УДК 681.322:621.391

А. С. Васюра, к. т. н., проф.; В. В. Лукічов

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ ШАБЛОННОГО ВБУДОВУВАННЯ ДАНИХ У ЗОБРАЖЕННЯ

Запропоновано метод вбудовування даних у зображення, які в подальшому підлягають обробці JPEG-алгоритмом. Розглянуто особливості вбудовування, що визначають таємність та стійкість прихованих даних. З метою розробки ефективного стеганографічного методу синтезовано критерій, який використано у якості цільової функції при вбудовуванні. Таким чином, процедура приховування реалізується шляхом вирішення задачі оптимізації.

***Ключові слова**: стеганографія, метод шаблонного вбудовування, таємність, робастність, JPEG-алгоритм, вейвлет-перетворення.*

Вступ

Стеганографія зображень є галуззю, що дістала стрімкого розвитку протягом останніх десяти років. Її ціль може бути окреслена як таємне та стійке до різноманітних перетворень приховування даних. Відповідно практичні задачі, що вирішуються в її межах, в більшій чи меншій мірі стосуються аспектів таємності та робастності [1, 2].

Оскільки порушення таємності може призвести до повної втрати повідомлення, то саме зазначена якість задає основні обмеження при проектуванні стегосистеми. Треба відмітити, що відносний характер цього показника обумовлює існування великої кількості критеріїв, ефективність яких неоднакова для різних методів вбудовування.

Іншим важливим аспектом є вимога стійкості. Оскільки широко розповсюджені схеми надлишкового кодування з захистом від помилок, то питання робастності може бути вирішено з ефективністю, що визначається достовірністю відновленої інформації [3].

Таким чином, проектування будь-якої стегосистеми можна розглядати як задачу умовної оптимізації, де цільова функція певним чином пов'язує робастність із ступенем таємності, а обмеження визначають область адекватності критерію. Такий універсальний підхід дозволить забезпечити високу адаптивність до умов безпосереднього функціонування стегосистеми.

У стеганографії зображень особливо розповсюдженою є схема сліпого вбудовування де передається лише стегоконтейнер. Це визначає особливості стегоаналізу, задача якого полягає у бінарній класифікації зображень на основі властивостей, що зазнають найбільших змін при вбудовуванні. Особливо перспективними є критерії на основі апаратів векторного поділу (SVM) [4], найбільшою перевагою яких є ефективність класифікації точок-характеристик в багатомірному просторі ознак.

Серед методів обробки зображень найбільшою популярністю користуються методи стиснення. Найбільший коефіцієнт ущільнення здатні забезпечити методи стиснення з втратами [5]. Стандарт стиснення JPEG і досі використовується широко, незважаючи на впровадження більш ефективних форматів на основі вейвлет-перетворень (наприклад JPEG2000). Така ситуація, вочевидь, обумовлена інертністю концепцій розробки програмного забезпечення у цій сфері, що в свою чергу дозволяє прогнозувати значну тривалість переходу.

Тому в якості основного фактору впливу на стегоконтейнер розглядається обробка JPEG. З іншого боку, стеганографічне використання вейвлет-перетворень дає підстави сподіватися на непомітність внесених змін. За допомогою розробленого критерію пропонується дослідити комплексний зв'язок між таємністю та робастністю зазначеного використання в області вейвлет-перетворень.

Коефіцієнти вирішено модифікувати відповідно до розповсюдженого підходу векторної квантизації. Його різновидом є шаблонна схема вбудовування, для якої значення таємної порції даних залежить від співвідношень набору коефіцієнтів з певним еталонним значенням [6]. Основною перевагою шаблонної схеми є можливість багатоваріантного представлення порції таємних даних, що дозволяє підвищити їх стійкість.

Під час розробки сучасних методів приховування в більшості випадків оптимізується одна з якостей таємності або робастності. Використання критерію, що поєднує визначені якості, покликано підвищити ефективність стегозахисту. Аспект актуальності не вичерпується лише даним критерієм: запропоновано адаптивний шлях його покращення. Для цього враховуються властивості кожного об'єкту стеганографічного маніпулювання, який несе елементарну частку таємних даних.

Передбачається, що особливості запропонованого у статті підходу забезпечать високу ефективність стегометоду на його основі. Розробка такого методу є метою даного дослідження.

Критерій стеганографічної ефективності

Комплексну оцінку ефективності стегометоду пропонується здійснювати з використанням незалежних показників таємності та робастності. Міру робастності визначено як частку збережених елементарних порцій таємних даних після обробки стегозображення. У якості критерію таємності обрано стегоаналітичний критерій запропонований в [4]. Він використовує SVM для класифікації зображень. Для цього кожне зображення характеризується вектором сталої довжини, значення якого отримують шляхом порівняння сусідніх пікселів.

