DOI 10.15276/imms.v9.no4.324
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 4, pp. 324-332

# СТЕГАНОГРАФІЧНИЙ МЕТОД, СТІЙКИЙ ДО ЗБУРНИХ ДІЙ

**М.Є. Шелест, Т.В. Варда, І.І. Родюк**

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: mishel3141@gmail.com, tomavarda@gmail.com, ivan.rodiuk1999@gmail.com

До стеганографічних систем висувається ряд вимог, серед яких одною з основних є вимога стійкості стеганометодів до атак проти вбудованого повідомлення. Задача забезпечення цієї вимоги не є повністю вирішеною в цей час, залишається актуальною. Головною причиною цього є орієнтованість математичних базисів існуючих методів на конкретні атаки проти вбудованого повідомлення. У роботі розроблений новий стеганографічний метод, стійкий до збурних дій, який використовує в якості контейнера цифрове зображення. Стійкість методу теоретично обґрунтована з використанням специфіки властивостей сингулярних чисел блоків матриці оригінального зображення: всі сингулярні числа є нечутливими до збурних дій; для більшості $l\times l$-блоків, отриманих шляхом стандартної розбивки матриці, максимальне сингулярне число значно перевищує всі інші, що приводить до близькості до нуля кута між вектором сингулярних чисел, узятих у порядку спадання значень, і першим вектором стандартного базису простору відповідної вимірності. Показано, що стійкість процесу стеганоперетворення може забезпечуватися за допомогою корекції максимальних сингулярних чисел блоків контейнера, що відповідає достатній умові нечутливості стеганоповідомлення. Використовувана специфіка сингулярних чисел ніяк не пов'язана з конкретним видом атаки проти вбудованого повідомлення. Вбудова біта додаткової інформації в блок контейнера здійснюється в одну із двох симетричних матриць, які ставляться у відповідність матриці блоку зображення шляхом віртуального відбиття верхнього (нижнього) трикутника щодо головної діагоналі. Це забезпечує пропускну спроможність прихованого каналу зв'язку, що організується, $1/l\times l$ біт/піксель.

**Ключові слова**: стеганографічний метод, стійкість методу, атаки проти вбудованого повідомлення, сингулярні числа, симетрична матриця.

## Вступ

Стеганографія сьогодні - це один з найбільш перспективних напрямків захисту інформації [1,2], яка в сучасних умовах, ефективно поєднуючись із криптографією [3,4], впевнено займає провідні позиції у використовуваних підходах забезпечення інформаційної безпеки.

У якості контейнерів у сучасній стеганографії широко використовуються цифрові контенти: зображення (ЦЗ), відео, аудіо. При цьому стеганоперетворенню саме ЦЗ присвячені численні дослідження в області захисту інформації, у тому числі дана робота.

До стеганографічних систем висувається ряд вимог, серед яких одною з основних є вимога стійкості стеганометодів до атак проти вбудованого повідомлення [1]. Робота в даному напрямку ведеться в даний момент дуже активно, при цьому для вбудови додаткової інформації (ДІ) використовуються різні області контейнера: просторова, перетворення (частотна, області різних розкладань матриці ЦЗ). Так в [5] був розроблений стеганографічний метод і реалізуючий його ефективний поліноміальний стеганоалгоритм, в якому в стеганоперетворенні задіюється просторова область ЦЗ-контейнера після попереднього розбиття його матриці на блоки, що не перетинаються. Однак недоліком методу є негарантоване збереження надійності сприйняття

