УДК 681.322:621.391

А. С. Васюра, к. т. н., проф.; Є. А. Золотавкін

ДЕТЕКТУВАННЯ ТАЄМНОГО ВМІСТУ В СТИСНЕНИХ ФРАКТАЛЬНИМ АЛГОРИТМОМ ЗОБРАЖЕННЯХ

Запропоновано критерій для встановлення присутності прихованих даних у фрактальному коді зображень. Використано підхід, що полягає в оцінюванні стеганографічної загрози кожного окремого запису у фрактальному коді. Дана оцінка базується на особливостях методів фрактального стиснення. Кількість позитивно оцінених блоків використовується для подальшого загального висновку про можливість існування вбудованих даних. Ефективність розробленого детектора встановлено експериментально та порівняно з існуючими.

Ключові слова: *стеганографія, приховування інформації, фрактальне стиснення зображення, детектування, стегоаналітичний критерій.*

Вступ

Серед галузей захисту інформації стеганографія зображень займає унікальну нішу та підтверджує свою ефективність стрімкими темпами розвитку. Це частково пояснюється популярністю криптографічних заходів захисту та необхідністю таємного зберігання ключа. Непомітна передача конфіденційних повідомлень теж складає значну частину практичного арсеналу. Широкого застосування стеганографія зображень знайшла в галузі захисту авторських прав, що призвело до відокремлення напрямку розробки та впровадження цифрових водяних знаків (ЦВЗ).

Кожна з практичних задач вимагає конкретного підходу для її вирішення, однак в більшості стеганографічна ефективність забезпечується поєднанням якостей таємності та робастності. При цьому рівень зазначених якостей необхідно співвідносити з об'ємом вбудованих даних [1].

Підходи забезпечення необхідного рівня стійкості описані в літературі [2]. На противагу робастності, питання таємності є неоднозначним, що пояснюється великою кількістю демаскуючих ознак. Це зумовлює складність розробки абсолютно адекватного детектора. Однак відносний показник правильного детектування дозволяє оцінити ефективність стегоаналітичного критерію. Протистояння виявленню за умови підвищення пропускної здатності таємного каналу передбачає володіння критерієм кращим, ніж у перехоплювача.

Незважаючи на різноманітність стегодетекторів, їх спільною структурною особливістю є бінарний класифікатор, що використовує певні чутливі до наявності таємного вмісту характеристики. Послідовність характеристик кожного зображення може бути представлена вектором, як у роботах [3, 4], де класифікація виконувалась за допомогою апаратів векторного поділу (SVM). Однак з метою покращення статистики детектування, навчання класифікатора має відбуватися на вибірці, що представляє дві підмножини зображень: перша утворена оригінальними зображеннями; друга – стегозображеннями. Причому ефективність визначається ступенем відповідності параметрів вбудовування в тренувальній сукупності дійсним параметрам тестової стегосистеми. Таким чином якість стегоаналізу знижується за невідомих параметрів реальної (тестової) стегосистеми або за умови їх зміни в процесі вбудовування.

Другою особливістю стегокритерію є склад характеристик, що мають сприяти відокремленню стегозображень від оригінальних зображень. Одним зі шляхів досягнення цього є врахування притаманних певному формату зображень властивостей, що зумовлені алгоритмом обробки.

Широке розповсюдження алгоритмів стиснення зумовлюється значними досягненнями в області обробки зображень. Це пояснює той факт, що переважна більшість сучасних форматів представлення зображень забезпечують стиснення з втратами. Файли форматів стиснених зображень рідко піддаються додатковій обробці та стиску, тому забезпечують більшу робастність при вбудовуванні даних. З іншого боку для більшості алгоритмів стиснення з втратами важко оцінити змінені особливості оригінального зображення, що сприяє приховуванню.

Фрактальні алгоритми забезпечують вдале співвідношення між коефіцієнтом стиснення та якістю і володіють унікальною властивістю деталізації при довільному масштабуванні [5, 6]. Розвиток фрактального стиснення забезпечує популярність форматів на його основі (як, наприклад, STING), що підтверджує доцільність їх стеганографічного використання.

