DOI 10.15276/imms.v13.no3-4.311
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 311-321

МОДИФІКАЦІЯ МЕТОДУ ВИБОРУ КОНТЕЙНЕРА ДЛЯ ЗМЕНШЕННЯ ЧУТЛИВОСТІ СТЕГАНОПОВІДОМЛЕННЯ ДО ЗБУРНИХ ДІЙ

С.М.Сокальський

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: sokalskiyserhiy1@gmail.com

Питання захисту інформації від несанкціонованого доступу сьогодні є одним із ключових в сфері інформаційних технологій. Оскільки поширення цифрових технологій в усі сфери людської діяльності не зупиняться, і методи захисту інформації від небажаного доступу покращуються, то не зупиняється і розвиток методів та технологій отримання несанкціонованого доступу до конфіденційної інформації у зловмисних цілях. Тому важливо продовжувати вдосконалювати системи захисту інформації, тим самим перешкоджаючи зловмисникам. Складовою частиною будь-якої сучасної системи захисту інформації є стеганосистема, що забезпечує прихований канал передачі даних, який дозволить передавати інформацію, не викриваючи перед зловмисником факт її наявності. Задача вибору стеганографічного контейнера дозволяє вирішити деякі із вимог, що ставляться до стеганосистеми при її побудові. Однією із найважливіших вимог є забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення, адже такі атаки не вимагають від зловмисника обширних знань у галузі стеганографії та стеганоаналіза і не вимагають наявності спеціальних технічних засобів, що робить даний вид атак простим та розповсюдженим. *Метою* робити є підвищення ефективності стеганосистеми шляхом модифікації методу вибору контейнера з поданої сукупності, розробленого автором раніше, що забезпечить максимально можливу для аналізованих зображень, або близьку до максимальної, стійкість стеганоповідомлення до атак проти вбудованого повідомлення. Поставлена мета була досягнута шляхом модифікації кількісної оцінки об'єму захищеної інформації, а саме використанням відносного значення об'єму захищеної інформації до об'єму всієї вбудованої інформації. Результатом роботи є розробка модифікації методу вибору стеганографічного контейнера, що готовий до практичного застосування. Ефективність запропонованого методу є вищою ніж методу-прототипу, та залишається високою незалежно від того, який стеганометод чи збурення були використані. Значущість результату полягає у підвищені загальної стійкості стеганосистеми до атак проти вбудованого повідомлення за рахунок використання даного методу для вибору стеганоконтейнера.

Ключові слова: стеганосистема, стеганографічний метод, стійкість стеганосистеми, стеганографічний контейнер, цифрове зображення, сингулярні трійки.

Вступ. В результаті бурхливого розвитку комп'ютерних та інформаційних технологій процеси обміну, передачі та збереження конфіденційної інформації зайняли важливе місце у кожній сфері людської діяльності. Саме тому питання захисту цієї інформації від несанкціонованого доступу, зміни та спотворення є надзвичайно важливими.

Зараз тяжко уявити комплексну систему захисту інформації без стеганосистеми, мета якої при організації каналу зв'язку полягає у приховуванні самого факту наявності секретної інформації шляхом вбудовування цієї інформації у деякий інформаційний контент – контейнер, зазвичай цифровий [1-5], який не привертає уваги. Після вбудови приховуваної інформації отриманий контент повинен ніяк візуально не відрізнятися від контейнера, тобто зберігати

надійність сприйняття. Але із розвитком технологій захисту інформації також розвиваються і способи отримання несанкціонованого доступу до конфіденційної інформації, її зміни або знищення, тому завдання покращення методів прихованої передачі даних залишається актуальним і на сьогоднішній день.

Процес стеганографування умовно можна розділити на три етапи: вибір контейнера, попереднє кодування інформації, що передається, результат якого надалі називається додатковою інформацією (ДІ), і вбудовування ДІ у контейнер, в результаті чого отримується стеганоповідомлення. Контейнери можуть бути двох типів – потокові або фіксовані. Потокові контейнери представляють собою послідовність бітів, яка постійно змінюється в часі, і ДІ вбудовується в них у реальному масштабі часу. У такому випадку завчасно неможливо визначити обсяг інформації, яку можна буде вбудувати у контейнер, на відміну від фіксованого контейнера, що має чітко визначені характеристики, зокрема розміри. Саме при використанні фіксованих контейнерів є можливість завчасно обчислити обсяг інформації, яку можна вбудувати у контейнер. Враховуючи це, а також специфіку задачі, що розглядається в роботі, яка зазначається нижче, далі розглядаються фіксовані контейнери – цифрові зображення (ЦЗ).

