УДК 004.056.5: 518: 512.624.3 **Мельник М.А.** (ОНПУ)

ПОВЫШЕНИЕ СКРЫТОЙ ПРОПУСКНОЙ СПОСОБНОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ, УСТОЙЧИВЫХ К АТАКЕ СЖАТИЕМ

У роботі запропоновано стеганографічний алгоритм, стійкий до атаки стиском, побудований на основі алгоритмів, розроблених автором раніше. Використання віртуальної симетричності блоків матриці контейнера дозволило підвищити приховану пропускну спроможність каналу зв'язку в три рази, в порівнянні з аналогічним параметром для алгоритмів, що використовуються в основі. Наведені результати обчислювального експерименту, які показують високу ефективність розробленого стеганоалгоритма.

Ключові слова: стеганографічний алгоритм, атака стиском, симетрична матриця, власне значення, власний вектор

Введение. Развитие современных информационных технологий привело к разработке различных методов, предназначенных для обеспечения безопасной передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Стеганографические методы, наряду с криптографическими, занимают важное место среди методов защиты информации [1,2]. Но если в криптографии наличие шифрованного сообщения само по себе привлекает внимание противников, то стеганография не предусматривает прямого оглашения факта существования защищаемой информации.

Общей чертой стеганографических алгоритмов является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый безобидный, не привлекающий внимание объект, или контейнер [3]. Процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС). Полученное СС пересылается адресату по открытому каналу связи или хранится в таком виде.

К любому стеганографическому алгоритму (СА) предъявляется ряд требований, основными из которых являются: обеспечение надежности восприятия СС [3,4]; требование устойчивости к преднамеренным (непреднамеренным) атакам [3,4]; обеспечение значительной скрытой пропускной способности (СПС) организуемого канала связи [4].

Проблеме создания устойчивых алгоритмов в современной печати уделено много внимания, однако вопрос создания СА, устойчивых к атаке сжатием, которая является чрезвычайно распространенной благодаря популярности использования форматов с потерями для хранения и передачи цифровых сигналов (в частности цифровых изображений (ЦИ), которые далее рассматриваются в качестве ОС), остается актуальным и на сегодняшний день [1].

В [5,6] автором настоящей работы на базе теории возмущений и матричного анализа [7,8] были разработаны СА, устойчивые к сжатию со значительными коэффициентами, один из которых основан на возмущениях максимальных сингулярных чисел (СНЧ) блоков матрицы контейнера, полученных после ее стандартного разбиения (далее будем его обозначать $A1$) [5], другой (обозначаемый далее $A2$) – на sign-нечувствительности левых и правых сингулярных векторов (СНВ) блоков, соответствующих максимальным СНЧ [6]. Недостатком обоих алгоритмов является малая СПС - $1/64$ бит/пиксель.

Цель статьи и постановка исследований. *Целью* настоящей работы является разработка стеганоалгоритма, устойчивого к атаке сжатием, на основе алгоритмов, предложенных автором ранее ($A1$, $A2$), для повышения СПС организуемого скрытого канала связи, по сравнению с СПС для $A1$, $A2$.

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

1. Определение возможности увеличения СПС канала скрытой связи за счет виртуального изменения свойств матриц блоков ЦИ-контейнера;
2. Анализ эффективности разработанного СА, сравнение его эффективности с $A1$, $A2$.

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 [9]. Матрице B поставим в соответствии две симметричные матрицы [10]:

$$B = \begin{pmatrix} b_{11}\ b_{12}\ b_{13}...b_{18} \\ b_{21}\ b_{22}\ b_{23}...b_{28} \\ b_{31}\ b_{32}\ b_{33}...b_{38} \\ \cdots\cdots\cdots\cdots \\ b_{81}\ b_{82}\ b_{83}...b_{88} \end{pmatrix} \to B_V = \begin{pmatrix} b_{11}\ b_{12}\ b_{13}...b_{18} \\ b_{12}\ b_{22}\ b_{23}...b_{28} \\ b_{13}\ b_{23}\ b_{33}...b_{38} \\ \cdots\cdots\cdots\cdots \\ b_{18}\ b_{28}\ b_{38}...b_{88} \end{pmatrix}, \quad B_N = \begin{pmatrix} b_{11}\ b_{21}\ b_{31}...b_{81} \\ b_{21}\ b_{22}\ b_{32}...b_{82} \\ b_{31}\ b_{32}\ b_{33}...b_{83} \\ \cdots\cdots\cdots\cdots \\ b_{81}\ b_{82}\ b_{83}...b_{88} \end{pmatrix}, \qquad (1)$$