Принцип фрактального стиснення зображень

Врахування особливостей алгоритму обробки зображень важливе для визначення характеристик та подальшого детектування таємного змісту, тому досягнення поставленої мети вимагає розгляду принципу фрактального стиснення зображень.

Фрактальна архівація ґрунтується на представленні зображення в компактній формі за допомогою коефіцієнтів системи ітерованих функцій (IFS). IFS – набір тривимірних афінних перетворень, що переводять одне зображення в інше. Перетворенню піддаються точки в тривимірному просторі (двомірний простір площинного зображення та яскравість).

Нехай парою (M, d) задається метричний простір цифрових зображень, де d – дана метрика. Для стиснення зображення $I \in M$ необхідно знайти відображення $\tau : M \to M$, яке задовольняє такі умови:

$$\exists\, 0 < z < 1, \quad \forall \mu, \nu \in M, d(\tau(\mu), \tau(\nu)) \le z.d(\mu, \nu), \tag{1}$$

$$d(I, \tau(I)) \cong 0, \tag{2}$$

де μ та ν є різними фрагментами зображення I.

Тоді за умови рівномірного розбиття

$$\forall \mu_i \in I, i = \overline{1,n}, \quad I = \bigcup_i \mu_i, \quad \mu_i \cap \mu_j = 0, i \ne j \tag{3}$$

та існування сукупності відображень $T = \{\tau_i\}$ таких, що $d(\mu_i, \tau_i(\nu_i)) \le \varepsilon$, справедливий вираз

$$d(I, F^m(T)) \le \frac{\varepsilon}{1-z}, m \to \infty, \tag{4}$$

де $F^l(T) = \bigcup_i (\mu_i^l \leftarrow \tau_i(\nu_i^{l-1}))$.

Відображення τ_i є афінним перетворенням та

$$\tau_i = N_i \circ S_i \circ G_i, \tag{5}$$

де G – оператор геометричної частини, що забезпечує стиск з коефіцієнтом z повороти на певні кути і симетричні відображення фрагментів зображення; S – оператор переносу, що реалізує зсув кожної елементарної частини фрагмента зображення у двомірному просторі; N – оператор інтенсивності фрагмента зображення, що змінює значення інтенсивності e – елементарної частини (пікселя) таким чином: $N_i(e) = s_i \cdot e + o_i$, де s – контрастність, o – яскравість [5, 6].

На практиці кількість ітерацій m обмежується невеликим числом, яке є достатнім для забезпечення візуальної подоби при задовільному ε. Метричний простір (M, d)

визначається способом розбиття на рангові та доменні блоки μ та ν відповідно. Зазвичай зображення I має прямокутну форму, рангові та доменні блоки є квадратами з розмірами $k \times k$ та $2k \times 2k$ пікселів, $z = 0{,}5$ та

$$d(\mu_l, \mu_m) = \sqrt{\sum_{i=1}^{k}\sum_{j=1}^{k}(e_{i,j}^{\mu_l} - e_{i,j}^{\mu_m})^2} \ . \qquad (6)$$

Отже, метою фрактального алгоритму стиснення зображень є пошук сукупності перетворень T для деякого зображення I при достатньо малому ε. Істотним обмеженням цього процесу є умова $inf(T) << inf(I)$, де функція inf визначає кількість інформації, необхідної для опису аргументу. Однак на практиці інтерпретація (I, ε) в T не є однозначною. Можливість маніпулювання T дозволяє застосовувати стеганографічну техніку, що використовує різноманітність взаємозамінних фрагментів реальних зображень.

Особливості розбиття зображення на доменні та рангові блоки можуть суттєво впливати на зазначену різноманітність варіантів співставлень. Найбільш розповсюдженою є схема квадро-дерева, що зображена на рис. 1. Таке розбиття спрощує пошук відповідностей між фрагментами та забезпечує високу різноманітність. Якщо не знайдено доменного блоку v_i, що внаслідок відображення τ_i відповідає ранговому μ_i в межах ε, ранговий блок ділиться на чотири менших блоки. З погляду стиснення таке подрібнення рангових блоків не є ефективним порівняно, наприклад, з HV-поділом [7]. Однак для стеганографічного використання це обертається перевагою: більша кількість рангових блоків дозволяє приховати більшу кількість даних.

