УДК 004.056.5: 518: 512.624.3

Informatics and Mathematical Methods in Simulation
Vol. 7 (2017), No. 1-2, pp. 19-28

# УСОВЕРШЕНСТВОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА, ОСНОВАННОГО НА SIGN-НЕЧУВСТВИТЕЛЬНОСТИ СИНГУЛЯРНЫХ ВЕКТОРОВ БЛОКОВ МАТРИЦЫ ИЗОБРАЖЕНИЯ

**А.А. Кобозева, В.А. Мокрицкий, Л.Е.М. Батиене, И.И. Бобок**

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

В работе предложен способ обработки цифрового изображения, результатом которой является понижение числа обусловленности большинства блоков его матрицы, полученных путем стандартного разбиения, за счет предобуславливания соответствующих матриц. Обработка сохраняет надежность восприятия искаженного изображения, которая в работе количественно оценивается при помощи пикового отношения «сигнал-шум». Использование предложенного способа обработки в качестве предобработки изображения-контейнера перед стеганопреобразованием позволяет расширить область применимости устойчивого к атакам против встроенного сообщения, в том числе значительным, стеганографического алгоритма, основанного на sign-нечувствительности сингулярных векторов блоков матрицы цифрового изображения, соответствующих максимальным сингулярным числам, разработанного одним из автором ранее. Предобуславливание матрицы блока происходит после его предварительного кодирования. Результатом предварительного кодирования являются 2 симметричные положительно определенные разреженные матрицы, которые ставятся в соответствие блоку изображения. Положительная определенность и разреженность полученных матриц дает возможность использовать в качестве предобуславливателя для них неполное разложение Холесского. Приведены результаты вычислительного эксперимента.

**Ключевые слова:** стеганографический алгоритм, цифровое изображение, предобуславливатель, неполное разложение Холесского, число обусловленности

## Введение

Развитие и совершенствование комплексной системы защиты информации сегодня невозможно без наличия в ее составе эффективной стеганографической системы. Современная стеганография переживает этап своего бурного развития, при этом требования, выдвигаемые к стеганографическим алгоритмам, используемым при организации скрытого канала связи, становятся все более жесткими: обеспечение надежности восприятия формируемого стеганосообщения (СС), устойчивость к атакам против встроенного сообщения, устойчивость к стеганоанализу, обеспечение достаточной пропускной способности скрытого канала связи, малая вычислительная сложность [1]. В качестве контейнера сегодня чаще всего используются цифровые изображения (ЦИ), видео (ЦВ), цифровые аудио.

С учетом особенностей современной коммуникации, одной из которых является передача информации (ЦИ, ЦВ) в форматах с потерями, одним из самых важных требований к стеганоалгоритмам становится устойчивость к различным возмущающим воздействиям.

Для устойчивого к атакам против встроенного сообщения стеганопреобразования могут использоваться как пространственная область [2,3] контейнера (ЦИ, ЦВ), так и область преобразования [4,5]: частотная, области различных разложений матрицы (матриц) контейнера [6,7]. Однако до настоящего момента окончательного решения упомянутая задача с одновременным обеспечением надежности восприятия формируемого стеганосообщения так и не получила.

Далее в работе в качестве контейнера рассматривается ЦИ.

Подавляющее большинство стеганоалгоритмов, позиционируемых как устойчивые к возмущающим воздействиям, осуществляют погружение дополнительной информации (ДИ) в частотной области изображения [8,9], основываясь на спорном в свете [10] убеждении, что более устойчивыми к разнообразным искажениям являются стеганоалгоритмы, использующие для стеганопреобразования именно частотную область. В [10] показано, что свойства стеганоалгоритмов, в том числе, их устойчивость к возмущающим воздействиям, определяются не областью, используемой для стеганопреобразования, а величинами и локализацией возмущений сингулярных чисел и сингулярных векторов матриц, отвечающих контейнеру, произошедших в ходе стеганопреобразования. С учетом этого в [11,12] на основе sign-нечувствительности к произвольным возмущающим воздействиям сингулярных векторов (СНВ) блоков матрицы ЦИ, отвечающих максимальным сингулярным числам (СНЧ), был разработан устойчивый к атакам, в том числе значительным, против встроенного сообщения стеганографический алгоритм (СА) *SNG*, эффективность которого превышает эффективность современных аналогов, но область применимости которого ограничивается некоторыми особенностями используемого в качестве контейнера изображения, в частности наличием в ЦИ плохо обусловленных (близких к вырожденным) блоков, получаемых после стандартного разбиения матрицы. Такие ограничения снижают практическую ценность предложенного алгоритма.