формованого стеганоповідомлення в тому випадку, коли ЦЗ-контейнер має значні по розмірі фонові області. Усуненню цього недоліку присвячена робота [6], в якій запропонована модифікація методу, що досягається за рахунок зменшення стрибка функції яскравості пікселів на границі блоків матриці ЦЗ-контейнера при вбудові ДІ шляхом зміни виду матриці збурення блоку контейнера при стеганоперетворенні. В [7] пропонується стійка до збурних дій схема вбудови ДІ для забезпечення захисту авторських прав. Тут вбудова біт ДІ відбувається в синю компоненту кольорового ЦЗ (в кольоровій схемі RGB) або в компоненту яскравості (в кольоровій схемі YUV) в області дискретного вейвлет-перетворення. Для забезпечення стійкості стеганоалгоритму кожний біт ДІ вбудовується в три позиції виділеної матриці контейнера, які визначаються секретним ключем. Велика частина сучасних розроблюваних стійких стеганоалгоритмів працюють в області дискретного косинусного перетворення та перетворення Фурьє. Актуальність таких алгоритмів визначається певними областями їх застосування з передбачуваними збурними діями. Прикладом таких алгоритмів є стеганоалгоритм з [8], заснований на теоремі лишків, та багато інших. Але проблема забезпечення стійкості стеганоалгоритмів до атак проти вбудованого повідомлення не є повною мірою вирішеною, залишається актуальною, оскільки більшість з існуючих методів орієнтована на конкретні збурні дії, стаючи неспроможними в умовах атак, що відрізняються від передбачуваних. Головною причиною цього є обмеженість математичних базисів існуючих методів, їх орієнтованість на конкретні атаки проти вбудованого повідомлення.

Враховуючи те, що збурення параметрів ЦЗ, що відбуваються при вбудові ДІ в будь-якій області контейнера (просторовій, області перетворення) приведуть до певних збурень в інших областях (перетворення, просторовій), стійкість стеганоалгоритму може бути забезпечена при проведенні стеганоперетворення в будь-якій області контейнера, але формальні достатні умови забезпечення стійкості стеганоалгоритму до атак проти вбудованого повідомлення, вперше запропоновані в [9, 10], використовують область сингулярного розкладання матриці (блоків матриці) контейнера, тому саме ця область ЦЗ розглядається в роботі.

## Мета статті та задачі дослідження

*Метою* роботи є розробка стеганографічного методу, стійкого до атак проти вбудованого повідомлення незалежно від конкретного виду збурної дії.

Для досягнення поставленої мети в роботі розв’язуються наступні *задачі*:

- обґрунтування вибору формальних параметрів цз, які задіюються при вбудові та аналізуються при декодуванні ді, та їх кількісних характеристик;
- обґрунтування стійкості до атак проти вбудованого повідомлення запропонованого стеганоперетворення.

## Основна частина

Розглядається ЦЗ, формальним представленням якого, не обмежуючи спільності міркувань, є одна $n \times n$-матриця $F$, яка піддається стандартній розбивці [11] на $l \times l$-блоки, що не перетинаються, довільний з яких далі позначається $B$. Для забезпечення стійкості стеганографічного алгоритму до атак проти вбудованого повідомлення необхідно задіяти в процесі стеганоперетворення ті формальні параметри, які, будучи такими, що визначаються однозначно, є нечутливими до збурних дій.

Як відомо [9], у якості набору параметрів, які однозначно визначають ЦЗ, можна розглянути множину сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) його

матриці (блоків матриці), що задовольняють певним властивостям, які можуть бути отримані шляхом її нормального сингулярного розкладання:

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

де $U^TU = E$, $V^TV = E$ ($E$ – одинична $n \times n$-матриця), стовпці матриці $U$ ($V$) – ліві (праві) СНВ $F$, ліві СНВ – лексикографічно додатні [9], $\Sigma = diag(\sigma_1(F),...,\sigma_n(F))$, $\sigma_1(F) \geq ... \geq \sigma_n(F) \geq 0$ - СНЧ $F$.

Всі СНЧ будь-якої матриці є нечутливими до збурних дій відповідно до співвідношення [12]:

$$\max_{1 \leq i \leq n} \left| \sigma_i(F) - \sigma_i(F + \Delta F) \right| \leq \left\| \Delta F \right\|_2,$$

де $\Delta F$ - матриця збурення $F$, $\left\| \bullet \right\|_2$ — спектральна матрична норма, чого не можна в загальному випадку сказати про СНВ [12], у силу чого в рамках задачі, що розглядається, множина СНЧ є кращою у порівнянні з множиною СНВ для організації процесу стеганоперетворення.