Таким чином, для кожного стегоаналітичного критерію зв'язок між PSNR та ентропією детектування $e^{\det} = -p\log p - \overline{p}\log\overline{p}$ є прямим, де $\overline{p} = 1 - p$, p – ймовірність вірної класифікації. Для даного критерію експериментально встановлено високу кореляцію між цими показниками. Тому надалі цей зв'язок розглядається за замовченням.

Оцінка ефективності вбудовування передбачає врахування наслідків певних характерних впливів з боку третьої особи. У випадку застосування JPEG-компресії, результат залежить від параметрів стиснення, які задаються користувачем. Квантування коефіцієнтів ДКП описується залежністю

$$dct_{i,j}^{jpeg} = \frac{Q_{i,j}}{q}\,\mathrm{round}\left(\frac{dct_{i,j}}{Q_{i,j}}q\right), \qquad (1)$$

де $Q_{i,j}$ – відповідний елемент матриці квантування Q, $i,j = 1\ldots8$, q – параметр, що задається користувачем та визначає якість і розмір стисненого зображення [5]. Звичайно, неможливо в кожному конкретному випадку передбачити значення q, однак використання статистичного розподілу f_q дозволяє перейти до обґрунтованої оцінки. Рис. 1 відображує типовий розподіл f_q.

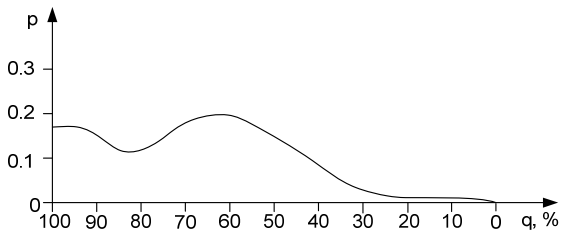

Рис.1. Типовий розподіл значень параметра q

Оскільки результат обробки JPEG-алгоритмом (квантування) залежить від значень коефіцієнтів ДКП, то стійкість вбудованих даних для різних блоків зображення буде різною.

Таке ж зауваження стосується кількісної міри спотворень вбудовування. При JPEG-стисненні блоки зображення 8×8 обробляються незалежно. Тому за умови незалежного вбудовування у ці блоки, можна отримати адаптивну до вимог таємності та робастності стегосистему.

Критерій ефективності вбудовування має бути інтегральним, оскільки замість значення q відомо лише розподіл f_q. Таким чином певній i-й умові квантування, що повністю визначається q_i, відповідає ймовірність f_{q_i} та комплексна характеристика ефективності системи z_i. Якщо z_i визначити як добуток стегоаналітичної ентропії детектування $e_i^{\det}$ та показника робастності $r_i = 1 - \mathrm{BER}_i$, де BER – показник бітових помилок, то критерій загальної ефективності вбудовування можна представити виразом:

$$E = \sum_i z_i f_{q_i} = \sum_i e_i^{\det} r_i f_{q_i} . \tag{2}$$

Враховуючи, що значення показників $e_i^{\det}$ та r_i є залежними від енергії вбудовування $d = \left\| I^{org} - I^{stg} \right\|^2$ (спотворення стегозображення I^{stg} у порівнянні з оригінальним I^{org}), попередній вираз приймає вигляд

$$E(d) = \sum_i e_{i,d}^{\det} r_{i,d} f_{q_i} . \tag{3}$$

Для випадку неперервної зміни умов квантування маємо:

$$E(d) = \int e^{\det}(q,d) r(q,d) f(q) dq . \tag{4}$$

Однак запропонований адаптивний підхід вимагає додаткового визначення критерію ефективності вбудовування. За вищезгаданим припущенням $e^{\det}(q,d)$ є однозначною функцією. Для більшості популярних стегометодів це стосується і показника робастності $r(q,d)$. У випадку адаптивного вбудовування, аргументів (q,d) недостатньо для адекватного представлення рівня робастності, оскільки кожен з об'єктів стеганографічного маніпулювання може зазнавати неоднозначного впливу. Тому ключовим моментом максимізації $E(d)$ буде пошук $r(q,d,\Omega)$, де $\Omega = \{\Omega_j\}$, $j = 1\ldots m$, Ω_j – вектор стану j-го об'єкту. Кінцева задача проектування стегометоду формалізується:

$$\max_d \left(\max_{\Omega} \int e^{\det}(q,d) r(q,d,\Omega) f(q) dq \right). \tag{5}$$

Вочевидь, ефективність вбудовування визначатиметься не тільки методами оптимізації при вирішенні поставленої вище задачі. Спосіб вбудовування (схема) в першу чергу задає обмеження і суттєво впливає на результат [2]. Хоча запропонований підхід можна поєднати з будь-якою схемою, вирішено використовувати шаблонну. Цей вибір пояснюється високим ступенем свободи маніпулювання.

