УДК 681.322:621.391

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

МЕТОД ШАБЛОННОГО ВБУДОВУВАННЯ ДАНИХ У ВЕЙВЛЕТ-КОЕФІЦІЄНТИ НА ОСНОВІ КРИТЕРІЮ СТЕГАНОГРАФІЧНОЇ СТІЙКОСТІ

Розглянуто особливості вбудовування, що визначають секретність і стійкість прихованих даних. З метою розробки ефективного стеганографічного методу синтезовано критерій, який використано у якості цільової функції при вбудовуванні.

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

Стеганографія зображень є галуззю, що стрімко розвивається протягом останніх десяти років. Її ціль може бути окреслена як секретність і стійкість до різноманітних перетворень приховування даних. Відповідно практичні задачі, що вирішуються в її межах, у більшій чи меншій мірі стосуються аспектів секретності та робастності [1, 2].

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

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

Отже, проектування будь-якої стегосистеми можна розглядати як задачу умовної оптимізації, де цільова функція певним чином пов'язує робастність із ступенем секретності, 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 в бінарній класифікації зображень на основі властивостей, що зазнають найбільших змін при вбудовуванні. Особливо перспективними є критерії на основі методу опорних векторів (SVM – support vector machines) [4], найбільшою перевагою яких є ефективність класифікації точок-характеристик у багатомірному просторі ознак.

Серед методів обробки зображень найбільшою популярністю користуються методи стиснення. Найбільший коефіцієнт ущільнення здатні забезпечити методи стиснення із втратами [5]. Стандарт стиснення JPEG і досі використовується широко, незважаючи на впровадження більш ефективних форматів на основі вейвлет-перетворень (наприклад, JPEG2000). Така ситуація, вочевидь, зумовлена інертністю концепцій розробки програмного забезпечення в цій сфері, що у 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 секретністю 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 секретних даних, що дозволяє підвищити їх стійкість.

Під час розробки сучасних методів приховування в більшості випадків оптимізується одна з якостей секретності або робастності. Використання критерію, що поєднує зазначені якості, підвищить ефективність стегозахисту. Аспект актуальності не вичерпується лише цим критерієм: запропоновано адаптивний шлях його покращення. Для цього враховуються властивості кожного об'єкта стеганографічного маніпулювання, який несе елементарну частку секретних даних.

Передбачається, що особливості запропонованого в статті підходу забезпечать високу ефективність стегометоду на його основі. Розробка такого методу є **метою** цього **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-метод опорних векторів для класифікації зображень.

Основна ідея методу опорних векторів − переведення вихідних векторів у простір більш високої розмірності та пошук поділяючої гіперплощини з максимальним проміжком у цьому просторі (рис. 1). Дві паралельні гіперплощини будуються по обидва боки гіперплощини, що розділяє класи. Поділяючою гіперплощиною буде гіперплощина, що максимізує відстань до двох паралельних гіперплощин. Алгоритм працює на основі припущення, що чим більше різниця або відстань між цими паралельними гіперплощинами, тим менше буде середня помилка класифікатора.

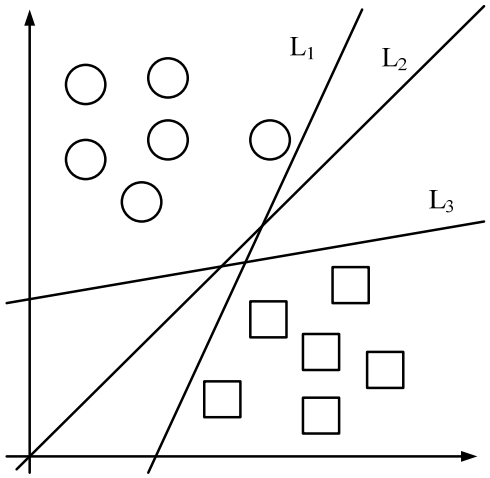

Рис.1. Декілька класифікуючих прямих (гіперплощин)