В [10] були отримані формальні достатні умови стійкості стеганометоду до стиску з втратами, що враховують специфіку збурення СНЧ блоків матриці контейнера, які забезпечують у цілому стійкість до атак проти вбудованого повідомлення й використовуються в роботі при розробці стеганометоду. Суть умов полягає в наступному. Для забезпечення стійкості стеганоперетворення достатньо проводити таким чином, щоб його формальним представленням була сукупність збурень найбільших СНЧ блоків матриці контейнера, при цьому для принципової можливості декодування ДІ сукупний результат збурень при її вбудові повинен перевищувати збурення, яке буде зазнавати блок стеганоповідомлення в результаті збурної дії [10].

Нехай $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_l \geq 0$ - СНЧ блоку $B$. Для СНЧ блоків оригінального ЦЗ останнє співвідношення можна уточнити [13]:

$$\sigma_1 >> \sigma_2 \geq ... \geq \sigma_l \geq 0. \tag{2}$$

Співвідношення (2) приводить до того, що для більшості блоків оригінального ЦЗ [13]

$$\angle(\sigma, e_1) \approx 0, \tag{3}$$

де $\angle(\sigma, e_1)$ - величина кута між векторам СНЧ $\sigma = (\sigma_1, \sigma_2, ..., \sigma_l)^T$ і $e_1 = (1,0,...,0)^T \in R^l$ - першим вектором стандартного базису простору $R^l$. Величина $\angle(\sigma, e_1)$ стане тою характеристикою, яка буде використовуватися для організації стеганоперетворення і декодування ДІ. В якості ДІ розглядається бінарна $\left[\frac{n}{l}\right] \times \left[\frac{m}{l}\right]$-матриця, що сформована випадковим чином (де $[\cdot]$ - ціла частина аргументу). В кожний $l \times l$-блок відбувається вбудова 1 біта ДІ, для чого необхідно передбачити два варіанти відповідного перетворення блоку. Враховуючи це, кожному блоку $B$ з елементами $b_{ij}$, $i, j = 1,...,l$, поставимо в відповідність дві симетричні $l \times l$-матриці $B_V$ і $B_N$ за наступним правилом [9]:

$$B=\begin{pmatrix} b_{11} & b_{12} & ... & b_{1l} \\ b_{21} & b_{22} & ... & b_{2l} \\ ..... & ..... & ..... & ..... \\ b_{l1} & b_{l2} & ... & b_{ll} \end{pmatrix} \rightarrow B_V=\begin{pmatrix} b_{11} & b_{12} & ... & b_{1l} \\ b_{12} & b_{22} & ... & b_{2l} \\ ..... & ..... & ..... & ..... \\ b_{1l} & b_{2l} & ... & b_{ll} \end{pmatrix}, \quad B_N=\begin{pmatrix} b_{11} & b_{21} & ... & b_{l1} \\ b_{21} & b_{22} & ... & b_{l2} \\ ..... & ..... & ..... & ..... \\ b_{l1} & b_{l2} & ... & b_{ll} \end{pmatrix}, \qquad (4)$$

відображаючи верхній (для $B_V$), нижній (для $B_N$) трикутник $B$ відносно головної діагоналі. Кожна з отриманих матриць буде використовуватися для вбудови конкретного значення біта ДІ.

Основні кроки методу, що пропонується, наступні.

*Вбудова ДІ.*

***Крок 1***. Матрицю $F$ ЦЗ-контейнера розбити стандартним чином на $l\times l$-блоки, що не перетинаються.

***Крок 2*** *(вбудова ДІ).* Для кожного $l\times l$-блоку $B$ матриці контейнера, що бере участь у стеганоперетворенні (порядок використання блоків є частиною секретного ключа) для вбудови $p_{ij}$ - чергового біта ДІ, робити:

2.1. Сформувати матриці $B_V$ і $B_N$ відповідно до (4).