## Цель статьи и постановка исследований

*Целью* работы является расширение области применимости стеганографического алгоритма *SNG*, устойчивого к атакам против встроенного сообщения, путем разработки алгоритма предобработки ЦИ-контейнера, предшествующей погружению ДИ.

Для достижения цели необходимо решить следующие *задачи*:

1. Обеспечить понижение числа обусловленности блоков матрицы ЦИ-контейнера в результате предобработки;
2. Обеспечить надежность восприятия ЦИ после его предобработки, с учетом чего выбрать способ предварительного кодирования блока изображения;
3. Обеспечить симметричность, положительную определенность и разреженность матрицы, являющейся результатом предварительного кодирования блока ЦИ;
4. Осуществить выбор предобуславливателя для блока ЦИ с учетом результата его кодирования.

## Основная часть

При организации скрытого канала связи часто задействуется одна цветовая составляющая (с учетом особенностей человеческого зрения – синяя) цветного ЦИ-контейнера, хранящегося в соответствии с цветовой схемой RGB. В силу этого, не ограничивая общности рассуждений, в качестве формального представления

контейнера в работе используется $m \times n$-матрица $F$. Как ДИ рассматривается случайно сформированная бинарная последовательность $p_1,...,p_t$, $p_i \in \{0,1\}$, $i = \overline{1,t}$.

Пусть $B$ – произвольный $8 \times 8$ – блок матрицы контейнера, полученный после ее стандартного разбиения [13], элементы которого $b_{kl}, k,l = \overline{1,8}$.

В ходе стеганопреобразования, осуществляемого алгоритмом *SNG*, для $B$ строится нормальное сингулярное разложение [11]:

$$B = U\Sigma V^T, \tag{1}$$

где $U,V$ – ортогональные $8 \times 8$ – матрицы левых $u_1,...,u_8$ лексикографически положительных и правых $v_1,...,v_8$ СНВ $B$ соответственно, отвечающих столбцам $U,V$, $\Sigma = diag(\sigma_1,...,\sigma_8)$ – матрица СНЧ, $\sigma_1 \geq ... \geq \sigma_8 \geq 0$.

Основная идея СА *SNG* заключается в том, что погружение ДИ в блок $B$ должно происходить путем такого возмущения СНВ $u_1, v_1$ (левого и/или правого), отвечающих максимальному СНЧ $\sigma_1$ блока, чтобы стеганопреобразование оставляло/делало его (их) близким (близкими) к *n*-оптимальному вектору $n^o = \left(1/\sqrt{8},...,1/\sqrt{8}\right)^T \in R^8$ пространства $R^8$.

При погружении очередного бита ДИ в очередной задействуемый для стеганопреобразования блок ЦИ-контейнера происходит отклонение $u_1$ и/или $v_1$ от первоначального положения. Для простоты дальнейшего изложения, не ограничивая общности рассуждений, будем считать, что стеганопреобразование происходит за счет модификации $u_1$, результат которой обозначим $\overline{u}_1$. Это требует приведение левых СНВ $u_2,...,u_8$ блока $B$ к ортонормированному с $\overline{u}_1$ лексикографически положительному виду, для чего в [12] предлагалось решать систему из 28 линейных алгебраических уравнений с неизвестными $x_i, i = \overline{1,28}$ (рис. 1):

$$\begin{cases} \left(\overline{u}_1, u_j{}^o\right) = 0, \; j = 2,..,8, \\ \left(u_i{}^o, u_j{}^o\right) = 0, \; i = 2,..,8, \; j = 2,..,i-1, \end{cases} \tag{2}$$

где $(\bullet,\bullet)$ – скалярное произведение векторов-аргументов, $u_i{}^o$ – вектор-столбец, ортогональный векторам $\overline{u}_1$ и $u_j{}^o, j = 2,..,i-1$. Матрица $\overline{U}$, фигурирующая при формировании матрицы $\overline{B}$ блока стеганосообщения при погружении ДИ, включает в себя нормированные векторы-столбцы $u_j{}^o \Big/ \left\| u_j{}^o \right\|, j = 2,..,8$:

$$\overline{U} = \left(\overline{u}_1, u_2{}^o \Big/ \left\| u_2{}^o \right\|,..., u_8{}^o \Big/ \left\| u_8{}^o \right\|\right) = (n^o, \overline{u}_2,..., \overline{u}_8). \tag{3}$$