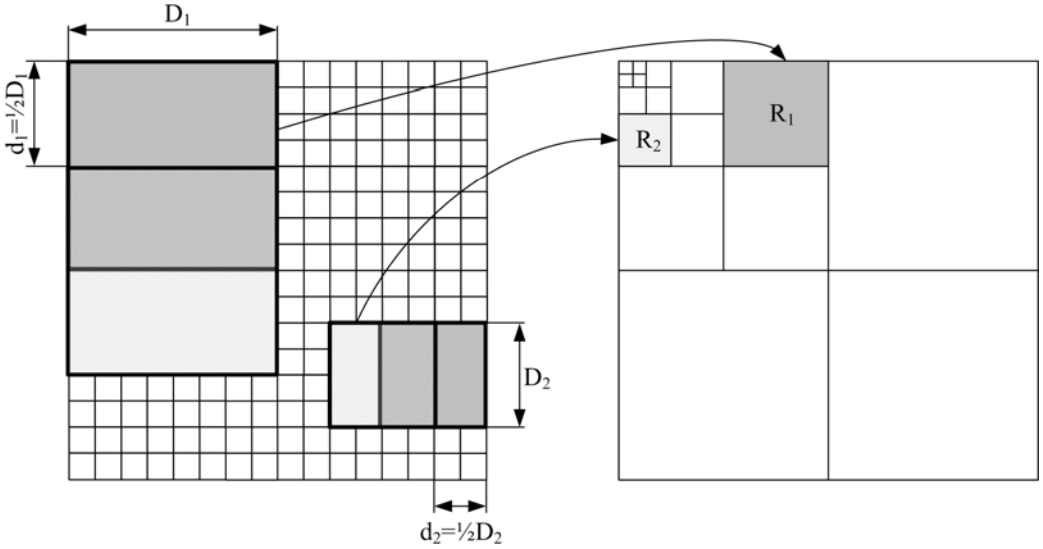

Рис. 1. Ілюстрація фрактального стиснення за схемою квадро-дерева

Універсальність квадратної форми блоків забезпечує різноманітність їх інтерпретацій шляхом встановлення різних параметрів відображень. Це дозволяє зменшити кількість доменних блоків (збільшення d_1, d_2) за рахунок широкого набору параметрів, що є виправданим при стисненні. Отже, стеганографічне застосування обмежується цією особливістю зазначеної схеми розбиття.

Наступним важливим моментом практичної реалізації моделі фрактального стиснення є спосіб організації пошуку відповідностей між ранговими та доменними блоками. Недоліком фрактального стиснення є значна складність за часом при повному переборі всіх варіантів співставлень блоків [8]. При вирішенні цієї проблеми зазвичай застосовують такі заходи: 1) замість пошуку доменного блоку, що найкращим чином відображається в певний ранговий,

задовольняються першим знайденим подібним в межах ε; 2) використовують різноманітні характеристики блоків з метою класифікації, що дозволяє значно спростити пошук. Саме перший пункт визначає основні вимоги таємності, оскільки другорядність обраного для співставлення доменного блоку не може узгоджуватися з жодною модифікацією методу фрактального стиснення зображень. Нехтування цією властивістю призведе до виникнення демаскуючої ознаки.

Деякі модифікації методів фрактального стиснення відрізняються від описаного базового підходу значенням коефіцієнту масштабування z, набором афінних перетворень та оператором N [7]. Однак навіть опосередкований вплив таких змін на особливості вбудовування даних є незначним, оскільки стосується лише відображення блоків і не пов'язаний з порядком їх вибору та кількістю.

Метод вбудовування даних на основі фрактального алгоритму

У літературі представлене широке розмаїття методів стеганографічного використання принципів фрактального стиснення [9 – 11], однак найвищу робастність забезпечують методи [10, 11], оскільки маніпулюють безпосередньо кодом стисненого зображення. Тому підвищення таємності вбудовування останніх підходів (шляхом розробки ефективного стегодетектора) забезпечить високий рівень захисту.

Як було зазначено, різноманітність взаємозамінних фрагментів зображення дозволяє кодувати таємні дані. Для цього в кожному випадку співставлення з ранговим блоком усі домени-кандидати необхідно описати: визначити множину кандидатів, співвіднести з кожним елементом множини відповідний числовий індекс.