При побудові стеганосистеми до неї висувається ряд вимог, серед яких забезпечення стійкості до атак проти вбудованого повідомлення, надійність сприйняття стеганоповідомлення, стійкість до стеганоаналізу, тощо [6,8]. На сьогодні саме стійкість стеганосистеми до атак проти вбудованого повідомлення, метою яких є внесення змін в стеганоповідомлення, наслідком чого може стати спотворення або навіть повне знищення вбудованої ДІ, вважається найбільш пріоритетною ціллю: на відміну від стеганоаналітичних атак, які, як правило, потребують спеціальних технічних та програмних засобів і високої кваліфікації атакуючого, атаки проти вбудованого повідомлення можуть проводитись без специфічного програмного або технічного забезпечення, без спеціальної підготовки та кваліфікації зловмисника, наприклад, атака стисненням, накладення шуму, фільтрація. Це робить такий вид атак надзвичайно простим і поширеним, і саме це диктує високу потребу у забезпеченні стійкості прихованого повідомлення до збурних дій.

При організації прихованого каналу зв’язку можуть бути використані випадкові, нав’язані або ж обрані контейнер. Саме обрані контейнери в більшій чи меншій степені дозволяють покращити властивості чи задовольнити вимоги, що висуваються до отримуваного стеганоповідомлення, залишаючи актуальною задачу їх вибору, розв’язку якої присвячена дана робота.

Питанням формування методу вибору контейнера з метою забезпечення певних вимог стеганоповідомлення займаються багато вчених-стеганографів. Так у [9] дані контейнера моделюються як процес Гауса-Маркова. Основною ціллю виступає забезпечення стійкості стеганосистеми до стеганоаналізу.

У роботі [6] піднімається питання забезпечення надійності сприйняття стеганоповідомлення та стійкості стеганосистеми до стеганоаналізу, але питання забезпечення стійкості до атак проти вбудованого повідомлення в [6,7] не розглядається.

У [10] вибір контейнера проводиться лише для одного стеганометода Бенгама-Мемона-Ео-Юнга. Таке значне обмеження для застосування цього методу робить його неможливим для розглядання у якості вирішення проблеми забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення в цілому.

У роботі [11] було представлено метод, що базується на основі поняття обсягу захищеної інформації, що кількісно визначає об'єм вбудованої інформації, яка є захищеною від деякої збурної дії. Значною перевагою цього методу є

відсутність обмежень на застосування стегнографічних алгоритмів і конкретики прогнозованих атак.

У роботі [12] запропоновано метод вибору стеганографічного контейнера на основі введеної кількісної характеристики, що характеризує об'єм інформації, яка буде правильно декодована після атаки на стеганоповідомлення, та обчислюється з врахуванням вектору розподілу ДІ серед власних векторів симетричної матриці контейнера та чутливості цих векторів до збурної дії *E*, що відображає збурення від прогнозованої атаки на стеганоповідомлення.

Цей метод базується на можливості представлення стеганоперетворення, тобто процесу вбудовування додаткової інформації, як деякої адитивної операції над матрицею ЦЗ-контейнера:

$$F = \overline{F} + \Delta F \tag{1}$$

де F - n×n-матриця контейнера, $\overline{F}$ - матриця СП, ΔF - n×n-матриця збурення, яке виникло в результаті вбудовування ДІ у контейнер. У роботі введене поняття захищеної від збурної дії E інформації, де E – матричне представлення збурної дії, що виникла в процесі атаки проти вбудованого повідомлення. Але, як показала практика, між об'ємом захищеної інформації (ЗІ), розрахункова формула якого запропонований в роботі, і обсягом правильно декодованої інформації систематична відповідність відсутня. Крім того викликає сумніви доцільність використання при розрахунках ЗІ спектру матриці контейнера та її власних векторів. Оскільки для отримання цих параметрів необхідно спочатку виконати процес симетризації матриці контейнера, то цей набір параметрів однозначно визначає не первісну матрицю контейнера, а її специфічну модифікацію. З урахуванням вищенаведеного у роботі [13] присвяченій задачі, що розглядається, цей набір параметрів був змінений на сукупність сингулярних векторів і сингулярних чисел $n \times n$-матриці контейнера F (довільної структури), які можна отримати за допомогою нормального сингулярного розкладу:

$$F = U\Sigma V^T \tag{2}$$

де U, V - ортогональні $n \times n$-матриці, стовпці яких u_i, v_i, $i = \overline{1,n}$, є лівими та правими сингулярними векторами (СНВ) відповідно, при цьому ліві СНВ додатково є лексикографічно додатними; $\Sigma = diag(\sigma_1, ..., \sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$ – сингулярні числа (СНЧ) F. СНЧ довільної F, як і власні значення симетричної матриці, є добре обумовленими через співвідношення [19]:

$$\max_i \left|\sigma_i(F) - \sigma_i(F+E)\right| \leq \|E\|_2 \tag{3}$$

де $\|\cdot\|_2$ – спектральна матрична норма, E – n×n матриця збурення, мірою ж чутливості до збурень СНВ u_i досі вважалася відокремленість

$$svdgap(i,F) = \min_{i \neq j} \left|\sigma_i - \sigma_j\right| \tag{4}$$

відповідного СНЧ σ_i згідно з формулою:

$$\sin 2\theta_i \leq 2\|E\|_2 / svdgap(i,F) \tag{5}$$

де θ_i - кут повороту u_i в результаті збурної дії E. Очевидно, що співвідношення (5) дає оцінку зверху для кута θ_i тільки тоді, коли його права частина менше чи дорівнює 1. Інакше поведінка вектора u_i після атаки непередбачувана. Для визначення «контрольованих» формальних параметрів (СНВ) в [13] було введено поняття СНЧ σ_i матриці F, яке має достатню відокремленість щодо збурної дії E. Для такого СНЧ має місце співвідношення:

$$svdgap(i,F) \geq 2\|E\|_2 \tag{6}$$

при цьому відповідний СНВ u_i називається захищеним від збурної дії E.