Модель шаблонного вбудовування даних у вейвлет-коефіцієнти

Шаблонна схема, що взята за основу стегометоду, є набором умов, які однозначно інтерпретуються при витяганні порції таємних даних. Але при вбудовуванні порція однакових даних може відображатися різними умовами. Таким чином має місце залежність «один-багато». Набір умов обраної шаблонної схеми описує співвідношення між чотирма скалярними значеннями та єдиною пороговою константою TH при вбудовуванні двох бітів таємних даних (табл.1). Кожна умова описується чотирма бітами, що відповідають логічному результату виконання нерівності $a_l^j \geq TH$, $l = 1\ldots 4$, $j = 1\ldots m$, де a_l^j – l-й елемент j-го об'єкту маніпулювання [6].

Таблиця 1

Логічні умови вбудовування даних за шаблонною схемою

Таємні дані	0 0	0 1	1 0	1 1
Умова	0 0 0 1	0 1 1 1	0 0 0 0	1 1 1 1
	0 0 1 0	1 0 1 1	0 0 1 1	1 0 0 1
	0 1 0 0	1 1 0 1	0 1 0 1	1 0 1 0
	1 0 0 0	1 1 1 0	0 1 1 0	1 1 0 0

Перевагами такої схеми є гнучкість та можливість забезпечення високої робастності. З іншого боку це призводить до надлишковості і як наслідок – більших спотворень, оскільки два біти вбудовуються у чотири елементи. Проте, вибір даної схеми пов'язаний з можливістю використання властивості гнучкості з метою забезпечення оптимального співвідношення між спотвореннями та робастністю.

Визначення методу перетворення для отримання елементів, що використовуються шаблонною схемою, суттєво впливатиме на загальну ефективність [7]. Головною особливістю вейвлет-перетворення є масштабоване відображення сигналу x:

$$\varphi_{j,n}(x) = \sqrt{2^j}\,\varphi(2^j x - n)\,,\ \psi_{j,n}(x) = \sqrt{2^j}\,\psi(2^j x - n)\,, \tag{6}$$

де $\varphi_{j,n}(x)$, $\psi_{j,n}(x)$ – функція масштабування та вейвлет-функція відповідно, j – рівень розкладання, n – зсув [8, 9]. Наприклад, за допомогою ортонормального базису Добеші

$$\mathbf{D} = \begin{bmatrix} h_0 & h_1 & h_2 & h_3 & \underbrace{0 \ \dots \ 0}_{n-4} \\ 0 & 0 & h_0 & h_1 & h_2 & h_3 & \dots \\ & & & \vdots & & & \\ & & & n/2-3 & & & \\ & & & \vdots & & & \\ h_2 & h_3 & 0 & \dots & 0 & h_0 & h_1 \\ g_0 & g_1 & g_2 & g_3 & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & \dots \\ & & & \vdots & & & \\ g_2 & g_3 & 0 & \dots & 0 & g_0 & g_1 \end{bmatrix} \tag{7}$$

перетворення сигналу $\mathbf{S} = [s_1 \ \dots \ s_i \ \dots \ s_n]$ може бути представлено у матричній формі:

$$\mathbf{W} = \mathbf{D} \times \mathbf{S}^T\,, \tag{8}$$

де $\mathbf{W}^T = [\underbrace{w_1 \ \dots \ w_{n/2}}_{low} \ \underbrace{w_{n/2+1} \ \dots \ w_n}_{high}]$. Шляхом подальшого розкладання компоненти *low* отримують систему масштабованих відображень сигналу $\mathbf{S}$. Для зображень використовується двомірне вейвлет-перетворення:

$$\begin{aligned} \varphi_{j,k,n}(x,y) &= 2^j \varphi(2^j x - k)\varphi(2^j y - n), \quad \psi^H_{j,k,n}(x,y) = 2^j \varphi(2^j x - k)\psi(2^j y - n), \\ \psi^V_{j,k,n}(x,y) &= 2^j \psi(2^j x - k)\varphi(2^j y - n), \quad \psi^D_{j,k,n}(x,y) = 2^j \psi(2^j x - k)\psi(2^j y - n). \end{aligned} \tag{10}$$

Масштабування за допомогою вейвлетів дозволяє обрати оптимальний з точки зору критерію E рівень відображення.