которые и будем рассматривать ниже как блоки контейнера. Для каждого из полученных виртуальных блоков в силу их симметричности возможно построение нормального спектрального разложения [10]:

$$B_V = U_V \Lambda_V U_V{}^T,\ B_N = U_N \Lambda_N U_N{}^T, \qquad (2)$$

где U_V, U_N - матрицы ортонормированных лексикографически положительных собственных векторов (СВ), $\Lambda_V = diag\left(\lambda_1{}^{(V)},...,\lambda_8{}^{(V)}\right), \Lambda_N = diag\left(\lambda_1{}^{(N)},...,\lambda_8{}^{(N)}\right)$ - матрицы собственных значений (СЗ) B_V, B_N соответственно. В соответствии с теоремой Фробениуса [11] матрицы B_V, B_N (неразложимые неотрицательные) имеют положительные СЗ $\overline{\lambda}_V, \overline{\lambda}_N$, являющиеся простыми корнями соответствующих матрицам B_V, B_N характеристических уравнений. Модули всех других СЗ B_V, B_N не превосходят $\overline{\lambda}_V, \overline{\lambda}_N$. Собственным значениям $\overline{\lambda}_V, \overline{\lambda}_N$ отвечают СВ $\overline{u}(B_V), \overline{u}(B_N)$ с положительными координатами. Для определенности предположим, что $\lambda_1{}^{(V)} \geq ... \geq \lambda_8{}^{(V)}$, $\lambda_1{}^{(N)} \geq ... \geq \lambda_8{}^{(N)}$, т.е. $\overline{\lambda}_V = \lambda_1{}^{(V)}$, $\overline{\lambda}_N = \lambda_1{}^{(N)}$. Соответствующие этим СЗ собственные векторы - $u_1{}^{(V)}$, $u_1{}^{(N)}$.

Обозначим K - пороговое значение вариации возмущений максимальных СЗ блоков (в соответствии с [5], учитывая связь между СНЧ и СЗ симметричной матрицы [12], K берется равным 200 для СЗ, как и для СНЧ несимметричных блоков в СА $A1$), n^o - n-оптимальный вектор пространства R^8 [8], $n^o = \left(\frac{1}{\sqrt{8}},...,\frac{1}{\sqrt{8}}\right)^T \in R^8$.

Основные шаги предлагаемого СА, называемого далее $A3$, следующие.

Погружение ДИ.

Шаг 1. Матрица F контейнера разбивается стандартным образом на блоки B размером 8×8. Каждый блок используется для погружения 3 бит ДИ.

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

2.1. Каждому блоку B ставятся в соответствии симметричные блоки B_V, B_N по правилу (1). p_i, p_{i+1}, p_{i+2} - очередные 3 бита ДИ.

2.2. Строятся нормальные спектральные разложения (2) для B_V, B_N;

2.3. ***Если*** $p_i = 0$

то $\overline{\lambda}_1{}^{(V)} = \lambda_2{}^{(V)} + K\left(n + \frac{1}{4}\right)$, где n - натуральное число здесь и ниже;

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

2.4. ***Если*** $p_{i+1} = 0$

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

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

2.5. ***Если*** $p_{i+2} = 1$,

то

2.5.1. $\overline{u}_1^{(V)} = n^o$, где $\overline{u}_1^{(V)}$ - возмущенный в ходе СП $u_1^{(V)}$

2.5.2. Приведение СВ $u_2^{(V)},...,u_8^{(V)}$ блока B_V к ортонормированному с $\overline{u}_1^{(V)}$ лексикографически положительному виду [6]. Результат - $\overline{u}_2^{(V)},...,\overline{u}_8^{(V)}$.

иначе

2.5.1. $\overline{u}_1^{(N)} = n^o$, где $\overline{u}_1^{(N)}$ - возмущенный в ходе СП $u_1^{(N)}$

2.5.2. Приведение СВ $u_2^{(N)},...,u_8^{(N)}$ блока B_N к ортонормированному с $\overline{u}_1^{(N)}$ лексикографически положительному виду [6]. Результат - $\overline{u}_2^{(N)},...,\overline{u}_8^{(N)}$.