У цьому випадку справедливо зауважити, що втрати таємної інформації зумовлені помилками невідповідності індексів при вбудовуванні та витяганні. З іншого боку, підвищення стеганографічної ефективності також може відбуватися шляхом збільшення кількості індексів.

Максимальна кількість різних індексів дорівнює кількості елементів у множині [12, 13]. За такого способу індексації множину кандидатів необхідно визначати не тільки при вбудовуванні, але й при витяганні даних. Складність відновлення індексів, зумовлена відсутністю оригінального зображення, може призвести до вищезгаданої невідповідності та втрати інформації.

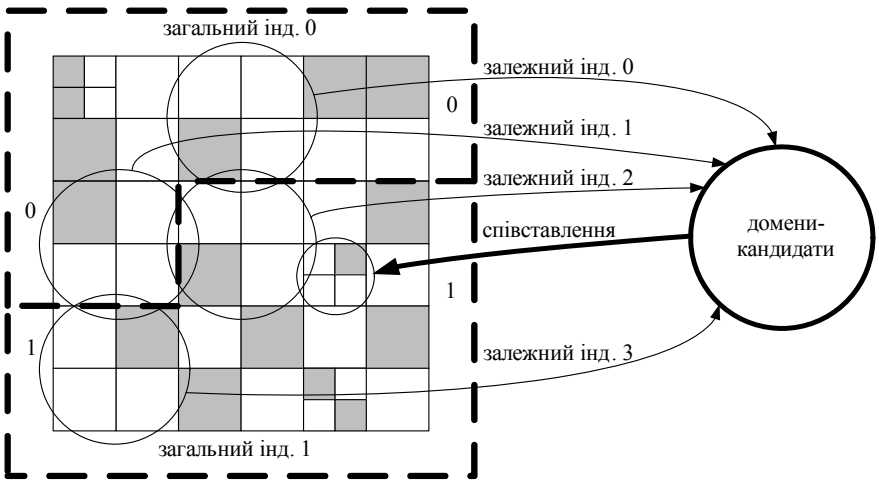

Рис. 2. Способи індексації доменних блоків при вбудовуванні даних

У разі універсального способу визначення індексів, їх кількість однакова для всіх множин, тому в межах однієї множини вони можуть повторюватися. Схематична ілюстрація двох описаних способів індексації наведена на рис. 2. Як видно, окрім повторень індексів,

відсутність елементів для їх інтерпретації при вбудовуванні (наприклад, фрагмент з шаховою текстурою) є ще одним недоліком універсальної індексації.

Реалізація способів як універсальної, так і локальної індексації може відрізнятися для різних стегометодів, однак принципово меншу обчислювальну складність та вищу надійність вбудовування забезпечить універсальний спосіб.

У ході вбудовування з метою забезпечення максимальної пропускної здатності за умови таємності при використанні універсальної індексації необхідно визначити такі особливості: 1) кількість індексів; 2) у випадку декількох елементів з необхідним індексом в межах однієї множини доменів-кандидатів, необхідно оптимізувати вибір одного з них; 3)необхідно визначити кількість стеганографічних зіставлень (частка рангових блоків).

Отже, при вирішенні поставленої задачі умова таємності є основним обмеженням, яке необхідно формалізувати за допомогою критерію.

Стегоаналітичний критерій

Висновок про прихований вміст пропонується виносити на основі проміжної характеристики зображень, що представляє кількість «підозрілих» рангових блоків, якими вважаються ті, що отримано всупереч фрактальному алгоритму стиснення. Рішення про «підозрілість» виноситься на основі класифікації умов (характеристик) співставлення доменного блоку з даним ранговим.

Недоліком використання існуючих критеріїв на основі SVM [3, 4] для детектування описаної стегосистеми є врахування лише локальних міжпіксельних характеристик. Тому для визначення «підозрілих» блоків пропонується набір характеристик, що стосується лише особливостей фрактального стиснення. Класифікацію на «підозрілі» та «непідозрілі» блоки вирішено проводити також з допомогою SVM, ефективність якого є досить високою.

