженному на рис. 1. Однако, основной вычислительный шаг при обработке каждого блока контейнера в $A4$ – это построение спектрального разложения, которое, в случае несимметричности блоков B_1, B_2, B_3, B_4 целесообразно будет заменить на сингулярное разложение, что, как известно, потребует больше вычислительных затрат для своей реализации [20], а потому является нежелательным.

Замечание 3. Учитывая вид (2) блока СС, а именно предложенный способ построения главной и побочной диагоналей (они остаются неизменными по сравнению с диагоналями контейнера), очевидным является увеличение вычислительной погрешности при формировании СС в $A4$ по сравнению с $A1$, $A2$, $A3$, и предсказуемым ухудшение эффективности. Такой результат является своеобразной «платой» за увеличение СПС соответствующего скрытого канала связи по сравнению с аналогичным параметром для $A1$, $A2$, $A3$.

Результаты сравнения эффективностей декодирования ДИ стеганоалгоритмов $A1$, $A2$, $A3$, $A4$ в условиях атаки сжатием на СС с различными коэффициентами качества для контейнеров в формате TIF представлены на рис. 2.

Из результатов эксперимента видно, что эффективность $A4$ действительно несколько уступает алгоритмам $A1$, $A2$, $A3$, но остается достаточно высокой по сравнению с другими современными аналогами, использованными для сравнения (табл. 1), особенно при малых QF. При этом разработанный стеганоалгоритм $A4$ имеет скрытую пропускную способность, превосходящую СПС $A1$, $A2$ в 6 раз, $A3$ – в два раза, и составляет $3/32$ бит/пиксель.

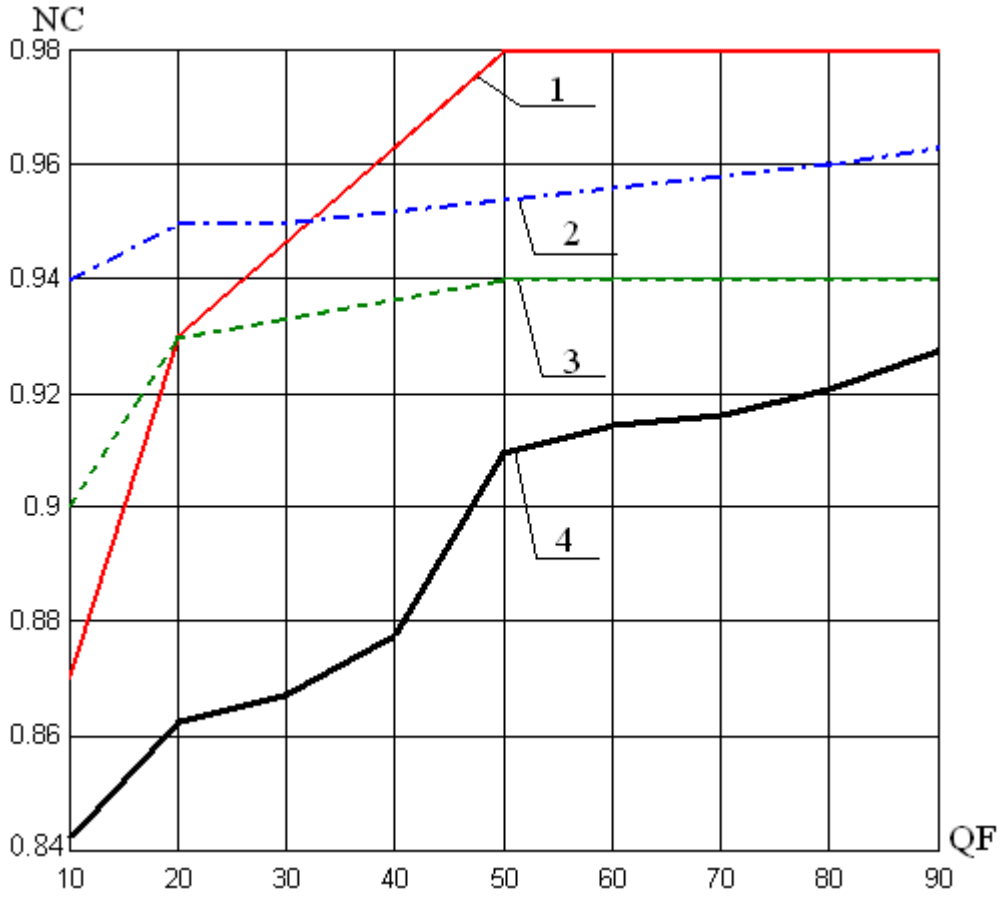

Рис. 2. Эффективность декодирования ДИ разработанными стеганоалгоритмами: 1 – $A1$; 2 – $A2$; 3 – $A3$; 4 – $A4$

Заключение

В настоящей работе разработан стеганографический алгоритм $A4$, устойчивый к сжатию со значительными коэффициентами: так для $QF = 10$ среднее значение $NC > 0.84$, при этом скрытая пропускная способность канала связи, организуемого при помощи $A4$, составила $3/32$ бит/пиксель, что в 6 раза превысило СПС $A1$, $A2$, положенных в его основу. Вычислительная сложность алгоритма составила $\underline{O}\left(n^2\right)$ операций.