Шаг 3. (*Формирование блока СС*).

3.1. ***Если*** $p_{i+2} = 1$,

то $\overline{B}_V = \overline{U}_V \overline{\Lambda}_V \overline{U}_V^T$, $\overline{B}_N = U_N \overline{\Lambda}_N U_N^T$,

где $\overline{U}_V = (n^o, \overline{u}_2^{(V)},...,\overline{u}_8^{(V)})$, $\overline{\Lambda}_V = diag\left(\overline{\lambda}_1^{(V)}, \lambda_2^{(V)},...,\lambda_8^{(V)}\right)$,

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

иначе $\overline{B}_V = U_V \overline{\Lambda}_V U_V^T$, $\overline{B}_N = \overline{U}_N \overline{\Lambda}_N \overline{U}_N^T$,

где $\overline{U}_N = (n^o, \overline{u}_2^{(N)},...,\overline{u}_8^{(N)})$, $\overline{\Lambda}_V = diag\left(\overline{\lambda}_1^{(V)}, \lambda_2^{(V)},...,\lambda_8^{(V)}\right)$,

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

3.2. Элементы матриц $\overline{B}_V$ и $\overline{B}_N$ обозначим соответственно $\overline{b}_{ij}^{(V)}$, $\overline{b}_{ij}^{(N)}$, $i, j = \overline{1,8}$.

Блок $\overline{B}$ СС будет иметь вид:

$$\overline{B} = \begin{pmatrix} b_{11}^{(d)} & \overline{b}_{12}^{(V)} & \overline{b}_{13}^{(V)} & ... & \overline{b}_{18}^{(V)} \\ \overline{b}_{21}^{(N)} & b_{22}^{(d)} & \overline{b}_{23}^{(V)} & ... & \overline{b}_{28}^{(V)} \\ \overline{b}_{31}^{(N)} & \overline{b}_{32}^{(N)} & b_{33}^{(d)} & ... & \overline{b}_{38}^{(V)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \overline{b}_{81}^{(N)} & \overline{b}_{82}^{(N)} & \overline{b}_{83}^{(N)} & ... & b_{88}^{(d)} \end{pmatrix}. \quad (3)$$

Вычисление элементов, стоящих на главной диагонали $\overline{B}$, обсуждается ниже.

Декодирование ДИ.

Шаг 1. Матрица $\overline{F}$ СС разбивается стандартным образом на блоки $\overline{B}$ размером 8×8. Каждый блок используется для декодирования 3 бит ДИ.

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

2.1. Каждому блоку ставятся в соответствии симметричные блоки $\overline{B}_V, \overline{B}_N$ по правилу (1).

2.2. Строятся нормальные спектральные разложения вида (2):

$$\overline{B}_V = \overline{U}_V \overline{\Lambda}_V \overline{U}_V{}^T,\ \overline{B}_N = \overline{U}_N \overline{\Lambda}_N \overline{U}_N{}^T.$$

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

то $\overline{p}_i = 0$;

иначе $\overline{p}_i = 1$.

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

то $\overline{p}_{i+1} = 0$;

иначе $\overline{p}_{i+1} = 1$.

2.5.Найти UN_V и UN_N - углы между векторами $\overline{u}_1{}^{(V)}$ и n^o, $\overline{u}_1{}^{(N)}$ и n^o соответственно.

Если $UN_V < UN_N$,

то $\overline{p}_{i+2} = 1$,

иначе $\overline{p}_{i+2} = 0$.

Для вычисления диагональных элементов в (3) рассматривались варианты: способ 1 – диагональ $\overline{B}$ совпадает с диагональю B; способ 2 – элементы диагональ $\overline{B}$ равны среднему арифметическому между соответствующими элементами $\overline{B}_V$ и $\overline{B}_N$; способ 3 – диагональ $\overline{B}$ совпадает с диагональю $\overline{B}_V$, если $\overline{B}_V = \overline{U}_V \overline{\Lambda}_V \overline{U}_V{}^T$ (т.е. $p_{i+2} = 1$), с диагональю $\overline{B}_N$, если $\overline{B}_N = \overline{U}_N \overline{\Lambda}_N \overline{U}_N{}^T$ ($p_{i+2} = 0$).