Оскільки під час компресії JPEG коефіцієнти ДКП квантуються неоднаково, можна виділити частину ДКП базису, де спотворення квантування будуть меншими. Відповідно повнота відображення області маніпулювання в цій частині базису буде більш бажаною для забезпечення робастності. Вибір рівня вейвлет-відображення для вбудовування напряму пов'язаний з цим пріоритетом. Це можна продемонструвати шляхом порівняння значень проекцій векторів вейвлет-базису на значущу частину базису ДКП. Поняття значущої частини є досить умовним, але в більшості параметри JPEG стиснення передбачають

ненульове значення частини коефіцієнтів ДКП, що відокремлені межею на рис. 2,а.

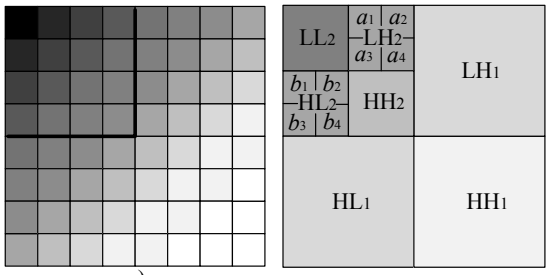

Рис.2. а) Ступінь значимості коефіцієнтів ДКП; б) Значимість коефіцієнтів різних рівнів вейвлет-перетворення

Коефіцієнти ДКП задаються виразом:

$$y(k) = \varpi(k)\sum_{n=1}^{N} x(n)\cos\frac{\pi(2n-1)(k-1)}{2N}, \quad k = 1,...,N, \tag{11}$$

де $\varpi(k) = \begin{cases} 1/\sqrt{N}, & k = 1 \\ \sqrt{2/N}, & 2 \le k \le N \end{cases}$, $x(n)$ – сигнал, N – кількість коефіцієнтів ДКП [5].

Відповідно двомірне ДКП визначається як

$$B_{pq} = \alpha_p \alpha_p \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} A_{mn}\cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1; \\ 0 \le q \le N-1; \end{matrix}$$
$$\alpha_p = \begin{cases} 1/M, & p = 0; \\ \sqrt{2/M}, & 1 \le p \le M-1; \end{cases} \quad \alpha_q = \begin{cases} 1/N, & q = 0; \\ \sqrt{2/N}, & 1 \le q \le N-1. \end{cases} \tag{12}$$

Нехай значущу частину ДКП базису для перетворення фрагменту зображення 8×8 позначимо $\mathbf{C}_{16}^{pr}$. Тоді проекції $T_i, i = 1\ldots16$ частини вейвлет-базису $\mathbf{H}_{16}^{pr}$, що визначає ліву верхню чверть коефіцієнтів на рис. 2,б, обчислюватимуться як $T_i = \sum_j (v_{i,j})^2$, $\mathbf{V} = \mathbf{H}_{16}^{pr}\left(\mathbf{C}_{16}^{pr}\right)^T$, $v_{i,j} \subset \mathbf{V}$ (оскільки обидва базиси є ортонормальними) [8, 9]. Гістограми значень проекцій для вейвлетів Хаара та Добеші наведені на рис. 3,а та 3,б відповідно.

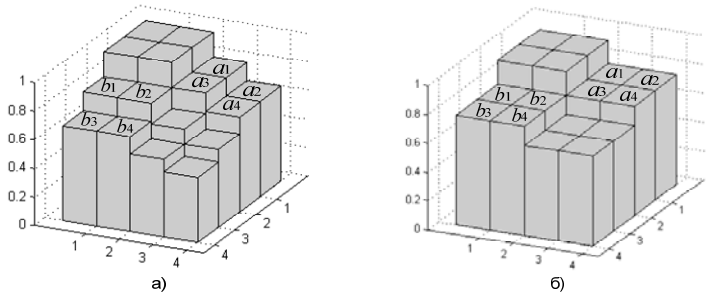

Рис.3. Значення проекцій векторів вейвлет-базисів на «головну» частину базису ДКП: а) базис Добеші, б) базис Хаара

Встановлений за допомогою проекцій зв'язок між базисами дозволяє обирати елементи для формування об'єктів стеганографічного маніпулювання. Вибір сукупностей елементів $\{a_1, a_2, a_3, a_4\}$ та $\{b_1, b_2, b_3, b_4\}$ пояснюється міркуванням про наслідки їх зміни на зображення (спотворення) з одного боку та чутливість відображення цих змін за умови JPEG-стиснення (робастність) з другого.