Нехай точки описуються: $\{(x_1, c_1), (x_2, c_2), ..., (x_n, c_n)\}$, де c_i приймає значення 1 або −1 залежно від того, до якого класу належить точка x_i. Кожна x_i − це p-мірний вектор, зазвичай нормалізований значеннями [0,1] або [-1,1]. Якщо точки не будуть нормалізовані, то точка з більшими відхиленнями від середніх значень координат точок дуже сильно вплине на класифікатор. Розглянемо це як навчальну вибірку, у якій для кожного елемента вже заданий клас, до якого він належить. Необхідно, щоб алгоритм методу опорних векторів класифікував їх у той самий спосіб. Для цього будуємо поділяючу гіперплощину, що має вигляд: $w \cdot x - b = 0$.

Вектор w – перпендикуляр до поділяючої гіперплощини. Параметр b залежить від найкоротшої відстані гіперплощини до початку координат. Якщо параметр b дорівнює нулю,

гіперплощина проходить через початок координат, що обмежує рішення.

При оптимальному поділі опорні вектори й гіперплощини паралельні оптимальній (рис. 2). Можна показати, що ці паралельні гіперплощини можуть бути описані таким рівнянням (з точністю до нормування): $w \cdot x - b = 1$, $w \cdot x - b = -1$.

Якщо навчальна вибірка лінійно роздільна, то можемо вибрати гіперплощини таким чином, щоб між ними не лежала жодна точка навчальної вибірки, й потім максимізувати відстань між гіперплощинами. Ширину смуги між ними легко знайти з міркувань геометрії, вона дорівнює $\frac{2}{\|w\|}$, у такий спосіб потрібно мінімізувати $\|w\|$. Щоб виключити всі точки зі смуги, повинні виконуватися для всіх i умови: $\begin{bmatrix} w \cdot x_i - b \geq 1 \\ w \cdot x_i - b \leq -1. \end{bmatrix}$

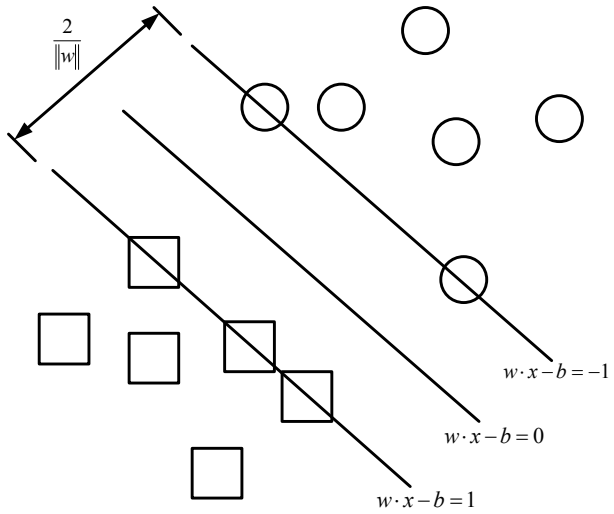

Рис. 2. Оптимальна поділяюча гіперплощина для методу опорних векторів, побудована на точках із двох класів

Це може бути також записано у вигляді:

$$c_i(w \cdot x_i - b) \geq 1, \ 1 \leq i \leq n. \tag{1}$$

У випадку лінійної подільності проблема побудови оптимальної поділяючої гіперплощини зводиться до мінімізації $\|w\|$, за умови (1). Це завдання квадратичної оптимізації, що має вигляд: $\begin{cases} \|w\|^2 \to \min \\ c_i(w \cdot x_i - b) \geq 1, \quad 1 \leq i \leq n. \end{cases}$

За теоремою Куна − Такера це завдання еквівалентне двоїстому завданню пошуку сідлової точки функції Лагранжа

$$\begin{cases} L(w,b;\lambda) = \frac{1}{2}\|w\|^2 - \sum_{i=1}^{n} \lambda_i c_i (w_i \cdot x_i) \to \min_{u,b} \max_{\lambda} \\ \lambda_i \geq 0, \quad 1 \leq i \leq n \\ \begin{bmatrix} \lambda_i = 0 \\ w \cdot x_i - b = c_i, \end{bmatrix} \quad 1 \leq i \leq n \end{cases} \tag{2}$$

де $\lambda = (\lambda_1, ..., \lambda_n)$ - вектор двоїстих змінних.