Для формування методу вибору контейнера з сукупності даних, що забезпечить максимальну (близьку до максимальної) стійкість відповідного

стеганоповідомлення до атак проти вбудованого повідомлення, в [13] було введене поняття поля, що захищене від збурення E, яке являє собою суму однорангових матриць, кожна з яких відповідає сингулярній трійці (σ_i, u_i, v_i) де СНЧ має достатню відокремленість стосовно збурення E, тобто є малоранговою апроксимацією матриці контейнера. Опираючись на це, було запропоновано формулу для обчислення об'єму захищеної від E інформації, яка стала основою відповідного методу:

$$S = \left\| \sum_{k=1}^{m} \overline{\sigma_k} \cdot \overline{u_k} \cdot \overline{v_k}^T - \sum_{k=1}^{m} \sigma_k \cdot u_k \cdot v_k^T \right\| \quad (7)$$

де m – максимальний індекс серед СНЧ F, які мають достатню по відношенню до E відокремленість, $(\overline{\sigma}_i, \overline{u}_i, \overline{v}_i)$ - сингулярні трійки матриці стеганоповідомлення. Формула (7) являє собою інформацію, що була вбудована у захищене поле контейнера і визначається як різниця малорангових апроксимацій матриці контейнера та стеганоповідомлення.

Запропонований в [13] метод є ефективнішим за наявні аналоги, але він не гарантує систематично вибір контейнера, що забезпечує максимально можливу стійкість відповідного стеганоповідомлення до збурень.

Мета статті та постановка досліджень. Метою роботи є підвищення ефективності стеганосистеми шляхом модифікації методу вибору контейнера з поданої сукупності, запропонованого в [13].

Під ефективністю стеганосистеми розуміється її стійкість до атак проти вбудованого повідомлення, що кількісно оцінюється значенням коефіцієнта кореляції NC між вбудованою ДІ, що представляє бінарну послідовність $p_1, p_2, \dots p_t, p_i \in \{0,1\}, i = \overline{1,t}$, та декодованою $\overline{p_1}, \overline{p_2}, \dots \overline{p_t}, \overline{p_i} \in \{0,1\}, i = \overline{1,t}$, ДІ [23]:

$$NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p_i'}}{t} \quad (8)$$

де $p_i' = 1, \bar{p}_i' = 1$, якщо $p_i = 1, \bar{p}_i = 1$, і $p_i' = -1, \bar{p}_i' = -1$, якщо $p_i = 0, \bar{p}_i = 0$.

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

1. Модифікувати кількісну оцінку об'єму захищеної інформації, що є основою для модифікації методу [13] вибору стеганографічного контейнера;
2. Провести оцінку ефективності, зокрема порівняльну, модифікованого методу вибору контейнера.

Об'єктом дослідження є процеси забезпечення певних характеристик стеганоповідомлень при організації прихованого каналу зв'язку.

Предметом дослідження є методи вибору контейнера з заданої скінченної сукупності можливих, якому відповідає стеганоповідомлення, що має максимально можливу/близьку до максимально можливої стійкість до атак проти вбудованого повідомлення.

Основна частина. Оскільки будь-яке стеганоперетворення можна представити як деяке збурення матриці ЦЗ-контейнера згідно із формулою (1), то формально ДІ, яка вбудовується, можна представити у вигляді матриці збурення ΔF, та вирахувати за формулою:

$$\Delta F = \overline{F} - F \quad (9)$$

де F – матриця ЦЗ контейнера, $\overline{F}$ - матриця ЦЗ стеганоповідомлення. Очевидно, що в загальному випадку навіть при одній і тій самій ДІ, яка вбудовується одним і тим самим стеганометодом, але в різні ЦЗ-контейнери, формальне представлення ДІ, що отримується за допомогою (9), буде різним.

У методі, що представлений у роботі [13], згідно до формули (7) об'єм ЗІ вираховується як норма матриці різниці малорангових апроксимацій матриць ЦЗ контейнера та стеганоповідомлення, а це значить, що на об'єм ЗІ впливає не лише кількість СНЧ, що мають достатню відокремленість по відношенню до збурної дії, що задовольняє співвідношення (6), але й збурення, що матриця контейнера отримує внаслідок вбудовування ДІ.