Система (2) может оказаться плохо обусловленной для некоторых блоков ЦИ-контейнера, что приводит к возникновению артефактов на ЦИ-стеганосообщении (рис. 2). Установлено, что, как правило, это блоки, отвечающие фоновым областям изображения, перепад значений яркости пикселей в их пределах очень незначительный, а матрица блока близка к вырожденной (плохо обусловлена). Такие блоки в алгоритме *SNG* не использовались для погружения ДИ. Как показал вычислительный эксперимент, количество таких блоков в пределах изображения невелико, их игнорирование при стеганопреобразовании не приводит к значимому снижению пропускной способности организуемого скрытого канала связи, но все же

ограничивает область применимости алгоритма *SNG*, что можно трактовать как его недостаток.

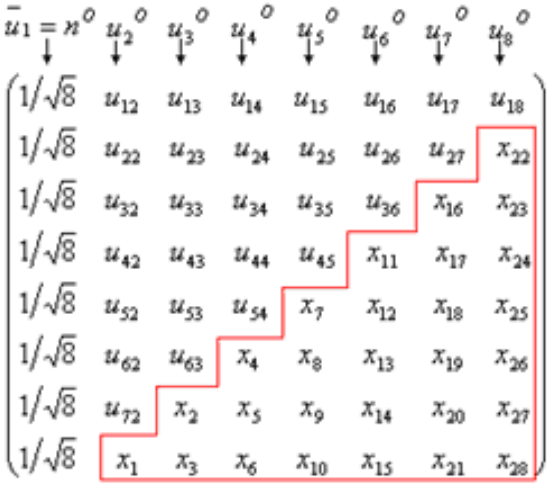
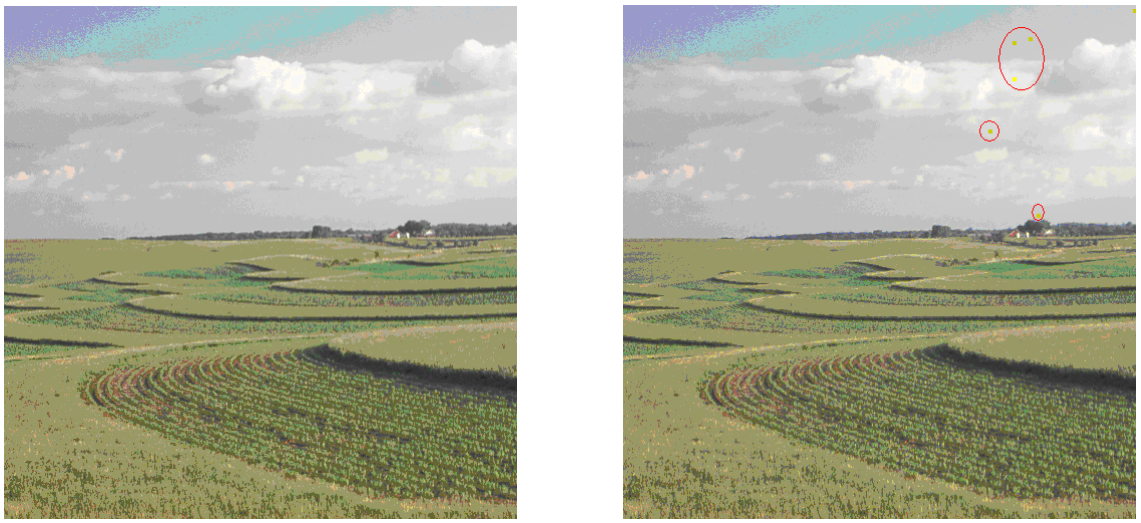


**Рис.1.** Возмущаемая в процессе стеганопреобразования блока $B$ алгоритмом *SNG* матрица левых СНВ $U$



а б

**Рис.2.** Пример нарушения надежности восприятия СС, формируемого стеганоалгоритмом *SNG*: а – ЦИ-контейнер (формат TIF); б – СС с обозначенными на нем областями, содержащими артефакты (формат TIF)

Одним из возможных способов решения возникшей проблемы является организация предобработки ЦИ-контейнера, предшествующей стеганопреобразованию алгоритмом *SNG*, таким образом, чтобы понизить числа обусловленности матриц (большинства) блоков, сохраняя при этом надежность восприятия результирующего изображения. Одним из широко используемых способов понижения числа обусловленности матрицы является ее предобуславливание [14] за счет выбора подходящей матрицы предобулавливателя, в качестве которого в случае разреженной симметричной и положительно определенной матрицы $A$ хорошо зарекомендовало себя ее неполное разложение Холесского [15]. Однако матрица $B$ блока ЦИ в общем случае не удовлетворяет ни одному из перечисленных выше свойств. Для обеспечения желаемых свойств проведем кодирование $B$ следующим образом.