Для выбора способа получения диагональных элементов $b_{ii}{}^{(d)}, i = \overline{1,8}$, блока $\overline{B}$ СС был проведен вычислительный эксперимент, где были задействованы 400 ЦИ из базы NRCS [13] (по 200 ЦИ в форматах JPEG, TIF), которая традиционно используется для тестирования стеганографических алгоритмов. При этом для оценки эффективности декодирования использовался коэффициент декодирования ДИ P, который вычислялся в соответствии с формулой:

$$P = \frac{t - \sum_{i=1}^{t} p_i \oplus \overline{p}_i}{t} \cdot 100\%,$$

где $\oplus$ - операция логического исключающего ИЛИ, $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $\overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$, - декодированное из СС секретное сообщение. Атака сжатием моделировалась в среде Adobe Photoshop путем сохранения СС в формат JPEG с различными коэффициентами качества Q. Будем говорить, что сжатие ЦИ проводится со значительным коэффициентом (или низким коэффициентом качества), если $Q \le 7$. Результаты эксперимента представлены в таблице 1.

Из результатов вычислительного эксперимента вытекает:

- при формировании блока СС целесообразно для вычисления элементов главной диагонали использовать способ 3;

• наибольшее возмущение погруженная ДИ получает в процессе формирования СС (накопление вычислительной погрешности), а не в процессе последующего сжатия;

• эффективность $A3$ не зависит от формата используемого контейнера.

Результат сравнения эффективности стеганоалгоритмов $A1$, $A2$, $A3$ (способ 3) для контейнеров в формате TIF, представлен на рис.1.

Таблица 1

Зависимость коэффициента декодирования ДИ P от значения коэффициента качества Q, используемого при атаке сжатием на СС, при различных способах определения диагональных элементов блока СС в алгоритме $A3$

Формат хранения ЦИ-контейнера	Способ получения диагональных элементов $\overline{B}$	Среднее значение P при различных значениях коэффициента качества Q, используемого при сжатии СС (%)		
		$Q=12$	$Q=7$	$Q=2$
TIF	1	89.63	87.12	86.11
	2	88.97	86.00	83.77
	3	94.01	93.74	93.17
JPEG	1	88.04	87.17	85.71
	2	87.75	84.17	84.05
	3	94.09	93.60	92.97

Из результатов эксперимента видно, что эффективности декодирования в условиях атаки сжатием на СС всех трех разработанных стеганоалгоритмов являются высокими и сравнимыми между собой. И хотя $A3$ несколько уступает $A2$ и $A1$ для $Q \geq 5$, это ухудшение является предсказуемым (в $A3$ вычислительная погрешность очевидно окажется больше при формировании СС, чем в $A2$ и $A1$) и незначительным, особенно при $Q < 5$, но СПС для $A3$ в три раза больше, чем для $A2$ и $A1$, и составляет $3/64$ бит/пиксель.

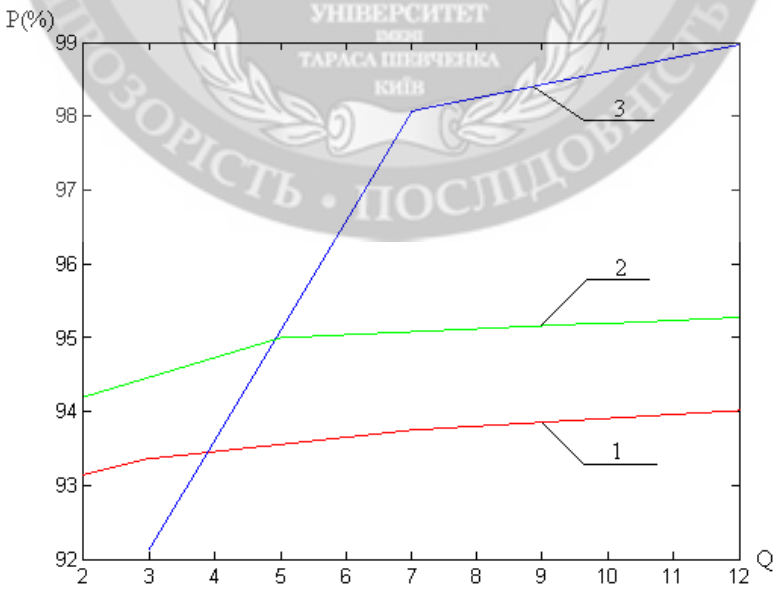

Рис.1. Эффективность декодирования ДИ стеганоалгоритмами: 1 - $A3$; 2 - $A2$; 3 - $A1$