Крім того, поняття достатньої відокремленості СНЧ (6), а також відповідного захищеного СНВ вводиться по відношенню до збурення E. Використовувана кількісна оцінка збурення, яке скрізь ((3), (5), (6)) фігурує у вигляді матричної норми $\|E\|_2$, буде залежати від розміру матриці E, тобто від розміру матриці ЦЗ-контейнера: чим більше розмір матриці, тим більше $\|E\|_2$, що підтверджується результатами обчислювального експерименту, наведеними на рис.1.

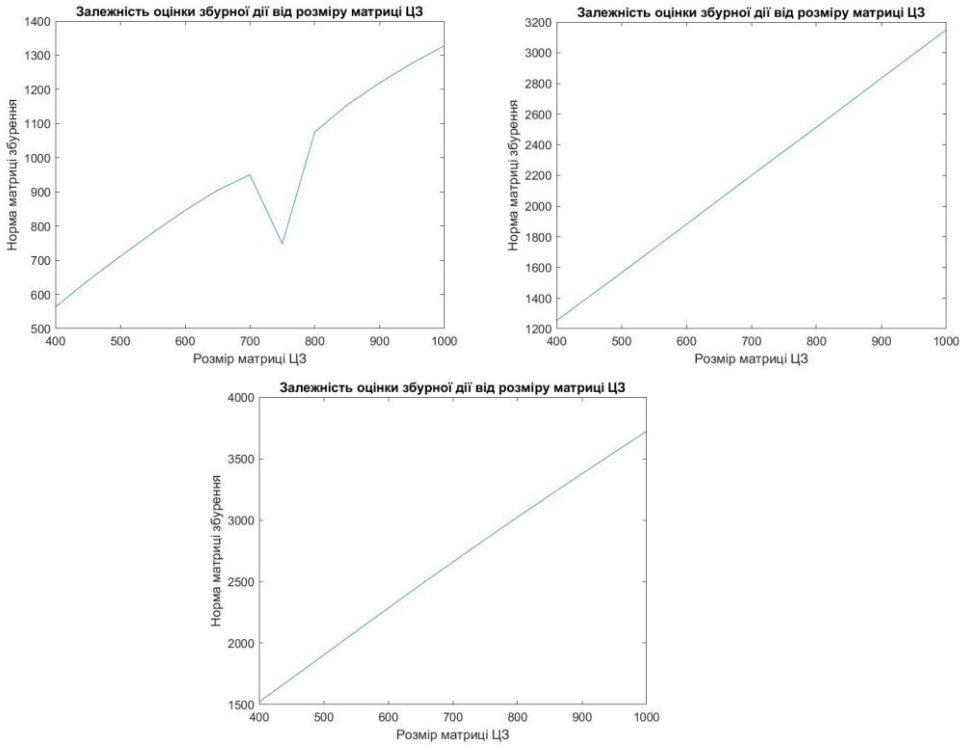


Рис.1. Залежність $\|E\|_2$ від розміру матриці ЦЗ, коли E відповідає: 1 – стиску ЦЗ з втратами з QF=75; 2 – накладанню гауссівського шуму з нульовим математичним очікуванням і D=0.001; 3 – накладанню пуассонівського шуму

Але ж конкретика збурення, характеристики атаки проти вбудованого повідомлення (стиску з втратами, накладання шуму, фільтрація, розмиття тощо), тобто її вид, властивості, зокрема «сила», ніяк не залежить від розміру того контенту, на який вона спрямована, зокрема ЦЗ, а визначаються параметрами цієї збурення (коефіцієнтом якості QF – стиск з втратами, математичним очікуванням і дисперсією – накладання шуму тощо).

СНЧ з достатньою відокремленістю – це m найбільших за значенням СНЧ [13]. Збільшення розміру ЦЗ, як правило, приводить до збільшення значення максимальних СНЧ. Дійсно, енергія $N(F)$ ЦЗ з $n\times n$-матрицею F з елементами f_{ij} може бути обчислена у відповідності з формулою [13]:

$$N(F)=\sum_{i,j=1}^{n} f_{ij}^2=\sum_{i=1}^{n}\sigma_i^2 \qquad (10)$$

Зі зростанням *n* трендом тут буде зростання $\sum_{i,j=1}^{n} f_{ij}^2$ і, як витікає з формули (10), зростання $N(F)$, а, враховуючи співвідношення між СНЧ матриці оригінального ЦЗ, а саме: $\sigma_1 >> \sigma_2 \geq ... \geq \sigma_n$, очікуваним є збільшення найбільших СНЧ *F*. Ці зміни ніяк не пов'язані з процесом, що розглядається, тобто зі збуреннями, що застосовуються до зображень в процесі стеганоперетворень та атак проти вбудованого повідомлення, але вони відіб'ються певним чином на складових формули (7).

З урахуванням вищенаведеного коректне використання формули (7) для порівняння властивостей контейнерів в однакових умовах їх використання вимагає, крім іншого, того, щоб всі ЦЗ, що претендують на роль контейнера, мали однакові розміри, але на практиці це, як правило, не виконується.