Як було зазначено, обґрунтований висновок про узгодженість співставлення конкретного доменного та рангового блоків з фрактальним алгоритмом можна зробити лише на основі усієї множини блоків. Це пояснюється вимогою першочерговості обраного доменного блоку, а також необхідністю порівняння міри локальної відповідності оточенню рангового блоку з іншими варіантами співставлень.

У роботі [14] на основі властивостей самоподоби фрагментів зображень розроблено критерій детектування спотворених областей. Для опису характерних областей зображення використовувались підходи кластеризації та пониження розмірності представлення. Усі фрагменти, що не увійшли до жодного кластеру, вважалися спотвореними.

З іншого боку, перевірка першочерговості доменного блоку вимагає лише встановлення можливостей співставлення доменів, що йому передують. Найповніше представлення про умови «конкуренції» доменів-кандидатів з обраним для співставлення блоком також можна отримати лише на основі взаємного розташування їх точок-характеристик.

Отже, рішення про локальну відповідність та першочерговість кожного обраного доменного блоку можна приймати на основі положення точок-характеристик фрагментів зображення в просторі ознак. Однак навіть для невеликого за розмірами блоку 8×8 пікселів загальна кількість ознак дорівнює 64, що робить опис взаємного розташування блоків (при великій їх кількості) занадто громіздким для класифікації за допомогою SVM.

Для пониження розмірності характеристичного вектора $\overline{\mathbf{q}}_{m,i}$, що описує особливості співставлення доменного блоку v_m в позицію рангового μ_i, пропонується формувати його зі скалярних значень $q^j_{m,i}$, що є відстанями між обраним доменним блоком та іншими фрагментами. При такому спрощенні не враховуються попарні відстані між рештою фрагментів, окрім того, що розглядається. Але при збільшенні кількості фрагментів ефективність характеристики зростає. Цьому сприяє також додатковий набір параметрів, що представляють собою міру відносної міжпіксельної невідповідності по периметру блоків.

Ступінь подібності обраного доменного блоку v_m оригінальному ранговому μ_i, який він замінив, описується g скалярними значеннями $q_{m,i}^j, 1 \le j \le g$ – відстанями між ним та g найбільш подібними блоками серед усього зображення. Для підтвердження того, що вибір цього блоку носив першочерговий характер, використовується h скалярних значень $q_{m,i}^j, g+1 \le j \le g+h$ – відстаней між ним та h найбільш подібними доменними блоками, які передують обраному.

З метою адекватного представлення ступеня подібності оригінальному ранговому блоку μ_i, обраний доменний (трансформований) блок $\tau_{m,i}(v_m)$ пропонується розглядати разом з оточенням у вигляді рамки f_i навколо нього (рис. 3) [15]. Тоді $q_{m,i}^j = \alpha_1 d(f_i, \dot{f}_i^j) + \alpha_2 d(\tau_{m,i}(v_m), \dot{\mu}_i^j), i = \overline{1,n}, 1 \le j \le g$, де $\alpha_1 \ge 1, \alpha_2 \le 1$ – константи, $\dot{f}_i^j$ та $\dot{\mu}_i^j$ – фрагменти, що за формою повторюють f_i та μ_i, і є складовими блоку зображення $\dot{b}_i^j = \dot{f}_i^j \circ \dot{\mu}_i^j$, який задовольняє умову

$$\begin{cases} \min\limits_{\dot{b}_i^j} q_{m,i}^j, \; j = 1 \\ \min\limits_{\dot{b}_i^j \notin \bigcup_{k=1}^{j-1} \dot{b}_i^k} q_{m,i}^j, \; j > 1 \end{cases}. \tag{7}$$

Врахування рамки навколо рангового блоку пояснюється тим, що вбудовування шляхом зміни відповідностей між ранговими та доменними блоками не охоплює усіх блоків зображення. Оскільки пікселі рамки належать восьми різним блокам, вона є більш стійкою до спотворень вбудовування. Ця властивість зумовлює вибір коефіцієнтів $\alpha_1 \ge \alpha_2$.