Зведемо це завдання до еквівалентного завдання квадратичного програмування, що містить тільки двоїсті змінні:

$$\begin{cases} -L(\lambda) = -\sum_{i=1}^{n}\lambda_i + \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\lambda_i\lambda_j(c_ic_j(x_i\cdot x_j - b) - 1) \to \min_{\lambda} \\ \lambda_i \geq 0, \quad 1 \leq i \leq n \\ \sum_{i=1}^{n}\lambda_i c_i = 0. \end{cases} \tag{3}$$

Припустимо, що вирішили це завдання, тоді w і b можна знайти за формулами:

$w = \sum_{i=1}^{n}\lambda_i c_i x_i$, $b = w\cdot x_i - c_i$.

Алгоритм класифікації може бути записаний у вигляді:

$$a(x) = sign\left(\sum_{i=1}^{n}\lambda_i c_i x_i \cdot x - b\right). \tag{4}$$

Звернемо увагу, що підсумовування йде не по всій вибірці, а тільки по опорних векторах, для яких $\lambda_i \neq 0$.

Для того, щоб алгоритм міг працювати у випадку, коли класи лінійно нероздільні, дозволимо йому допускати помилки на навчальній вибірці. Введемо набір додаткових змінних $\xi_i \geq 0$, що характеризують величину помилки на об'єктах x_i, $1 \leq i \leq n$. Зм'якшимо обмеження нерівності (2), так само введемо в мінімізуючий функціонал штраф за сумарну помилку:

$$\begin{cases} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}\xi_i \to \min_{\varpi, b, \xi_i} \\ c_i(w\cdot x_i - b) \geq 1 - \xi_i, \quad 1 \leq i \leq n \\ \xi_i \geq 0, \quad 1 \leq i \leq n. \end{cases}$$

Коефіцієнт C − параметр настроювання методу, що дозволяє регулювати відношення між максимізацією ширини поділяючої смуги й мінімізацією сумарної помилки.

Аналогічно за теоремою Куна − Такера зводимо завдання до пошуку сідлової точки функції Лагранжа:

$$\begin{cases} L(w,b;\xi,\lambda,\eta) = \frac{1}{2}\|w\|^2 - \sum_{i=1}^{n}\lambda_i(c_i(w_i\cdot x_i) - 1) - \sum_{i=1}^{n}\xi_i(\lambda_i + \eta_i - C) \to \min_{u,b,\xi}\max_{\lambda,\eta} \\ \xi_i \geq 0, \lambda_i \geq 0, \eta_i \geq 0, \quad 1 \leq i \leq n \\ \left[\begin{array}{l} \lambda_i = 0 \\ c_i(w\cdot x_i - b) = 1 - \xi_i, \end{array}\right. \quad 1 \leq i \leq n \\ \left[\begin{array}{l} \eta_i = 0 \\ \xi_i = c_i, \end{array}\right. \quad 1 \leq i \leq n. \end{cases}$$

За аналогією зведемо це завдання до еквівалентного:

$$\begin{cases} -L(\lambda) = -\sum_{i=1}^{n}\lambda_i + \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\lambda_i\lambda_j c_i c_j(x_i\cdot x_j) \to \min_{\lambda} \\ 0 \leq \lambda_i \leq C, \quad 1 \leq i \leq n \\ \sum_{i=1}^{n}\lambda_i c_i = 0. \end{cases}$$

На практиці для побудови машини опорних векторів вирішують саме це завдання, а не (3), тому що гарантувати лінійну подільність точок на два класи загалом практично неможливо.