2.2. Для $B_V$ і $B_N$ визначити вектори СНЧ: $\sigma(B_V)=(\sigma_1(B_V),...,\sigma_l(B_V))^T$ і $\sigma(B_N)=(\sigma_1(B_N),...,\sigma_l(B_N))^T$ відповідно шляхом нормальних сингулярних розкладань (1):

$$B_V=U_V\Sigma_V{V_V}^T, \quad B_N=U_N\Sigma_N{V_N}^T.$$

При вбудові біта ДІ зміни будуть вноситися в одну з матриць $B_V$, $B_N$.

2.3. *Якщо*

$$p_{ij}=0,$$

*то*

2.3.1. Забезпечити умову:

$$\angle(\sigma(B_N),e_1)>\angle(\sigma(B_V),e_1), \qquad (5)$$

збурюючи СНЧ $B_N$. Результат: збурена матриця СНЧ $\overline{\Sigma}_N$.

2.3.2. Сформувати збурену матрицю $\overline{B}_N$ з елементами $\bar{b}_{ij}^{(N)}, i,j=\overline{1,l}$:

$$\overline{B}_N=U_N\overline{\Sigma}_N{V_N}^T.$$

2.3.3. Сформувати блок $\overline{B}$ стеганоповідомлення, який відповідає блоку $B$ контейнера, в вигляді:

$$\overline{B}=\begin{pmatrix} b_{11} & b_{12} & ... & b_{1l} \\ \bar{b}_{21}^{(N)} & b_{22} & ... & b_{2l} \\ ..... & ..... & ..... & .. \\ \bar{b}_{l1}^{(N)} & \bar{b}_{l2}^{(N)} & ... & b_{ll} \end{pmatrix} \qquad (6)$$

*інакше*

2.3.1. Забезпечити умову:

$$\angle(\sigma(B_N),e_1) < \angle(\sigma(B_V),e_1), \tag{7}$$

збурюючи СНЧ $B_V$. Результат: збурена матриця СНЧ $\bar{\Sigma}_V$.

2.3.2. Сформувати збурену матрицю $\bar{B}_V$ з елементами $\bar{b}_{ij}^{(V)}, i, j = \overline{1,l}$:

$$\bar{B}_V = U_V \bar{\Sigma}_V V_V{}^T.$$

2.3.3. Сформувати блок $\bar{B}$ стеганоповідомлення, який відповідає блоку *B* контейнера, в вигляді:

$$\bar{B} = \begin{pmatrix} b_{11} & \bar{b}_{12}^{(V)} & \ldots & \bar{b}_{1l}^{(V)} \\ b_{21} & b_{22} & \ldots & \bar{b}_{2l}^{(V)} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots \\ b_{l1} & b_{l2} & \ldots & b_{ll} \end{pmatrix}. \tag{8}$$

***Крок 3***. З урахуванням змінених у результаті стеганоперетворення блоків матриці ЦЗ сформувати матрицю $\bar{F}$ стеганоповідомлення. Процес вбудови ДІ завершено.

У результаті атак проти вбудованого повідомлення в ході пересилання або зберігання стеганоповідомлення його матриця може зазнати зміни й тому далі при декодуванні позначається $\bar{\bar{F}}$.

*Декодування ДІ.*

***Крок 1***. Матрицю $\bar{\bar{F}}$ ЦЗ-стеганоповідомлення розбити стандартним чином на $l \times l$-блоки, що не перетинаються.

***Крок 2*** *(декодування ДІ)*. Для кожного $l \times l$-блоку $\bar{\bar{B}}$ матриці стеганоповідомлення, який брав участь в стеганоперетворенні (порядок блоків є частиною секретного ключа), робити:

2.1. Для блока $\bar{\bar{B}}$ сформувати матриці $\bar{\bar{B}}_V$ і $\bar{\bar{B}}_N$ відповідно до (4).

2.2. Для $\bar{\bar{B}}_V$ і $\bar{\bar{B}}_N$ визначити вектори СНЧ: $\bar{\bar{\sigma}}(B_V) = \left(\bar{\bar{\sigma}}_1(B_V),\ldots,\bar{\bar{\sigma}}_l(B_V)\right)^T$ і $\bar{\bar{\sigma}}(B_N) = \left(\bar{\bar{\sigma}}_1(B_N),\ldots,\bar{\bar{\sigma}}_l(B_N)\right)^T$. Нехай $\bar{\bar{p}}_{ij}$ - черговий біт ДІ, що декодується з чергового блоку $\bar{\bar{B}}$ стеганоповідомлення.