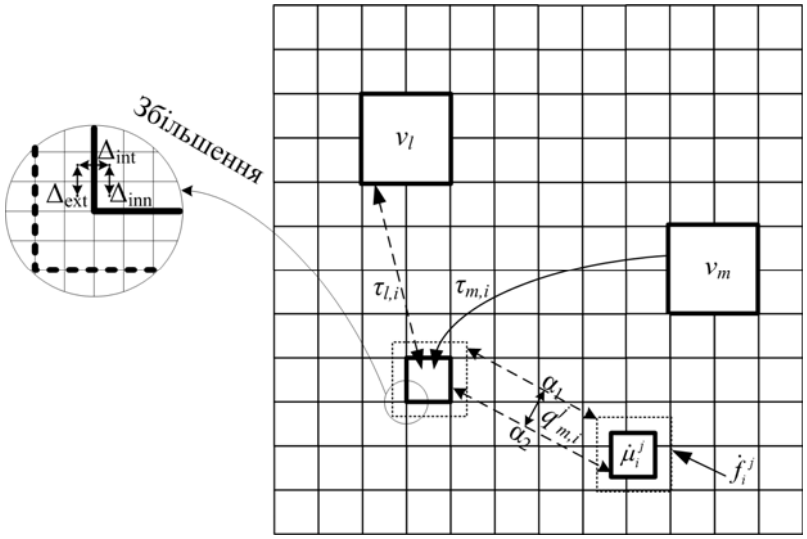

Рис. 3. Визначення характеристик співставлення

Як видно з рис. 3, місце положення $\dot{b}_i^j$ не обмежується лише стандартною сіткою. З іншого боку, при визначенні $q_{m,i}^j$ не передбачається застосування операторів N та G. Отже, для оцінки ступеня подібності між обраним доменним та оригінальним ранговим блоками використовуються лише природні закономірності зображення [14].

Характеристикою, що визначає якість першочерговості, є послідовність елементів $q_{m,i}^j = d(\tau_{m,i}(v_m), \tau_{l,i}(v_l)), l < m, g+1 \le j \le g+h$, де індекс l не повинен повторюватися при різних j та $q_{m,i}^j \to \min$. Обґрунтуванням даної характеристики є така властивість: чим

більше доменних блоків, що достатньо близькі до обраного, тим більша ймовірність його другорядності.

З метою доповнення наведених вище двох типів характеристик пропонується розглянути особливості зміни інтенсивності пікселів по периметру блоків. При порівнянні різниці за модулем між пікселями, як показано на рис. 3, може з'ясуватися, що одна з трьох пар пікселів забезпечує більше значення цього показника, ніж інші дві, отже, перехід в цьому напрямку позначається як різкий (верхній індекс shp). За умови порушення відповідностей між доменним та ранговим блоками, це підтверджується більшою часткою різких переходів між сусідніми блоками. Отже, кількість різких переходів $\Delta_{\text{int}}^{shp}$ доцільно використовувати для представлення узгодженості блоку з його оточенням. Застосування цієї характеристики до блоків-претендентів $v_l, l < m$ на місце рангового μ_i дозволить уточнити ступінь локальної узгодженості з даною областю зображення та підвищить якість висновку про першочерговість. Передбачається враховувати цю характеристику також при з'ясуванні локальної узгодженості доменного блоку v_m.

Отже, характеристичний вектор $\overline{\mathbf{q}}_{m,i}$, що описує особливості співставлення $\tau_{m,i}(v_m) \to \mu_i$ з метою подальшої класифікації за допомогою SVM, можна структурно представити таким чином:

$$\begin{aligned} &\left\{q_{m,i}^{j} = \alpha_1 d(f_i, \dot{f}_i^{j}) + \alpha_2 d(\tau_{m,i}(v_m), \dot{\mu}_i^{j}), 1 \le j \le g\right\} \cup \\ &\cup \left\{ \begin{cases} q_{m,i}^{j} = d(\tau_{m,i}(v_m), \tau_{l,i}(v_l)) \\ q_{m,i}^{j+h} = \Delta_{\text{int}}^{shp}[\tau_{l,i}(v_l)] \end{cases} \middle| \, l < m, g+1 \le j \le g+h \right\} \cup \\ &\cup \left\{q_{m,i}^{g+2h+1} = \Delta_{\text{int}}^{shp}(\tau_{m,i}(v_m))\right\}. \end{aligned} \tag{8}$$

Перевагами такої характеристики є висока чутливість до порушень порядку дій, що передбачений фрактальним стисненням зображень. Обчислювальна складність навчання та класифікації при використанні SVM також може бути значно зменшена в порівнянні з [3, 4], оскільки довжина вектора $\overline{\mathbf{q}}_{m,i}^{j}$ складає $g + 2h + 1$ і за умови $g = h = 10$ забезпечується необхідна чутливість для детектування таємного вмісту (при стеганографічному використанні 50 % рангових блоків).