Основным возмущающим воздействием для получаемого при помощи $A4$ стеганосообщения, очевидно является процесс округлений, происходящий после СП. Это заключение определяет направление дальнейших исследований автора: организации процесса СП таким образом, чтобы уменьшить вычислительную погрешность при построении СС.

Список литературы

1. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
2. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. — 2012. — № 2(8). — С. 99–106.

3. Мельник, М.А. Sign-нечувствительность сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / М.А. Мельник // Інформатика та математичні методи в моделюванні. — 2013. — Том 3, № 2. — С. 146–155.
4. Мельник, М.А. Повышение скрытой пропускной способности стеганографических алгоритмов, устойчивых к атаке сжатием / М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. — 2013. — Вип. 41. — С. 56–62.
5. 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.
6. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А. Кобозева, М.А. Мельник // Збірник наукових праць Військового інституту Київського нац-го ун-ту ім. Т.Шевченка. — 2012. — Вип. 38. — С. 193–203.
7. Wang, S.H. Wavelet tree quantization for copyright protection watermarking / S.H. Wang, Y.P. Lin // IEEE Transactions on Image Processing. — 2004. — Vol. 13, Iss. 2. — PP. 154–165.
8. 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.
9. Lien, B.K. A watermarking method based on maximum distance wavelet tree quantization / B.K. Lien, W.H. Lin // Proceedings of the 19th Conference on Computer Vision, Graphics and Image Processing. – 2006. – PP. 269–276.
10. Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin *et al.* // Expert Systems with Applications. — 2009. — Vol. 36, Iss. 9. — PP. 11509–11516.
11. Li, C. A novel watermarking scheme for image authentication in DWT domain / C. Li, H. Song // Proceedings of 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication (ASID'09), Hong Kong, 20–22 Aug. 2009. — 2009. — PP. 160–162.
12. Peng, L. A blind image watermarking scheme based on wavelet tree quantization / L. Peng, D. Zhizhong // Second International Symposium on Electronic Commerce and Security (ISECS'09), 22–24 May 2009, Nanchang. — 2009. — Vol. 1. — PP. 218–222.
13. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
14. Lu, W. Robust digital image watermarking based on subsampling / W. Lu, H. Lu, F.-L. Chung // Applied Mathematics and Computation. — 2006. — Vol. 181, Iss. 2. — PP. 886–893.
15. Nasir, I. Subsampling-based image watermarking in compressed DCT domain / I. Nasir *et al.* // The Tenth IASTED International Conference on Signal and Image Processing (SIP 2008), August 18 – 20, 2008, Kailua-Kona, Hawaii, USA. — 2008. — PP. 339–344.
16. 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.
17. Shahraeini, S. A Robust Digital Image Watermarking Approach against JPEG Compression Attack Based on Hybrid Fractal-Wavelet / S.Shahraeini, M.Yaghoobi // Proceedings of 8th International Conference on Computer Science and Information Technologies (CSIT 2011), 26–30 September, 2011, Yerevan, Armenia. — 2011. — Vol. 5. — PP. 616–622.
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. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
20. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.

ПІДВИЩЕННЯ ПРИХОВАНОЇ ПРОПУСКНОЇ СПРОМОЖНОСТІ СТІЙКИХ ДО СТИСКУ СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ ДЛЯ ДОВІЛЬНИХ ЗОБРАЖЕНЬ-КОНТЕЙНЕРІВ

М.О. Мельник

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: ritochek@yandex.ua

Розроблений стеганографічний алгоритм, стійкий до атаки стиском, у тому числі, з малими коефіцієнтами якості. Як контейнер використовується цифрове зображення, збережене в довільному форматі. Розробка алгоритму проведена на основі існуючих аналогів, математичним базисом яких є загальний підхід до аналізу стану й технології функціонування інформаційних систем. Основною перевагою нового стеганоалгоритму є збільшення в 6 разів його прихованої пропускної спроможності, у порівнянні з алгоритмами, покладеними в його основу. Наведені результати обчислювального експерименту, що підтверджують високу ефективність декодування вбудованої інформації в умовах атаки стиском з малими коефіцієнтами якості на стеганоповідомлення.

Ключові слова: стеганографічний алгоритм, атака стиском, стеганоповідомлення, цифрове зображення, симетрична матриця, власні значення, власні вектори, спектральне розкладання

INCREASE STEGANOGRAPHIC CAPACITY OF COMPRESSIVE STRENGTH ALGORITHMS FOR ARBITRARY COVER IMAGES

Margaret A. Melnik

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: ritochek@yandex.ua

Developed steganographic algorithm is compressive strength algorithms for arbitrary cover images including attacks with low quality factor. Cover is digital image stored in arbitrary format. Development of proposed algorithm based on existing analogues that based on general approach to the analysis of the status and technology functioning of information systems. The main advantage of the new steganographic algorithm is 6 times increase of its capacity, compared with the algorithms which it is based. The results of computational experiment confirming the high performance decoding of embedded information by compression attacks with low quality factor.

Keywords: steganographic algorithm, compression attack, stegano message, digital image, symmetric matrix, eigenvalues, eigenvectors, spectral decomposition