2.3. Визначити значення кутів $\angle\left(\bar{\bar{\sigma}}(B_N),e_1\right)$, $\angle\left(\bar{\bar{\sigma}}(B_V),e_1\right)$.

2.4. *Якщо*

$$\angle\left(\bar{\bar{\sigma}}(B_N),e_1\right) < \angle\left(\bar{\bar{\sigma}}(B_V),e_1\right),$$

*то*

$$\bar{\bar{p}}_{ij} = 1,$$

*інакше*

$$\bar{\bar{p}}_{ij} = 0.$$

Основним питанням у ході розробки алгоритмічної реалізації методу є питання забезпечення умови (5) (або (7)) при вбудові ДІ (крок 2.3.1). Одна з можливостей ґрунтується на врахуванні співвідношення (2) наступним чином. Очевидно, що для СНЧ блоків ЦЗ величина кута $\angle(\sigma,e_1)$ буде залежати від того, наскільки відрізняються одне від іншого перше й друге СНЧ, оскільки всі наступні СНЧ будуть незначно (значно менше) відрізнятися друг від друга, залишаючись невід'ємними. Виходячи з цього, керувати величиною кута $\angle(\sigma,e_1)$ можна дуже «недорого» в обчислювальному сенсі, коректуючи значення лише другого й першого СНЧ блоку, зменшуючи відстань між ними, забезпечуючи при цьому виконання достатньої умови стійкості до атак проти вбудованого повідомлення [10]. Таким чином, крок 2.3.1 при вбудові ДІ можна уточнити, наприклад, у такий спосіб:

2.3.1. Забезпечити умову:

$$\angle(\sigma(B_N),e_1) > \angle(\sigma(B_V),e_1) \ldots (\angle(\sigma(B_N),e_1) < \angle(\sigma(B_V),e_1)),$$

збурюючи СНЧ $B_N$ ($B_V$):

$$\sigma_1(B_N) = \sigma_1(B_V) - T,\ \sigma_2(B_N) = \sigma_2(B_V) + T \quad (\sigma_1(B_V) = \sigma_1(B_N) - T,\ \sigma_2(B_V) = \sigma_2(B_N) + T),$$

де $T > 0$ - параметр, установлюваний експериментально. Результат: збурена матриця СНЧ $\overline{\Sigma}_N$ ($\overline{\Sigma}_V$).

При визначенні значення параметра *T* необхідно враховувати дві взаємовиключні вимоги: для забезпечення стійкості відповідного алгоритму до атак проти вбудованого повідомлення T бажано зробити якнайбільше, оскільки для принципової можливості декодування ДІ сукупний результат збурень при вбудові ДІ повинен перевищувати збурення, яке буде зазнавати блок стеганоповідомлення в результаті збурної дії [10], але для забезпечення надійності сприйняття формованого стеганоповідомлення T повинне мати як можна менше значення. Необхідно відзначити, що говорячи про стійкість стеганографічних алгоритмів до атак проти вбудованого повідомлення, найчастіше маються на увазі атаки, формальним представленням яких є незначні збурення матриці стеганоповідомлення, оскільки інакше атака може привести до появи видимих артефактів на ЦЗ - втраті надійності сприйняття, у чому атакуюча сторона очевидно не зацікавлена. Компромісне значення буде встановлено експериментально в ході розробки алгоритмічної реалізації методу.

***Зауваження***. При формуванні блоку $\overline{B}$ стеганоповідомлення згідно з (6) і (8) важливо, що головна діагональ матриці $\overline{B}$ відповідає блоку *B* контейнера: така діагональ залишається оригінальною для тієї з матриць $B_V$, $B_N$, яку вбудова біта ДІ не торкнулася, залишаючи кут у ній між нормованим вектором СНЧ і першим вектором стандартного базису відповідного простору близьким до нуля (тобто в оригінальному виді (3)), і ця ж діагональ є додатковим збуренням для матриці, шляхом зміни якої проводилося стеганоперетворення, додатково збурюючи кут $\angle(\sigma,e_1)$, що позитивно відбивається на ході декодування ДІ.