На ефективність шаблонної схеми вбудовування суттєво впливає вибір значення TH. За умови маніпулювання в області вейвлет-коефіцієнтів $LH2$ та $HL2$, їх значення коливатимуться навколо нуля. Тому вибір $TH = 0$ дозволить збільшити кількість вбудованих

двобітових порцій таємних даних за фіксованих обмежень на спотворення (рис. 4).

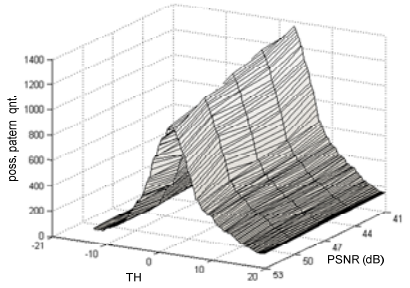

Рис. 4. Залежність кількості вбудованих шаблонів від значення TH та допустимого рівня PSNR

Повертаючись до вирішення задачі

$$\max_{d}\left(\max_{\Omega}\int e^{\det}(q,d)r(q,d,\Omega)f(q)dq\right) \tag{13}$$

стосовно запропонованої схеми та об'єкту стеганографічного маніпулювання, необхідно визначити особливості формування Ω. Очевидно, інтерпретація Ω в області зображення повинна бути однозначною. З іншого боку Ω є єдиним аргументом першого етапу оптимізації, але формується поступово за допомогою Ω_j, $j=1\ldots m$. Тому необхідно, щоб усім можливим значенням Ω_j відповідало оптимальне співвідношення між робастністю та рівнем спотворень. Тому для кожного j-го об'єкту при всіх наперед встановлених (табульованих) значеннях q_i потрібно поставити і вирішити задачу мінімізації спотворень.

Однак особливості обмежень не дозволяють застосовувати методи класичної оптимізації для вирішення сформульованої задачі [10]. Це пояснюється по-перше, необхідністю отримання цілочисельного результату (значення пікселів – цілі числа), по-друге, після ДКП та відповідного q_i квантування шаблонна інтерпретація значень вейвлет-коефіцієнтів повинна співпадати з порцією вбудованих даних:

$$\left\|P^{org}-P^{stg}\right\|^2 \to \min, \tag{14}$$

за обмежень

$$\begin{cases} p_{i,j}^{stg}\in Z, \quad i,j=1\ldots 8; \\ \mathbf{M}^{emb}\times(\mathbf{D}\times\mathbf{C}\times Q_i(\mathbf{C}\times\overline{P}^{stg})-\mathbf{TH})\le\mathbf{0}, \end{cases} \tag{15}$$

де $\overline{P}^{stg}$ – стовбець, що представляє пікселі P^{stg}; $Q_i(\bullet)$ – оператор квантування відповідно до i-ї умови; $\mathbf{M}^{emb}$ – маска, що інтерпретує порцію даних для вбудовування; **TH** та **0** – стовбці, що містять лише значення TH і 0 відповідно.

Етапи оптимізації стеганографічної моделі

У розділі насамперед пропонується метод, покликаний забезпечити субоптимальність рішення для всіх можливих значень Ω_j, $j=1\ldots m$, потім – метод оптимального формування Ω.

Єдиною перепоною на шляху розв'язання поставленої наприкінці попереднього розділу задачі методом найменших квадратів з лінійними обмеженнями є нелінійність оператора $Q_i(\bullet)$. Це пояснює необхідність ітеративного підходу використання даного методу при наближенні до оптимуму [11].

Запропоновано еволюційний алгоритм, суть якого полягає в наступному. Генотипом є вектор G_i довжиною 64, елементи якого приймають значення з $\{0,1\}$. Кожне покоління p

формується сукупністю $\mathbf{G}^p = \{G_i^p\}, \quad i = 1 \ldots g$. Для утворення $\mathbf{G}^{p+1}$:

1) здійснюється вибір c найкращих носіїв $\dot{G}_i^p$ генотипу з найменшим значенням показників

$$A_i = \sum_{j=1}^{64} (G_{i,j}^p - \dot{G}_{i,j}^p), \tag{16}$$

$$\dot{G}_{i,j}^p = \begin{cases} 0, G_{i,j}^p = 0; \\ 1, Q_i^i(\mathbf{C} \times \overline{P}^{stg^p}) \neq Q_i^i(\mathbf{C} \times \overline{P}^{stg^{p-1}}); \quad , \\ -1, Q_i^i(\mathbf{C} \times \overline{P}^{stg^p}) = Q_i^i(\mathbf{C} \times \overline{P}^{stg^{p-1}}), \end{cases} \tag{17}$$