Для зменшення впливу наведених негативних факторів пропонується модифікувати розрахункову формулу (7) об'єму ЗІ наступним чином:

$$S = \frac{\left\| \sum_{k=1}^{m} \overline{\sigma_k} \cdot \overline{u_k} \cdot \overline{v_k}^T - \sum_{k=1}^{m} \sigma_k \cdot u_k \cdot v_k^T \right\|}{\left\| \overline{F} - F \right\|} \qquad (11)$$

Формула (11) за змістом умовно надає відносну кількість ЗІ відносно ДІ в її конкретному для даного ЦЗ представленні і є основою для модифікованого методу вибору контейнера, що забезпечує максимальну/близьку до максимальної стійкість відповідного стеганоповідомлення до атак проти вбудованого повідомлення, основні кроки якого наступні.

Нехай *K* – задана множина ЦЗ-контейнерів, з яких відбувається вибір, $p_1, p_2 ... p_l$ - бінарна послідовність – результат попереднього кодування повідомлення, що пересилається, M_S - обраний для застосування ДІ стеганометод, *E* – формальне представлення передбачуваної атаки проти вбудованого повідомлення.

Крок 1. Для кожного ЦЗ $F \in K$:

1.1. Виконати вбудовування ДІ $p_1, p_2 ... p_l$ за допомогою вибраного стеганографічного методу M_S в контейнер *F*. Результат – СП з матрицею $\overline{F}$;

1.2. Побудувати нормальне сингулярне розкладання (2) для *F*;

1.3. Визначити відокремленості (4) для отриманих СНЧ;

1.4. Визначити множину *M* індексів СНЧ з достатньою відокремленістю по відношенню до збурення *E*;

1.5. Побудувати нормальне сингулярне розкладання (2) для $\overline{F}$;

1.6. Вирахувати відносне значення об'єму ЗІ *S* за формулою (11);

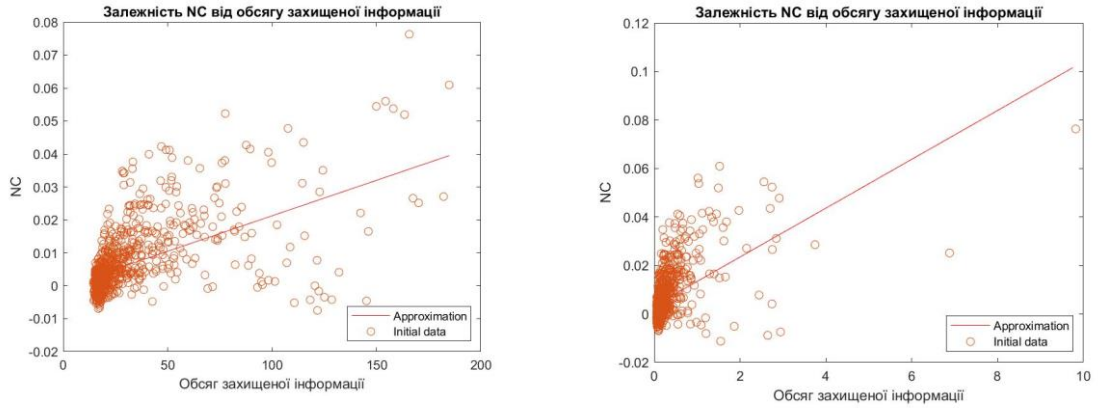
Крок 2. Серед всіх ЦЗ множини *K* визначити таке F_V, для якого відносне значення об'єму ЗІ $S(10)$ відповідатиме відношенню $S_V = \max_{F \in K} S$, ЦЗ F_V - шуканий контейнер.

Оцінка ефективності модифікованого методу вибору контейнера. Для оцінки ефективності модифікованого методу вибору стеганографічного контейнера було проведено обчислювальний експеримент, в ході якого були використані стеганометоди: Жао і Коха [14], модифікації найменшого значущого біта (LSB) [15], а також методи запропоновані у роботі [16] та [17]). В якості атак проти вбудованого повідомлення розглядалися: накладання мульиплікативного та гауссівського шумів з різними параметрами, атака стисненням з різними коефіцієнтами якості. Кінцева сукупність контейнерів-претендентів була представлена 1000 цифровими зображеннями формату .jpg та розміром 400x400

пікселів, що були взяті із незалежного джерела [18] і 100 цифровими зображеннями зробленими на аматорську цифрову камеру розміром 400x400 пікселів.

Для оцінки ефективності запропонованого методу вибору стеганоконтейнера використовується, по аналогії з [13], різниця між NC (8) контейнера з найбільшим об'ємом захищеної інформації (11), та найбільшим NC з усієї вибірки контейнерів-претендентів.