Одним з основних питань при розробці алгоритмічної реалізації методу є питання вибору розміру блоків, на які матриця ЦЗ розбивається в процесі стеганоперетворення й декодування ДІ. Цей вибір буде проводитися таким чином, щоб співвідношення (3) виконувалося для як можна більшої кількості отримуваних при розбивці $l \times l$-блоків матриці контейнера.

Пропускна спроможність формованого за допомогою розробленого стеганометоду прихованого каналу зв'язку в незалежності від його алгоритмічної реалізації буде

визначатися як $1/l^2$ біт/піксель. Обчислювальна складність визначається кількістю блоків, на які розбивається матриця ЦЗ в ході роботи методу, і для $n \times n$-ЦЗ складе $O(n^2)$ операцій.

## Висновки

У роботі розроблений новий стеганографічний метод, стійкий до атак проти вбудованого повідомлення, що теоретично обґрунтовано з використанням специфіки властивостей сингулярних чисел блоків матриці ЦЗ: усі сингулярні числа є нечутливими до збурних дій; для більшості блоків оригінального ЦЗ, отриманих шляхом стандартної розбивки його матриці, максимальне СНЧ значно перевищує всі інші, що приводить до близькості до нуля кута між вектором СНЧ і першим вектором стандартного базису простору відповідної вимірності.

Запропонований метод може бути використаний як для ЦЗ в градаціях сірого, так і для кольорових. При цьому для кольорового зображення, збереженого відповідно до колірної схеми RGB, у стеганоперетвореній може бути задіяна кожна (декілька) з матриць R, G, B. Для колірної схеми YUV передбачається задіяти матрицю яскравості.

Результати розробки алгоритмічної реалізації представленого методу, що підтверджують на практиці його ефективність, у даний момент готуються до публікації.

## Література


1. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский и др. М.: Вузовская книга, 2009. 220 с.
2. Hindi A.Y., Dwairi M.O., AlQadi Z.A. A novel technique for data steganography.*Engineering, Technology & Applied Science Research*. 2019. 9(6). P. 4942-4945.
3. Combination of steganography and cryptography: A short survey / M.S. Taha et al. *IOP Conference Series: Materials Science and Engineering*. 2019. 518. 052003.
4. Almuhammadi S., Al-Shaaby A. A survey on recent approaches combining cryptography and steganography. *Comput. Sci. Inf. Technol.* 2017. 7(3). P. 63-74.
5. Кобозева А.А., Лебедева Е.Ю., Костырка О.В. Стеганопреобразование пространственной области изображения-контейнера, устойчивоек атакам против встроенного сообщения. *ProblemeleEnergeticiiRegionale*. 2014. 1(24). URL: http://journal.ie.asm.md/ru/contents/elektronnyij-zhurnal-n-124-2014 (дата звернення: 20.02.2019).
6. Костирка О.В. Модифікація стійкого до збурних дій стеганоперетворення просторової області зображення-контейнера. *Інформатика та математичні методи в моделюванні*. 2016. 6(1). С. 85–93.
7. Nasir I.A., Abdurrman A. A robust color image watermarking scheme based on image normalization. *Proceedings of the World Congress on Engineering (WCE 2013)*. London, 2013. Vol. III.
8. Patra J.C., Kishore A.K.,Bornand C. Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital media authentication. *Proceedings of 2011 IEEE International Conference on Systems, Man, and Cybernetics.* Anchorage, 2011. P. 2940-2945.
9. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
10. Кобозева А.А., Мельник М.А. Формальные условия обеспечения устойчивости стеганометода к сжатию. *Сучасна спеціальна техніка*. 2012. 4(31). С. 60–69.
11. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.
12. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
13. Кобозева А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. *Праці Одеського політехнічного університету*. 2014. 2. С. 136–146.