де $\overline{P}^{stg^p}$ отримуємо внаслідок розв'язання задачі

$$\left\| P^{org} - P^{stg^p} \right\|^2 \to \min, \tag{18}$$

за обмежень

$$\begin{cases} p_{i,j}^{stg^p} \in Z, \quad i, j = 1 \ldots 8; \\ \mathbf{M}^{emb} \times (\mathbf{D} \times \mathbf{C} \times (\widehat{\mathbf{C}}^{G_i^p} \times \overline{P}^{mid^p} + \breve{\mathbf{C}}^{G_i^p} \times \overline{P}^{stg^{p-1}}) - \mathbf{TH}) \leq -\Delta^p; \end{cases} \tag{19}$$

тоді проміжне стегозображення на ітерації p буде:

$$\overline{P}^{stg^p} = \mathbf{C} \times (\widehat{\mathbf{C}}^{G_i^p} \times \overline{P}^{mid^p} + \breve{\mathbf{C}}^{G_i^p} \times \overline{P}^{stg^{p-1}}), \tag{20}$$

де $\widehat{c}_{l,m}^{G_i^p} = G_{i,l}^p \cdot c_{l,m}$; $\breve{c}_{l,m}^{G_i^p} = (1 - G_{i,l}^p) \cdot c_{l,m}$; $\widehat{c}_{l,m}^{G_i^p} \subset \widehat{\mathbf{C}}^{G_i^p}$, $\breve{c}_{l,m}^{G_i^p} \subset \breve{\mathbf{C}}^{G_i^p}$; $\overline{P}^{mid^p}$ – стовбець проміжних значень пікселів, Δ^p – стовбець елементів із значенням Δ^p, яке є додатнім та визначається на основі $\mathbf{G}^p$ та Δ^{p-1};

2) отримуємо $g = C_c^2$ комбінацій схрещених послідовностей $\ddot{G}_i^p$ шляхом утворення однієї точки розриву для двох $\dot{G}_l^p$ та $\dot{G}_m^p$, $l \neq m$, і попарним їх суміщенням;

3) реалізується заміна з випадковим результатом (мутація) для всіх значень - 1, внаслідок чого отримуємо $\mathbf{G}^{p+1}$: $\mathbf{G}^{p+1} \Leftarrow \ddot{\mathbf{G}}^p$,

$$\forall i, j \; G_{i,j}^{p+1}(-1) = \begin{cases} 1, p^{mut}(1) = y; \\ 0, p^{mut}(0) = 1 - y, \end{cases} \tag{21}$$

де y – певне стале значення. Еволюція триватиме, доки не виконається умова (15), або Δ^p не перевищить певний встановлений поріг $T\Delta$.

Таким чином, основна властивість розв'язання запропонованим методом полягає в ітеративному генеруванні директив вбудовування, що покликано забезпечити найвищу чутливість за умови квантування з параметром q_i. Однак збіжність до умов (15) не може бути обґрунтована, тому, з метою заощадження обчислювальних ресурсів, встановлено $T\Delta$ [10, 11].

Наступний етап передбачає визначення Ω. Для спрощення при постановці та вирішенні задачі використовуються лише значення спотворень d_i^j, які відповідають збереженню відповідної порції таємних даних у j-му фрагменті зображення за i-ї умови квантування коефіцієнтів ДКП при JPEG-стисненні. Якщо співвідношення між d_i^j та q_i є найбільш вдалим, це відображується одиницею в i-й позиції вектора Ω_j, де решта позицій є нулями. Для визначення таких співвідношень необхідно брати до уваги усі m об'єктів та загальне

обмеження на спотворення Td. Головною особливістю, яка використовується при розв'язанні, є можливість визначення впливу на значення цільової функції та спотворення при виборі Ω_j незалежно від решти об'єктів.