Поставим $B$ в соответствие бинарную матрицу $\overline{B}$ с элементами $\overline{b}_{kl}, k,l=\overline{1,8}$:

$$\overline{b}_{kl}=\begin{cases}0, \textit{если } b_{kl}<P,\\ 1, \textit{если } b_{kl}\geq P\end{cases} \quad k,l=\overline{1,8}, \tag{4}$$

где

$$P=\left(\min_{1\leq k,l\leq 8} b_{kl}+\max_{1\leq k,l\leq 8} b_{kl}\right)\Big/2 \tag{5}$$

– пороговое значение, вычисляемое для каждого блока $B$, после чего матрице $\overline{B}$ поставим в соответствие две симметричных матрицы $B^{(V)}$ и $B^{(N)}$, отражая верхний (нижний) треугольник матрицы $\overline{B}$ относительно главной диагонали:

$$B^{(V)}=\begin{pmatrix}\overline{b}_{1,1} & \overline{b}_{1,2} & \overline{b}_{1,3} & \dots & \overline{b}_{1,8}\\ \overline{b}_{1,2} & \overline{b}_{2,2} & \overline{b}_{2,3} & \dots & \overline{b}_{2,8}\\ \overline{b}_{1,3} & \overline{b}_{2,3} & \overline{b}_{3,3} & \dots & \overline{b}_{3,8}\\ \dots & \dots & \dots & \dots & \dots\\ \overline{b}_{1,8} & \overline{b}_{2,8} & \overline{b}_{3,8} & \dots & \overline{b}_{8,8}\end{pmatrix},\ B^{(N)}=\begin{pmatrix}\overline{b}_{1,1} & \overline{b}_{2,1} & \overline{b}_{3,1} & \dots & \overline{b}_{8,1}\\ \overline{b}_{2,1} & \overline{b}_{2,2} & \overline{b}_{3,2} & \dots & \overline{b}_{8,2}\\ \overline{b}_{3,1} & \overline{b}_{3,2} & \overline{b}_{3,3} & \dots & \overline{b}_{8,3}\\ \dots & \dots & \dots & \dots & \dots\\ \overline{b}_{8,1} & \overline{b}_{8,2} & \overline{b}_{8,3} & \dots & \overline{b}_{8,8}\end{pmatrix}. \tag{6}$$

Матрицы $B^{(V)}$ и $B^{(N)}$, элементы которых далее обозначаются $b_{kl}{}^{(V)}$ и $b_{kl}{}^{(N)}$, $k,l=\overline{1,8}$, соответственно, являясь симметричными, могут не оказаться положительно определенными, более того, они могут оказаться вырожденными. Для обеспечения их положительной определенности положим:

$$b_{kk}{}^{(V)}=b_{kk}{}^{(N)}=8, \quad k=\overline{1,8}, \tag{7}$$

что гарантирует диагональное преобладание, а с учетом того, что после преобразования (7) $b_{kk}>0,\ k=\overline{1,8}$, то и положительную определенность. Модифицированные таким образом матрицы $B^{(V)}$ и $B^{(N)}$, обозначаемые далее $B_M^{(V)}$ и $B_M^{(N)}$, допускают разложения Холесского:

$$B_M^{(V)}=L^{(V)}\left(L^{(V)}\right)^T,\ B_M^{(N)}=L^{(N)}\left(L^{(N)}\right)^T, \tag{8}$$

где $L^{(V)}, L^{(N)}$ – нижние треугольные матрицы с положительными диагональными элементами, элементы которых далее обозначаются $l_{kl}{}^{(V)}, l_{kl}^{(N)}, k,l=\overline{1,8}$.