Вывод. В настоящей работе предложен стеганографический алгоритм, устойчивый к сжатию со значительными коэффициентами: так для $Q=2$ среднее значение коэффициента

декодирования ДИ превысило 93%, причем устойчивость алгоритма не зависит от формата используемого ЦИ-контейнера. Устойчивость $A3$ сравнима с устойчивость стеганоалгоритмов, положенных в его основу, хотя в абсолютном значении несколько уступает им, однако СПС канала связи, организуемого при помощи $A3$, составила $3/64$ бит/пиксель, что в 3 раза превысило СПС $A1$, $A2$.

Основным возмущающим воздействием для получаемого при помощи $A3$ стеганосообщения, отрицательно сказывающимся на декодировании ДИ, как свидетельствуют результаты эксперимента, является не процесс сжатия, а процессы округлений, происходящие после СП, очевидно связанные с определением диагонали $\overline{B}$, а также введением значений элементов $\overline{B}$ в диапазон целых значений от 0 до 255. В последующем процессе сжатия дальнейшее уменьшение коэффициента декодирования информации практически не происходит. Это заключение определяет направление дальнейших исследований автора: организации процесса СП таким образом, чтобы уменьшить вычислительную погрешность в процессе формирования СС.

ЛИТЕРАТУРА:

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

2. Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. – К.: Арий, 2008.

Т.2: Информационная безопасность. – 2008. – 344 с.

3. Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А.Кобозєва, І.О.Мачалін, В.О.Хорошко. – К.: Вид. ДУІКТ, 2010. – 316 с.

4. Грибунин В.Г. Цифровая стеганография / В.Г.Грибунин, И.Н.Оков, И.В.Туринцев. – М.: Солон-Пресс, 2002. – 272с.

5. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию / М.А.Мельник // Інформаційна безпека. – 2012. – №2(8). – С. 99-106.

6. 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. – Т.3, №1. – С. 21–30.

7. 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.

8. 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 національного університету ім.Т.Шевченка. – 2012. – Вип.38. – С.193–203.

9. Гонсалес Р. Цифровая обработка изображений / Р.Гонсалес, Р.Вудс; пер. с англ. под ред. П.А.Чочиа. – М.: Техносфера, 2005. – 1072 с.

10.Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах / А.А.Кобозева // Вісник Східноукраїнського нац-го ун-ту ім. В. Даля. – 2006. – №9(103), ч.1. – С.74–82.

11.Гантмахер Ф.Р. Теория матриц / Ф.Р.Гантмахер. – М.: Наука, 1988. – 552 с.

12.Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х.Д.Икрамова. – М.: Мир, 2001. – 430 с.

13.http://photogallery.nrcs.usda.gov

Рецензент: д.т.н., проф. Хорошко В.О., Національний авіаційний університет

Мельник М.О.

ПОВЫШЕНИЕ СКРЫТОЙ ПРОПУСКНОЙ СПОСОБНОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ, УСТОЙЧИВЫХ К АТАКЕ СЖАТИЕМ

В работе предложен стеганографический алгоритм, устойчивый к атаке сжатием, построенный на основе алгоритмов, разработанных автором ранее. Использование виртуальной симметричности блоков матрицы контейнера позволило повысить скрытую пропускную способность организуемого канала связи в три раза, по сравнению с аналогичным параметром для алгоритмов, используемых в качестве основы. Приведены результаты вычислительного эксперимента, показывающие высокую эффективность разработанного стеганоалгоритма.

Ключевые слова: стеганографический алгоритм, атака сжатием, симметричная матрица, собственные значения, собственные векторы

Melnik M.

INCREASE HIDDEN CHANNEL CAPACITY OF STEGANOGRAPHIC ALGORITHMS THAT STABLE TO COMPRESSION ATTACKS

Steganographic algorithm stable to compression attacks based on previous author's works is proposed. Using virtual symmetric matrix blocks of cover allowed to increase the hidden channel capacity three times, compared to the same parameter for the algorithms used as a basis. The results of computer simulation are given.

Keywords: steganographic algorithm, compression attacks, symmetric matrix, eigenvalues, eigenvectors