За умови відомого та незмінного стегоключа і таємних даних, кожна порція даних співвідноситься з певним фрагментом зображення. Нехай умову квантування, що відповідає вбудовуванню j-ї порції даних з мінімальним спотворенням $d^j_{\min}$, позначимо $q^j_{\min}$. Тоді нижня межа загальних спотворень зображення $Td_{\min} = \sum_j d^j_{\min}$. При задаванні Td необхідно дотримуватись $Td \geq Td_{\min}$. Таким чином, при робастному вбудовуванні даних у j-й фрагмент з параметром $q^j_i \neq q^j_{\min}$ отримуємо покращення (збільшення) критерію E на ΔE^j_i та відповідне збільшення спотворень на Δd^j_i. За умови фіксованого набору значень $q_i, i = 1 \ldots r$, кількість варіантів оптимізації E відповідно лише до j-го фрагменту не перевищуватиме $r-1$. Нехай в результаті кожної ітерації алгоритму оптимізації отримуємо підтвердження або спростовування переходу від $q^j_{\min}$ до q^j_i для всіх m фрагментів, де для кожного j-го фрагменту може встановлюватися незалежне від інших i-те значення параметру квантування. Якщо для j-го фрагменту можливість переходу відкинута, то при подальших ітераціях параметр q_i не розглядається у якості варіанта переходу. Якщо перехід підтверджено, на наступній ітерації перевіряється можливість цього ж варіанту переходу. Оптимізацію закінчено, коли для всіх спростувань відкинуто останній можливий перехід, або отримано m підтверджень. Отже у випадку найповільнішого розв'язання, де в результаті кожної ітерації спростовується лише один перехід серед m, вимагається не більше $m(r-1)$ ітерацій для досягнення збіжності [11].

Останнім аргументом оптимізації є Td, який визначається в результаті вирішення задачі без обмежень.

Експеримент

Метою експерименту є порівняння ефективності приховування даних розробленим методом та методами, що широко використовуються на практиці. Для порівняння обрано: метод останнього значущого біту (ОЗБ) [12], шаблонний метод на основі цілочисельного вейвлет-перетворення (IWT) [6] та метод, що оперує в області ДКП [13]. В обрані зображення за єдиним стегоключем було вбудовано таємні дані. Ефективність методів визначалася за двома залежностями: таємність стегоманіпуляцій та робастність вбудованих даних від параметра q, що задає ступінь стиснення. Оскільки розробка методу велася на основі запропонованого критерію ефективності вбудовування, то порівняння з рештою методів за цим критерієм та згаданими вище залежностями дозволить встановити адекватність критерію.

Відповідно до описаних особливостей проектування стегометоду, для постановки та вирішення задачі оптимізації вбудовування необхідно попередньо визначити розподіл $f(q)$ та функцію стегоаналітичної ентропії детектування $e^{\det}(q,d)$. Залежність $f(q)$ встановлена шляхом експертного розпізнавання популярних та широко використовуваних зображень у градаціях сірого розміром 256×256, що в залежності від потреб оглянутих web-сторінок оброблялися JPEG алгоритмом з різним значенням параметра q. При визначенні $e^{\det}(q,d)$ для кожного q_i (значення q_i змінювалися від 1 до 0.65 з кроком 0.05) було сформовано навчальну та тестову вибірки. Перша використовувалась для тренування SVM відповідно до запропонованого в [4] вектору характеристик, на другій визначалася середня ймовірність вірного детектування в залежності від значення спотворень d. Зображення у навчальній та

тестовій вибірках не співпадають. Кожна вибірка наполовину складається з оригінальних зображень (кількістю 400), решта – стегозображення, отримані з оригінальних за допомогою описаної шаблонної схеми вбудовування. На рис. 5 зображено графік функції ймовірності детектування $p^{\det}(q,d)$.

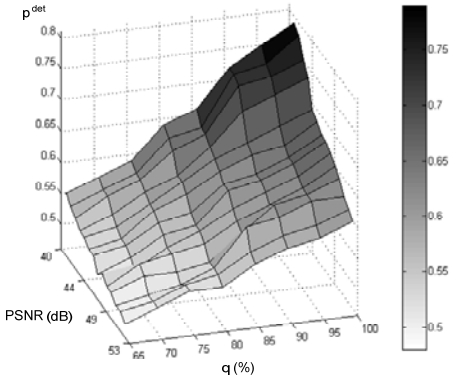

Рис.5. Залежність ймовірності детектування від параметра q та рівня спотворення(PSNR).

Внаслідок проведення описаних етапів оптимізації вбудовування 2000 бітів таємних даних у вейвлет-коефіцієнти Хаара відповідно до критерію E, кількісний показник ефективності, що є середнім для 20 зображень, складає 0.63. Для описаного в [6] методу на основі цілочисельного вейвлет-базису значення критерію складає 0.48, ефективність вбудовування в область ДКП [13] оцінюється 0.42, стеганографічна ефективність методу [12] на основі ОЗБ – 0.28.