Неполные разложения Холесского для $B_M^{(V)}$ и $B_M^{(N)}$, обозначаемые далее

$$M^{(V)}=\overline{L}^{(V)}\left(\overline{L}^{(V)}\right)^T,\ M^{(N)}=\overline{L}^{(N)}\left(\overline{L}^{(N)}\right)^T \tag{9}$$

соответственно, будут отличаться от классических (8) тем, что нижние треугольные матрицы $\overline{L}^{(V)}$, $\overline{L}^{(N)}$ с элементами $\overline{l}_{kl}{}^{(V)}, \overline{l}_{kl}^{(N)}, k,l=\overline{1,8}$, соответственно будут иметь нулевые элементы в тех же позициях, что и нижние треугольные части матриц $B_M^{(V)}$ и $B_M^{(N)}$ соответственно, т.е.:

$$\bar{l}_{kl}^{(V)} = \begin{cases} l_{kl}^{(V)}, \text{если } b_{kl}^{(V)} \neq 0, \\ 0, \text{если } b_{kl}^{(V)} = 0 \end{cases}, \; \bar{l}_{kl}^{(N)} = \begin{cases} l_{kl}^{(N)}, \text{если } b_{kl}^{(N)} \neq 0, \\ 0, \text{если } b_{kl}^{(N)} = 0 \end{cases}, \quad k > l. \tag{10}$$

Предобусловленные матрицы $B_M^{(V)}$ и $B_M^{(N)}$, обозначаемые далее $W^{(V)}$ и $W^{(N)}$, будут выглядеть следующим образом:

$$W^{(V)} = \left(M^{(V)}\right)^{-1} B_M^{(V)}, \; W^{(N)} = \left(M^{(N)}\right)^{-1} B_M^{(N)}. \tag{11}$$

Числа обусловленности $W^{(V)}$ и $W^{(N)}$, которые не являются бинарными (их элементы в общем случае вещественные числа), практически для всех блоков ЦИ будут меньше чисел обусловленности $B_M^{(V)}$ и $B_M^{(N)}$:

$$cond\left(W^{(V)}\right) < cond\left(B_M^{(V)}\right), \; cond\left(W^{(N)}\right) < cond\left(B_M^{(N)}\right),$$

что подтверждается результатами вычислительного эксперимента. С учетом полученных предобусловленных матриц $W^{(V)}$ и $W^{(N)}$, отвечающих блоку $B$, поставим в соответствие $B$ блок ЦИ после предобработки, обозначаемый далее $\overline{\overline{B}}$ с элементами $\overline{\overline{b}}_{kl}$, $k,l = \overline{1,8}$, используя для восстановления элементов нижнего/верхнего треугольника $\overline{\overline{B}}$ нижний/верхний треугольник матрицы $W^{(V)}/W^{(N)}$ соответственно, учитывая первоначальное соответствие (4) между $B$ и $\overline{B}$ (1/0 в бинарной матрице $\overline{B}$ отвечал элементу оригинального блока $B$, величина которого превосходила/не превосходила пороговое значение $P$):

$$\overline{\overline{b}}_{kl} = \begin{cases} P-1, \text{если } \left(m_{kl}^{(V)} < 0.5\right) \& \left(b_{kl} \geq P\right), \\ P+1, \text{если } \left(m_{kl}^{(V)} \geq 0.5\right) \& \left(b_{kl} < P\right), \\ b_{kl} \text{ в противном случае} \end{cases} \quad \overline{\overline{b}}_{lk} = \begin{cases} P-1, \text{если } \left(m_{lk}^{(N)} < 0.5\right) \& \left(b_{lk} \geq P\right), \\ P+1, \text{если } \left(m_{lk}^{(N)} \geq 0.5\right) \& \left(b_{lk} < P\right), \\ b_{kl} \text{ в противном случае} \end{cases} \tag{12}$$

$$l > k.$$

Таким образом, усовершенствованный стеганоалгоритм *SNG* с учетом разработанного алгоритма предобработки блока ЦИ выглядит следующим образом.

***Погружение ДИ***

***Шаг 1***. Матрица $F$ ЦИ-контейнера разбивается стандартным образом на непересекающиеся $8 \times 8$ – блоки.

***Шаг 2***. В очередной блок $B$, используемый в процессе стеганопреобразования, погружается очередной бит $p_i$ ДИ:

2.1 (*предобработка блока*).

2.1.1. Для блока $B$ вычислить пороговое значение $P$ в соответствии с (5).