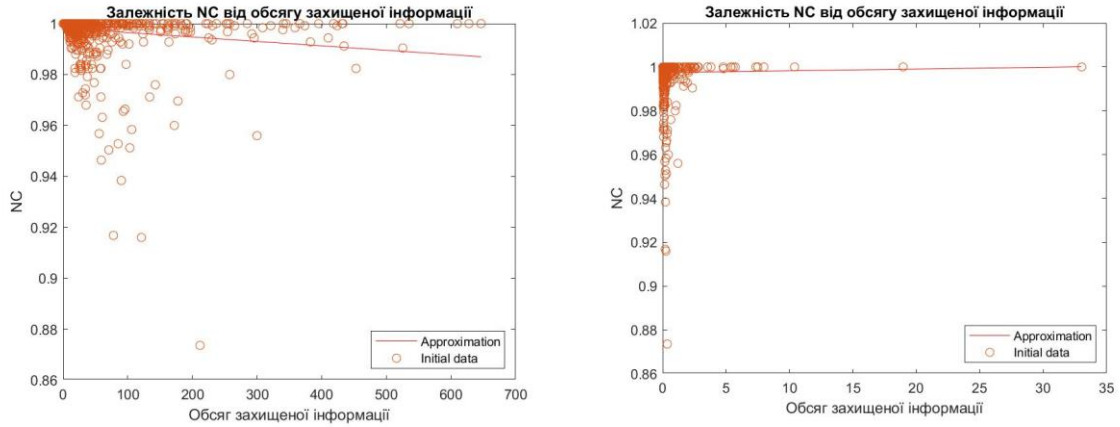
Деякі з результатів обчислювального експерименту відображені на рис.2-5.



а) б)

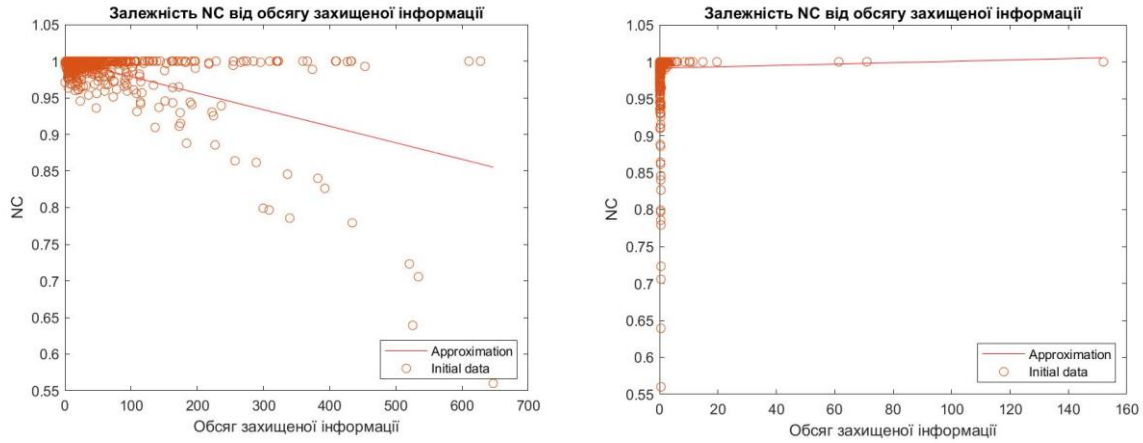
Рис. 2. Залежність NC від об'єму захищеної інформації: а – метод [13], б – метод, запропонований в роботі, з використанням стеганометоду LSB в умовах атаки стисненням з коефіцієнтом якості QF=85

На рис. 2 наглядно виражено залежність між NC та об'ємом захищеної інформації для цифрових зображень. І хоча пряма залежність відслідковується як і в випадку використання методу обчислення абсолютного значення об'єму захищеної інформації, так і в випадку обчислення відносного об'єму, але ефективність методів відрізняється: так у першому випадку NC, що відповідає цифровому зображенню з найбільшим абсолютним значенням об'єму захищеної інформації, становить 0,0609, а у другому випадку – 0,0763.



а) б)

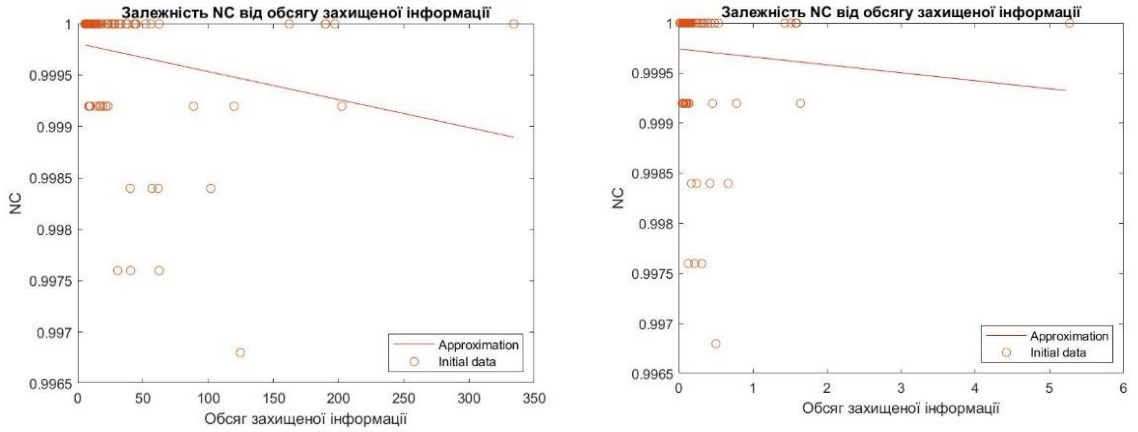
Рис. 3. Залежність NC від об'єму захищеної: а – методу [13], б – метод, запропонований в роботі, з використанням стеганометоду Жао і Коха та атаки стисненням з QF=75