Отже, 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 – імовірність правильної класифікації. Для описаного 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

$$dct_{i,j}^{jpeg} = \frac{Q_{i,j}}{q}\,\mathrm{round}\left(\frac{dct_{i,j}}{Q_{i,j}}q\right), \tag{5}$$

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. 3 відображає типовий розподіл f_q.

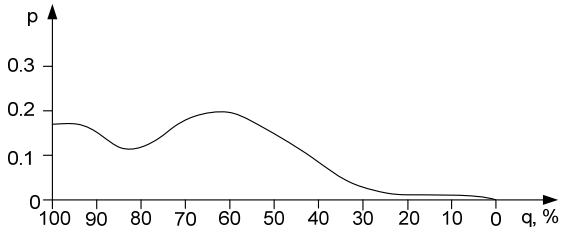

Рис. 3. Типовий розподіл значень параметра q

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 в ці блоки, можна отримати адаптивну до вимог таємності та робастності стегосистему.

Критерій ефективності вбудовування має бути інтегральним, оскільки замість значення q відомий лише розподіл f_q. Отже, 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:

$$E = \sum_i z_i f_{q_i} = \sum_i e_i^{\det} r_i f_{q_i}\,. \tag{6}$$

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} порівняно з оригінальним I^{org}), попередній вираз набуде вигляду:

$$E(d) = \sum_i e_{i,d}^{\det} r_{i,d} f_{q_i}\,. \tag{7}$$

Для випадку неперервної зміни умов квантування маємо:

$$E(d) = \int e^{\det}(q,d) r(q,d) f(q) dq \,. \quad (8)$$

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'єкта. Кінцева задача проектування стегометоду формалізується:

$$\max_d \left(\max_{\Omega} \int e^{\det}(q,d) r(q,d,\Omega) f(q) dq \right). \quad (9)$$

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

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) [7], шаблонний метод на основі цілочисельного вейвлет-перетворення (IWT) [6] та метод, що оперує в області ДКП [8]. В обрані зображення за єдиним стегоключем було вбудовано таємні дані. Ефективність методів визначалася за двома залежностями: секретність 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 залежно 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] вектора характеристик, на другій визначалася середня ймовірність правильного детектування залежно від значення спотворень d. Зображення в навчальній та тестовій вибірках не збігаються. Кожна вибірка наполовину складається з оригінальних зображень (кількістю 400), решта – стегозображення, отримані з оригінальних за допомогою описаної шаблонної схеми вбудовування.

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, стеганографічна ефективність методу [7] на основі ОЗБ – 0.28, ефективність вбудовування в область ДКП [8] оцінюється 0.42.

З метою демонстрації адекватності критерію та ефективності розробленого методу, наведено два графіки залежностей імовірності детектування $p^{\det}$ від q (рис. 4) та

робастності вбудовування r від q (рис. 5), що наглядно висвітлюють переваги та недоліки кожного з оцінених вище методів.

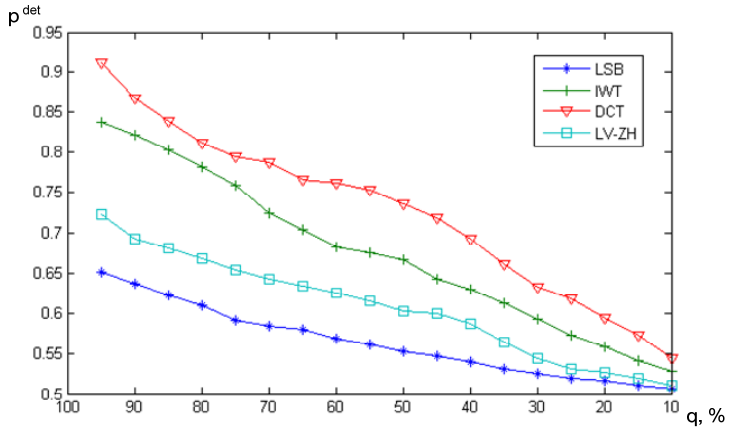

Рис. 4. Залежність імовірності детектування p^{det} від параметра якості JPEG-стиснення q