2.1.2. Матрице блока $B$ поставить в соответствие бинарную матрицу $\overline{B}$ в соответствии с (4).

2.1.3. Для матрицы $\overline{B}$ построить матрицы $B^{(V)}$ и $B^{(N)}$ в соответствии с (6).

2.1.4. Модифицировать матрицы $B^{(V)}$ и $B^{(N)}$ в соответствии с (7). Результат – симметричные положительно определенные разреженные матрицы $B_M^{(V)}$ и $B_M^{(N)}$.

2.1.5. Для матриц $B_M^{(V)}$ и $B_M^{(N)}$ построить разложения Холесского в соответствии с (8).

2.1.6. Для матриц $B_M^{(V)}$ и $B_M^{(N)}$ построить нижние треугольные матрицы $\overline{L}^{(V)}$, $\overline{L}^{(N)}$ – множители неполного разложения Холесского в соответствии с (10).

2.1.7. Для матриц $B_M^{(V)}$ и $B_M^{(N)}$ построить неполные разложения Холесского в соответствии с (9).

2.1.8. Выполнить предобуславливание матриц $B_M^{(V)}$ и $B_M^{(N)}$ в соответствии с (11). Результат – матрицы $W^{(V)}$, $W^{(N)}$.

2.1.9. Матрице $B$ поставить в соответствие блок $\overline{\overline{B}}$, построенный в соответствии с (12). $\overline{\overline{B}}$ – результат предобработки блока $B$, предшествующей погружению ДИ.

2.2. Для $\overline{\overline{B}}$ построить нормальное сингулярное разложение (1): $\overline{\overline{B}} = U\Sigma V^T$.

2.3. (*погружение* $p_i$):

*Если* $p_i = 1$, *то*

2.3.1. $\overline{u}_1 = n^o$, где $\overline{u}_1$ – возмущенный в ходе стеганопреобразования $u_1$;

2.3.2. Приведение левых СНВ $u_2,...,u_8$ блока $\overline{\overline{B}}$ к ортонормированному с $\overline{u}_1$ лексикографически положительному виду путем решения системы линейных уравнений (2) с последующей нормализацией (3) левых СНВ. Результат – $\overline{u}_2,...,\overline{u}_8$.

*иначе*

2.3.1. $\overline{v}_1 = n^o$, где $\overline{v}_1$ – возмущенный в ходе стеганопреобразования $v_1$;

2.3.2. Приведение правых СНВ $v_2,...,v_8$ блока $\overline{\overline{B}}$ к ортонормированному с $\overline{v}_1$ виду путем решения соответствующей системы линейных уравнений (2), составленной для правых СНВ, с последующей нормализацией (3) правых СНВ. Результат – $\overline{v}_2,...,\overline{v}_8$.

2.4. (*Формирование блока* $B_S$ *стеганосообщения, отвечающего блоку* $B$ *контейнера*).

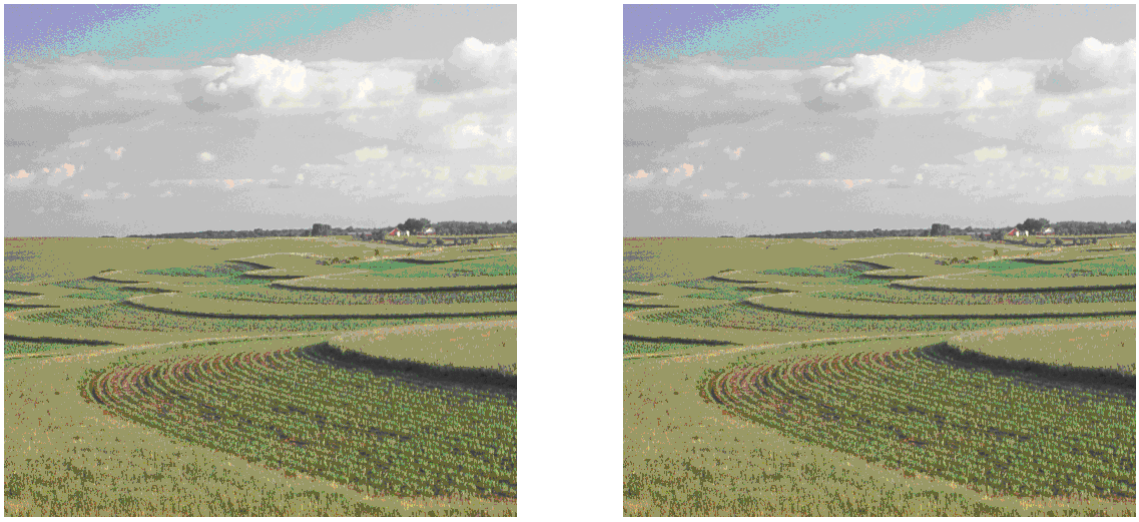
*Если* $p_i = 1$, *то* $B_S = \overline{U}\Sigma V^T$, где $\overline{U} = (n^o, \overline{u}_2,..., \overline{u}_8)$