а) б)

Рис. 4. Залежність NC від об'єму захищеної інформації: а – метод [13], б – метод, запропонований в роботі, з використанням стеганометоду Жао і Коха в умовах накладання мультиплікативного шуму з дисперсією 0,001

При чому максимальний NC з усієї вибірки становить 0,0763. Таким чином ефективність методу [13] в умовах використання стеганометода LSB та атаки стисненням з коефіцієнтом якості 85 становить 79,8 %, а методу представленого в цій роботі – 100%, що говорить про підвищення ефективності методу на 20,2 %.



а) б)

Рис. 5. Залежність NC від об'єму захищеної інформації: а – метод [13], б – метод, запропонований в роботі, з використанням стеганометоду Жао і Коха та атаки стисненням з *QF*=75, де в якості контейнерів-претендентів були використані ЦЗ зроблені на аматорську цифрову камеру.

З результатів, наведених на рисунках 2-5 випливає перевага запропонованого модифікованого методу в порівнянні з прототипом, яка підтверджується результатами, наведеними в табл.1.

Таблиця 1

Результати порівняльного аналізу запропонованого методу та методу [13]

Стеганометод	Збурення	Значення *NC*, що відповідає максимальному об'єму ЗІ		Максимальне значення NC в умовах експерименту
		Метод [13]	Наш метод	
Метод LSB (просторова область вбудовування ДІ) [15]	Стиснення з втратами, *QF*=75	0.0864	0.0985	0.0985
	Гауссівський шум с матоочікуванням 0 і *D*=0.000001	0,9007	0,9007	0,9241

продовження табл.1

	Мультиплікативний шум с *D*=0.000001	0.9993	0.9993	0.9993
Метод з кодовим управлінням вбудовування ДІ (просторова область вбудовування ДІ) [16]	Стиснення з втратами, *QF*=75	1	1	1
	Гауссівський шум з матоочікуванням 0 і *D*=0.0005	0.4856	1	1
	Мультиплікативний шум с *D*=0.0005	0.4920	1	1
Метод модифікації максимального СНЧ (вбудовування ДІ - область сингулярного розкладання) [17]	Стиснення з втратами, *QF*=75	0.9944	1	1
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	0.9944	0.9944	1
	Мультиплікативний шум с *D*=0.0005	0.9888	1	1
Метод Коха і Жао (частотна область вбудовування ДИ) [14]	Стиснення з втратами, *QF*=75	0,8312	0,9864	1
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	0,7944	1	1
	Мультиплікативний шум с *D*=0.0005	1	1	1

Як видно, запропонований метод не тільки не гірший за метод [13], але й показав кращі результати в деяких випадках. Так, наприклад, при використанні стеганометоду LSB [15] в умовах стиснення з втратами з *QF*=75 значення *NC*, що відповідає максимальному об'єму ЗІ, при використані методу [13] становить 0.0864, а при використанні запропонованого методу - 0.0985, що свідчить про підвищення ефективності на 12,3%. Найбільше підвищення ефективності було досягнуто при використанні методу з кодовим управлінням вбудовування ДІ (просторова область вбудовування ДІ) [16] в умовах накладанням гауссівського та мультиплікативного шуму, що становить 51,5% та 50,8% відповідно. Якщо оцінювати ефективність методу [13] та запропонованого методу, виходячи із результатів експерименту в цілому, то середня ефективність методу [13] становить 86,975%, а методу, що був представлений у даній роботі – 99,67%.

Висновки. В роботі вирішено важливу науково-практичну задачу, що полягає у підвищенні ефективності стеганосистеми шляхом розробки модифікації методу вибору контейнера з поданої сукупності, запропонованого в [13].

В ході модифікації запропоноване поліпшення кількісної оцінки об'єму захищеної від збурення *E* інформації, що міститься у певному стеганоповідомленні, шляхом обґрунтування доцільності введення нормування об’єму відповідно до формули (11).

Проведену оцінку ефективності, зокрема порівняльну, модифікованого методу.

Отримані результати свідчать про підвищення ефективності методу вибору стеганографічного контейнера в умовах атаки проти вбудованого повідомлення, а тому і стійкості стеганосистеми в цілому, шляхом використання не абсолютного, а відносного значення об'єму захищеної інформації на 12,695%.