# СТЕГАНОГРАФИЧЕСКИЙ МЕТОД, УСТОЙЧИВЫЙ К ВОЗМУЩАЮЩИМ ВОЗДЕЙСТВИЯМ

М.Е. Шелест, Т.В. Варда, И.И. Родюк

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: mishel3141@gmail.com,
tomavarda@gmail.com, ivan.rodiuk1999@gmail.com

К стеганографическим системам выдвигается ряд требований, среди которых одним из основных является требование устойчивости стеганометодов к атакам против встроенного сообщения. Задача обеспечения этого требования не является полностью решенной в настоящее время, остается актуальной. Главной причиной этого является ориентированность математических базисов существующих методов на конкретные атаки против встроенного сообщения. В работе разработан новый метод, устойчивый к возмущающим воздействиям, использующий в качестве контейнера цифровое изображение. Устойчивость метода теоретически обоснована с использованием специфики свойств сингулярных чисел блоков матрицы оригинального изображения: все сингулярные числа являются нечувствительными к возмущающим воздействиям; для большинства $l\times l$-блоков, полученных путем стандартного разбиения матрицы, максимальное сингулярное число значительно превосходит все остальные, что приводит к близости к нулю угла между вектором сингулярных чисел, взятых в порядке убывания значений, и первым вектором стандартного базиса пространства соответствующей размерности. Показано, что устойчивость процесса стеганопреобразования может обеспечиваться при помощи коррекции максимальных сингулярных чисел блоков контейнера, что отвечает достаточному условию нечувствительности стеганосообщения. Используемая специфика сингулярных чисел никак не связана с конкретным видом атаки против встроенного сообщения. Погружение бита дополнительной информации в блок контейнера осуществляется в одну из двух симметричных матриц, которые ставятся в соответствие матрице блока путем виртуального отражения верхнего (нижнего) треугольника относительно главной диагонали. Это обеспечивает пропускную способность организуемого скрытого канала связи $1/l\times l$ бит/пиксель.

**Ключевые слова**: стеганографический метод, устойчивость метода, атаки против встроенного сообщения, сингулярные числа, симметричная матрица.

**STEGANOGRAPHIC METHOD RESISTANT TO DISTURBING INFLUENCES**

M.E. Shelest, T.V. Varda, I.I. Rodiuk

Odessa National Polytechnic University,
Shevchenko Ave., 1, Odessa, 65044, Ukraine; e-mail: mishel3141@gmail.com,
tomavarda@gmail.com, ivan.rodiuk1999@gmail.com

A number of requirements are being put forward for steganographic systems. One of the main requirements is the stability of steganomethods against attacks against embedded messages. The task of ensuring this requirement is not completely solved at this time. This task remains relevant. The main reason is the orientation of the mathematical bases of existing methods to specific attacks against the embedded message. Therefore, most of the existing steganographic methods are effective only for specific small attacks. A new method has been developed that is resistant to disturbing influences. This method uses a digital image as a container. The stability of the method is justified theoretically. This justification is based on the specific properties of matrix blocks singular numbers of the original image. All singular numbers are insensitive to disturbing influences, well conditioned. The maximum singular number significantly exceeds all other singular numbers in most $l \times l$-blocks of the image matrix. Blocks obtained as a result of the standard partition of the matrix. Therefore, the angle between the vector of singular numbers and the first vector of the standard basis of the corresponding space is close to zero. In a vector of singular numbers, they are taken in descending order of their values. It is shown that the stability of the stegano process can be ensured by correcting the maximum singular numbers of container blocks. Such a process corresponds to a sufficient condition for the steganomessage to be insensitive to disturbing influences. The specificity of the singular numbers that is used does not depend on the specific type of attack against the embedded message. Embedding a bit of additional information in the container block is carried out in one of two symmetric matrices. These matrices are mapped to the block matrix by virtual reflection of the upper (lower) triangle relative to the main diagonal. This provides the hidden communication channel capacity $1/l \times l$ bit/pixel.

**Keywords**: steganographic method, method stability, attacks against embedded messages, singular numbers, symmetric matrix.