*иначе* $B_S = U\Sigma\overline{V}^T$, где $\overline{V} = (n^o, \overline{v}_2,..., \overline{v}_8)$.

***Декодирование ДИ*** отвечает [12].

Для оценки изменения числа обусловленности блоков ЦИ после предложенной предобработки был проведен вычислительный эксперимент, в котором было задействовано более 200 ЦИ, хранимых как в формате с потерями (Jpeg), так и в формате без потерь (Tif), в ходе которого было установлено, что в среднем для 68% блоков ЦИ число обусловленности соответствующей матрицы уменьшалось (в среднем на 78%), при этом значение пикового отношения «сигнал-шум» PSNR, используемого для оценки искажения ЦИ в результате предобработки, в среднем составило 42 dB, что говорит о большой вероятности сохранения надежности восприятия изображения [16]. Максимально количество блоков изображения, для которых понижалось число обусловленности, составляло 88%, минимально – 52%. Искажения ЦИ в процессе предобработки находились в пределах 38-54 dB. Нарушения надежности восприятия обработанного ЦИ путем субъективного ранжирования в ходе вычислительного эксперимента установлено не было.

Погружение ДИ стеганоалгоритмом *SNG* после предложенной предобработки контейнера позволило значительно расширить область применимости алгоритма, иллюстрацией чего служит рис.3.



а б

**Рис.3.** Сохранение надежности восприятия стеганосообщения, формируемого стеганоалгоритмом *SNG* после предобработки контейнера: а – ЦИ-контейнер (формат TIF); б – стеганосообщение (формат TIF)

***Замечание***. Вычислительная сложность предложенного алгоритма обработки ЦИ определяется количеством блоков его матрицы, полученных в результате ее стандартного разбиения, и составляет $\underline{O}\left(n^2\right)$ для $n \times n$ – матрицы изображения, оставляя СА *SNG* при использовании предобработки контейнера полиномиальным степени 2.

## Выводы

В работе предложено усовершенствование устойчивого к атакам против встроенного сообщения, в том числе значительным, стеганографического алгоритма *SNG*, основанного на sign-нечувствительности сингулярных векторов блоков матрицы цифрового изображения, соответствующих максимальным сингулярным числам: предобработка блоков контейнера, осуществляемая перед непосредственным погружением ДИ. Результатом предобработки является понижение числа обусловленности большинства блоков матрицы контейнера, что позволило расширить область применимости алгоритма *SNG*, оставляя его полиномиальным степени 2.

## Список литературы


1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
2. Huang, H.Y. Robust technique for watermark embedding in a video stream based on block matching algorithm / H.Y. Huang, Y.R. Lin, W.H. Hsu // Optical Engineering. — 2008. — Vol. 47, Iss. 3. — PP. 037402-1–037402-14.
3. Кобозева, А.А. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного сообщения / А.А. Кобозева, О.В. Костырка, Е.Ю. Лебедева // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2014. – № 1(24). – С. 1-12.