Список літератури

1. Torten R., Reaiche C., Boyle S. The impact of security awareness on information technology professionals' behavior. *Computers & Security*. 2018. Vol. 79. P. 68-79.
2. Alqahtani F. Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*. 2017. Vol. 124. P. 691-697
3. Mandal P.C., Mukherjee I., Goutam P., Chatterji B.N. Digital image steganography: A literature survey. *Information Sciences.* 2022. Vol. 609, P.1451-1488
4. Taher M. M., Ahmad A.R.B.HJ, Hameed R.S., Mokri S.S. A literature review of various steganography methods. *Journal of Theoretical and Applied Information Technology*. 2022. Vol.100. No 5. P.1412-1427.
5. Gupta D., Gupta S., Gupta R. Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective.* 2021. Vol. 30.2. P. 63-87.
6. Abed S., Al-Roomi S. A., Al-Shayeji M. Efficient cover image selection based on spatial block analysis and DCT embedding. *Journal on Image and Video Processing.* 2019. No. 1. https://doi.org/10.1186/s13640-019-0486-8
7. Mohammed A. M., Rossilawati S., Shukur Z., Hasan M. K. A Review on Text Steganography Techniques. *Mathematics*. 2021. No.9. 2829. URL: https://doi.org/10.3390/math9212829
8. Qi Q. A Study on Countermeasures against Steganography: an Active Warden Approach. URL: https://digitalcommons.unl.edu/ceendiss/25/
9. Selecting Cover for Image Steganography by Correlation Coefficient URL: https://ieeexplore.ieee.org/document/5459929
10. Nikishova A.V., Omelchenko T.A., Makedonskij S.A. Steganographic embedding in containersimages. *Journal of Physics: Conference Series*. 2018. Vol. 1015. No. 4. doi: 10.1088/1742- 6596/1015/4/042041
11. Kobozeva A.A., Narimanova E.V. Stegoimage disturb sensitivity estimate. *System Research and Information Technologies*. 2008. No. 3. P. 52-65.
12. Надвоцький О.Ю., Кобозєва А.А.. Метод розв'язку задачі про вибір контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій. URL: http://immm.op.edu.ua/files/archive/n3_v11_2021/immm_n3_v11_2021.pdf
13. Bobok I., Kobozieva A., Sokalsky S. The Problem of Choosing a Steganographic Container in Conditions of Attacks against an Embedded Message. URL: https://journal.ie.asm.md/assets/files/07_04_56_2022.pdf
14. Fedorov A., Rubel A.S. Detection of Hidden Data Embedded by the Koch and Zhao Method. URL: https://www.researchgate.net/publication/283463767
15. Singh A.K., Singh J., Singh H.V. Steganography in Images Using LSB Technique. *International Journal of Latest Trends in Engineering and Technology*. 2015. Vol. 5, No. 1, P. 426-430.
16. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, No. 3, P. 147-161.
17. Melnik M.A. Steganoalgoritm, ustoichivyi k szhatiyu [A compression resistant stegano algorithm]. *Informatsiyna Bezpeka – Information Security*. 2012. No. 2. P. 99-106.
18. Images Dataset. URL: https://www.kaggle.com/datasets/pavansanagapati/images-dataset

MODIFICATION OF THE CONTAINER SELECTION METHOD TO REDUCE THE SENSITIVITY OF THE STEGANOMESSAGE TO DISTURBING INFLUENCES

S. Sokalsky

National Odesa Polytechnic University
1, Shevchenko Ave, Odesa, 65044, Ukraine
email: sokalskiyserhiy1@gmail.com

Today, the issue of protecting information from unauthorized access is one of the key issues in the field of information technology. As digital technologies continue to spread into all areas of human activity and methods of protecting information from unwanted access are improving, the development of methods and technologies for obtaining unauthorized access to confidential information for malicious purposes does not stop either. Therefore, it is important to continue to improve information security systems, thereby hindering intruders. An integral part of any modern information security system is a steganographic system that provides a hidden data transmission channel that allows you to transmit information without revealing the fact of its existence to an attacker. The task of choosing a steganographic container allows you to solve some of the requirements for a steganographic system when building it. One of the most important requirements is to ensure the steganographic system's resistance to attacks against the embedded message, since such attacks do not require extensive knowledge of steganography and steganalysis from the attacker and do not require special technical means, which makes this type of attack simple and widespread. The aim of the work is to improve the efficiency of the steganosystem by modifying the method of selecting a container from the given set, developed by the author earlier, which will ensure the maximum possible, or at least close to the maximum, resistance of the steganomessage to attack against the embedded message for the analyzed images. This goal was achieved by modifying the quantitative assessment of the amount of protected information, namely, using the relative value of the amount of protected information to the amount of all embedded information. The result of the work is the development of a modification of the method for selecting a steganographic container, which is ready for practical application. The effectiveness of the proposed method is higher than the prototype method, and remains high regardless of which steganomethod or perturbation was used. The significance of the result is to increase the overall resistance of the steganosystem to attacks against the embedded message by using this method to select the steganocontainer.

Keywords: steganosystem, steganographic method, resistance of the steganosystem, steganographic container, digital image, singular threes.