Експеримент

Основною задачею експерименту є визначення критичної кількості Q_S «підозрілих» блоків у зображенні, перевищення якої дозволяє зробити висновок про виконане вбудовування. Для цього необхідно провести тренування SVM з використанням описаного набору ознак, що об'єднанні в характеристичний вектор. При тренуванні повинні використовуватися різноманітні зображення з таємними даними, що вбудовані за описаною стеганографічною схемою, а також зображення без таємного вмісту. На результат тестування не впливатиме кількість вбудованих у стегозображення даних, оскільки кожний блок аналізується окремо.

Оптимізація порогового значення Q_S має на меті мінімізацію ентропії детектування. При цьому задача детектування обмежується наперед визначеною схемою вбудовування, що передбачає незмінний та відомий об'єм таємних даних у стегозображенні. Порівняльний аналіз результатів детектування змішаної сукупності зображень на основі критеріїв [3, 4] та запропонованого критерію дозволить оцінити його ефективність.

З метою класифікації на «підозрілі» та «непідозрілі» блоки для тренування SVM використовувалось 200 зображень у градаціях сірого розміром 256×256. Кількість

вбудованих у зображення даних змінювалася в діапазоні від 300 до 1000 біт, але загальна кількість, узгоджених з фрактальним алгоритмом, та кількість, стеганографічно змінених, рангових блоків була однаковою. При формуванні характеристичного вектора $g = h = 10$, отже, загальна довжина його склала 31, $\alpha_1 = 1.2, \alpha_2 = 0.8$, товщина рамки 3 пікселя. Ефективність класифікації, встановлена внаслідок тестування, склала 70.3%.

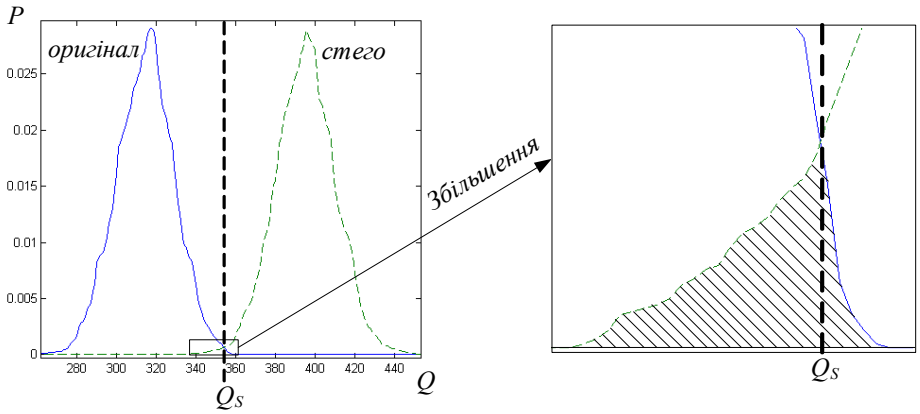

Рис. 4. Результат детектування таємного вмісту

При визначенні Q_S для детектування стегозображень з об'ємом таємних даних рівним 400 біт було використано дві залежності, графіки яких зображені на рис. 4. Перша з них відображає кількість оригінальних зображень з відповідною кількістю «підозрілих» блоків. Друга – кількість стегозображень з певним числом «підозрілих» блоків. Оптимальне значення Q_S має забезпечувати мінімум заштрихованої площі, що відповідає точці перетину графіків. Для даних умов вбудовування встановлено $Q_s = 354$. Отже, при кількості «підозрілих» блоків, що перевищує Q_S, зображення вважається стеганографічно значимим. Результуюча ймовірність правильного детектування на основі запропонованого стегоаналітичного критерію склала 97.1%.