4. Subhashini, D. Comparison analysis of spatial Domain and compressed Domain steganographic techniques / D. Subhashini, P. Nalini, G. Chandrasekhar // International Journal of Engineering Research and Technology. — 2012. — Vol. 1, Iss. 4. — PP. 1–6.
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. Veeraswamy, K. Adaptive AC-Coefficient Prediction for Image Compression and Blind Watermarking / K. Veeraswamy, S. Srinivas Kumar // Journal of Multimedia. — 2008. — Vol. 3, No. 1. — PP. 16-22.
7. Yongdong, W. On the security of an SVD based ownership watermarking / W. Yongdong // IEEE Transactions on Multimedia. — 2005. — Vol. 7, Iss. 4. — PP. 624–627.
8. 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.
9. Patra, J.C. Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital media authentication / J.C. Patra, A.K. Kishore, C. Bornand // In Proc. of 2011 IEEE International Conference on Systems, Man, and Cybernetics. — 2011. — P. 2940–2945.
10. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. — 2007. — № 4. — С. 531–538.
11. Кобозева, А.А. Анализ чувствительности сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / А.А. Кобозева, М.А. Мельник // Захист інформації. – 2013. – №2. – С.49-58.
12. Кобозева, А.А. Стеганографический алгоритм, основанный на sign-нечувствительности сингулярных векторов матрицы изображения / А.А. Кобозева, М.А. Мельник // Системи обробки інформації. – 2013. – Вип. 3(110), том 2. – С.90-94.
13. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. под ред. П.А. Чочиа. — М.: Техносфера, 2005. — 1072 с.
14. Деммель, Дж. Вычислительная линейная алгебра / Дж. Деммель; пер.с англ. Х.Д. Икрамова. — М.: Мир, 2001. — 430 с.
15. Альчиков, В.В. Использование метода неполной факторизации Холесского — сопряженных градиентов для решения трехмерных уравнений Лапласа / В.В. Альчиков, В.И. Быков // Вычислительные технологии. – 2000. – Т.5, № 6. – С.15-19.
16. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика. / Г.Ф. Конахович, , А.Ю. Пузыренко. — К.: МК — Пресс, 2006. – 288 с.

## УДОСКОНАЛЕННЯ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ, ЗАСНОВАНОГО НА SIGN-НЕЧУТЛИВОСТІ СИНГУЛЯРНИХ ВЕКТОРІВ БЛОКІВ МАТРИЦІ ЗОБРАЖЕННЯ

А.А. Кобозєва, В.А. Мокріцький, Л.Е.М. Батієне, І.І. Бобок

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

В роботі запропонований спосіб обробки цифрового зображення, результатом якої є зниження числа обумовленості більшості блоків його матриці, отриманих шляхом стандартного розбиття, за рахунок передобумовлення відповідних матриць. Обробка зберігає надійність сприйняття спотвореного зображення, яка в роботі кількісно оцінюється за допомогою пікового відношення «сигнал-шум». Використання запропонованого способу обробки як передобробки зображення-контейнера перед стеганоперетворенням дозволяє розширити область застосовності стійкого до атак проти вбудованого повідомлення, в тому числі значних, стеганографічного алгоритму, заснованого на sign-нечутливості сингулярних векторів блоків матриці цифрового зображення, які відповідають максимальним сингулярним числам, розробленого одним з автором раніше. Передобумовлення матриці блоку відбувається після його попереднього кодування. Результатом попереднього кодування є 2 симетричні додатно визначені розріджені матриці, які ставляться у відповідність блоку зображення. Додатна визначеність і розрідженість отриманих матриць дає можливість використовувати в якості передобумовника для них неповне розкладання Холеського. Наведено результати обчислювального експерименту.

**Ключові слова:** стеганографічний алгоритм, цифрове зображення, передобумовник, неповне розкладання Холеського, число обумовленості

## IMPROVEMENT OF THE STEGANOGRAPHY ALGORITHM BASED ON THE SIGN-INSENSITIVITY OF THE SINGULAR VECTORS OF BLOCKS OF THE DIGITAL IMAGE MATRIX

A.A. Kobozeva, V.A. Mokritsky**,** L.E.M. Batiiene, I.I. Bobok

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: kobozeva@opu.ua

In this paper the new method for digital image processing is proposed. Application of this method leads to decrease the conditioning number of the majority of matrix blocks obtained by standard partitioning as a result of preconditioning of the corresponding matrices. The proposed method preserves the reliability of the perception of the distorted image, which in the work is quantitatively estimated using the peak signal-to-noise ratio. The application of the proposed method as pre-processing of the cover image before steganography transformation makes it possible to extend the application domain of the steganography algorithm based on the sign-insensitivity of the singular vectors of blocks of the digital image matrix developed by one of the authors earlier. The preconditioning of the block matrix occurred after its precoding. The result of precoding is a symmetric positive-definite sparse matrix, which is mapped to the image block. The positive definiteness and sparsification of obtained matrix make it possible to use as its preconditioner the incomplete Cholesky factorization. The results of the computational experiment are presented.

**Keywords*:*** steganographic algorithm, digital image, preconditioner, incomplete Cholesky decomposition, condition number