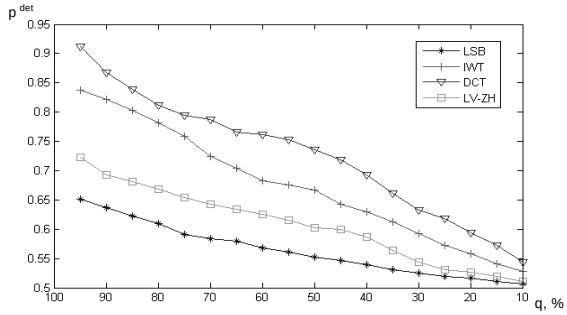

Рис.6. Залежність ймовірності детектування $p^{\det}$ від параметра якості JPEG-стиснення q

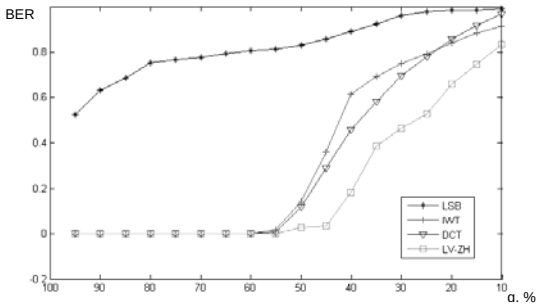

Рис.7. Зв'язок робастності r вбудованих даних від параметра q

З метою демонстрації адекватності критерію та ефективності розробленого методу, наведено два графіки залежностей ймовірності детектування $p^{\det}$ від q (рис. 6) та робастності вбудовування r від q (рис. 7), що наглядно висвітлюють переваги та недоліки кожного з оцінених вище методів.

Висновки

Розроблено стеганографічний метод, що використовує принцип шаблонного вбудовування в області вейвлет-коефіцієнтів. Особливістю метода є врахування вимог таємності та робастності до JPEG-перетворення, що реалізовано шляхом їх об'єднання за допомогою запропонованого критерію. Таким чином, задачу розробки було поставлено як задачу оптимізації з обмеженнями, яку вирішено поетапно.

Запропонований підхід дозволяє підвищити загальну ефективність вбудовування даних, що підтверджено експериментально при порівнянні з популярними стегометодами.

Недоліком методу є складність, що обумовлена диференційною особливістю вбудовування та, як наслідок, необхідністю ітеративного вирішення чисельних задач оптимізації.

Проте, використані підходи оптимізації допускають пошук компромісів між обчислювальною складністю та ефективністю вирішення, що є метою подальших досліджень. Ще одним перспективним напрямком досліджень є використання запропонованого підходу вбудовування за інших перетворень обробки зображень (не лише JPEG).

СПИСОК ЛІТЕРАТУРИ

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – СПб.: Солон-Пресс, 2002. – 272с.

2. Johnson N., Duric Z., Jajodia S. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, New York. – NY.: Kluwer Academic Pub, 2000. – 200p.

3. Glavieux A. Channel Coding in Communication Networks. – London: Hermes Science Pub. Ltd., 2007. – 416p.

4. Zou D., Shi Y., Su W., Xuan G. Steganalysis based on Markov Model of Thresholded Prediction-Error Image // IEEE ICME Conference Record, 2006. – P. 1365-1368.

5. Pennebaker W., Mitchell J. JPEG: Still Image Compression Standard. – NY.: Kluwer Academic Pub., 1993.

6. Васюра А.С., Лукічов В.В. Метод вбудовування даних на основі алгоритму вейвлет-стиснення зображень // Матеріали XIII міжнародної конференції з автоматичного управління „Автоматика-2006". – Вінниця: Универсум-Вінниця, 2007. – С. 491-495.

7. Marvel L. M., Retter C. T. Spread Spectrum Image Steganography // IEEE Transactions on Image Processing, 1999. – № 8. – P. 1075-1083.

8. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. – М.: Триумф, 2003. – 320с.

9. Mertin A. Signal Analysis: Wavelets, Filter Banks, Time-Frequency Transforms and Applications. – NY.: John Wiley and Sons, 1999. – 310p.

10. Fletcher R. Practical Methods of Optimization, second edition. – NY.: John Wiley and Sons, 2000. – 450p.

11. Kelley C. T. Iterative Methods for Optimization. Frontiers in Applied Mathematics. – Philadelphia: SIAM, 1999. – 196p.

12. Wu H.C., Wu N.I., Tsai C.S., Hwang M.S. Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods // IEEE Transactions on Image and Signal Processing, 2005. – № 5. – P. 611-615.

13. Quan L., Qingsong A Combination of DCT-Based and SVD-Based Watermarking Scheme // IEEE ICSP Conference Record, 2004. – № 1. – P. 873-876.

Васюра Анатолій Степанович – директор інституту, професор кафедри автоматики та інформаційно-вимірювальної техніки;

Лукічов Віталій Володимирович – здобувач кафедри автоматики та інформаційно-вимірювальної техніки.

Вінницький національний технічний університет