Для перевірки ефективності детектування за допомогою критеріїв [3, 4] навчання SVM для кожного з них відбувалося на тренувальній сукупності, половину якої складали стегозображення з об'ємом таємних даних 400 біт. Імовірність вірного детектування склала 56.7% і 52.5% для [3] та [4] відповідно, що підтверджує надзвичайні переваги запропонованого способу детектування таємного вмісту у фрактальному коді зображень над існуючими критеріями.

Висновки

У роботі запропоновано стегоаналітичний критерій, призначення якого полягає в детектуванні зображень з прихованим вмістом, який вбудовано на етапі стиснення фрактальним алгоритмом. З метою синтезу ефективного критерію було визначено особливості фрактального стиснення, які змінюються внаслідок вбудовування даних. На основі цих особливостей сформовано характеристики окремих блоків зображення з метою подальшої бінарної класифікації за допомогою SVM. Отже, кількість «підозрілих» блоків, що отримано внаслідок класифікації, використовується для встановлення присутності таємного вмісту шляхом порівняння з критичним порогом Q_S.

Такий підхід дозволяє значно підвищити ефективність детектування стегозображень, які зазнали вбудовування внаслідок зміни послідовностей дій, що передбачені фрактальним алгоритмом стиснення. Завдяки використанню запропонованих характеристик, точність класифікації на «підозрілі» та «непідозрілі» блоки склала 70.3%, що дозволяє детектувати

стегозображення з об'ємом таємних даних усього 400 бітів з точністю 97.1%.

З іншого боку, основним недоліком є необхідність характеристики та класифікації кожного блоку зображення. Але невелика розмірність характеристичного вектора та можливість паралельної організації однотипних обчислень дозволяють сподіватися на ефективне вирішення проблеми.

У подальших дослідженнях планується розглянути адаптивні підходи вбудовування даних у фрактальний код зображень та підвищити їх ефективність.

СПИСОК ЛІТЕРАТУРИ

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

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

3. 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.

4. Chen, X., Wang, Y., Tan, T., Guo, L. Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix // IEEE ICPR'06, 2006. – № 3. – P. 1107 – 1110.

5. Barnsley, M., Hard, L. Fractal Image Compression. – Wellesley: A.K. Peters, Ltd., 1993. – 256 p.

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

7. Zhao, E., Liu, D. Fractal Image Compression Methods: A Review // ICITA'05, 2005. – P. 756 – 759.

8. Polvere, M., Nappi, M. Speed-up in Fractal Image Coding: Comparison of Methods // IEEE TIP, 2000. – № 6. – P. 1002 – 1009.

9. Bas, P., Chassery, J. M., Davoine, F. Using the Fractal Code to Watermark Images // Proc ICIP'98, 1998. – № 1. P. 469 – 473.

10. Li, C., Wang, S. Digital Watermarking Using Fractal Image Coding // IEICE Trans. Fund., 2000. – № 6. – P. 1286 – 1288.

11. Liao, P., Chen, C., Chen, C., Pan, J. Interlacing Domain Partition for Fractal Watermarking // IIH-MSP'06, 2006. – P. 441 – 444.

12. Васюра А.С., Золотавкін Є.А., Лукічов В.В. Адаптивний метод вбудовування даних у фрактальний код зображень // Інформаційні технології та комп'ютерна інженерія. – Вінниця, 2006. – № 2. – С. 105 – 110.

13. Васюра А.С., Золотавкін Є.А. Визначення та забезпечення стійкості методу таємної передачі даних на основі фрактального стиснення зображення // Вісник Хмельницького національного університету. – Хмельницький, 2007. – № 2 .– С. 133 – 138.

14. Amano, T. Correlation Based Image Defect Detection // IEEE ICPR'06, 2006. – P. 163 – 166.

15. Liang, X., Chenrong, H., Haijun, L., Huizhong, W. Concealment of Damaged Block Coded Images Using Intelligent Two-Step Best Neighborhood Matching Algorithm // Proc CGIV'05, 2005. – P. 38 – 42.

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

Золотавкін Євген Анатолійович – аспірант кафедри автоматики та інформаційно-вимірювальної техніки.

Вінницький національний технічний університет