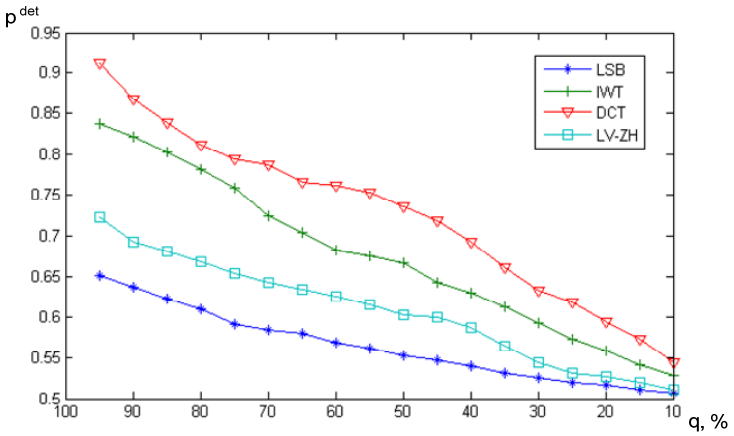

Рис. 5. Зв'язок робастності r вбудованих даних від параметра q

Висновки. Розроблено стеганографічний метод, що використовує принцип шаблонного вбудовування в області вейвлет-коефіцієнтів. Особливістю методу є врахування вимог таємності та робастності до JPEG-перетворення, що реалізовано шляхом їх об'єднання за допомогою запропонованого критерію.

Запропонований підхід дозволяє підвищити загальну ефективність вбудовування даних, що підтверджено експериментально при порівнянні з популярними стегометодами. Недоліком методу є складність, що зумовлена диференційною особливістю вбудовування та, як наслідок, необхідністю ітеративного вирішення чисельних задач оптимізації.

СПИСОК ЛІТЕРАТУРИ

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – СПб.: Солон-Пресс, 2002. – 272 с. – ISBN 5-98003-011-5.

2. Johnson N. F. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures / N. F. Johnson, Z. Duric, S. Jajodia. – Berlin: Springer, 2001. – 160 p. – ISBN 0-7923-7204-2.

3. Glavieux A. Channel Coding in Communication Networks / A. Glavieux. – London: Hermes Science Pub. Ltd., 2007. – 416 p. – ISBN 978-1-905209-24-8.

4. Zou D. Steganalysis based on Markov Model of Thresholded Prediction-Error Image / D. Zou, Y. Shi, W.Su, G. Xuan // IEEE ICME. – 2006. – № 1. – P. 1365 − 1368. – ISBN: 1-4244-0367-7.

5. Pennebaker W. JPEG: Still Image Compression Standard / W. Pennebaker, J. Mitchell. – NY.: Kluwer Academic Pub., 1993. – 650 p. – ISBN 0-4420-1272-1.

6. Метод вбудовування даних на основі алгоритму вейвлет-стиснення зображень: праці конференції, 25 − 28 вер. 2006 р., Вінниця. Т. 1 / Відп. ред. В. М. Дубовой. – Вінниця: Универсум-Вінниця, 2007. – С. 491 − 495. – ISBN 978-966-641-210-5.

7. Wu H.C. Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods / H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang // IEEE Transactions on Image and Signal Processing. – 2005. – № 5. – P. 611 − 615. – ISBN 0-8247-2777-0.

8. Quan L. Combination of DCT-Based and SVD-Based Watermarking Scheme / L. Quan, A. Qingsong // IEEE ICSP Conference Record. – 2004. – № 1. – P. 873 − 876. – ISBN 0-7803-8510-1.

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.