УДК 681.511:3

О.Ю. Пузиренко

# ПРОТОКОЛ ОЦІНКИ ЕФЕКТИВНОСТІ АЛГОРИТМІВ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

## Постановка проблеми

Питання, пов'язані із здійсненням дієвої захищеності авторських прав і прав інтелектуальної власності, з оперативним контролем доступу до сучасного медіапродукту або конфіденційної інформації, протягом останніх років залишаються проблемами державного масштабу і гостро стоять перед правовласниками і споживачами інформаційного контенту. Комп'ютерна злочинність, завдяки використанню з кримінальною метою сучасних інформаційних технологій (ІТ), стала не лише прибутковою, але й досить безпечною для порушників справою [1,2]. Зрозуміло, що в такій ситуації особлива увага повинна бути приділена превентивному створенню інформаційних систем, які були б надійно захищеними від різноманітних загроз. Одним з альтернативних засобів захисту інформації є *комп'ютерна стеганографія* [3,4].

Крім того, сучасний етап розвитку ІТ характеризується і підвищенням вимог до якості надаваних послуг, у даному випадку — послуг у захисті інформації. Достатньо важливим є встановлення конкретної причини неефективної роботи тих або інших методів і алгоритмів захисту інформації в існуючих інформаційно-телекомунікаційних системах, оскільки визначення загальної бази критеріїв робитиме результати оцінки ефективності значимими для більш широкої аудиторії.

## Аналіз останніх досліджень і публікацій

Дослідження методів і алгоритмів комп'ютерної стеганографії інтенсивно ведуться вже протягом багатьох років. У сучасній літературі представлено детальні описи і програмні реалізації більшості з відомих на сьогодні алгоритмів [3-5], що, таким чином, спричинило потребу в наявності методики наочної оцінки відносної ефективності зазначених алгоритмів проти різноманітних видів атак на стеганосистеми.

На сьогодні найбільш відомими і широковживаними наборами тестів оцінки якості стеганоалгоритмів (а саме, алгоритмів вбудовування цифрових водяних знаків (ЦВЗ)) є *StirMark*, *UnZign* та ін. [6]. Зазначені тести не орієнтовані на атаку яких-небудь конкретних алгоритмів і, в принципі, можуть розглядатися як універсальні тести стійкості останніх. Стеганоалгоритми тестуються з метою виявити наявність вбудованого ЦВЗ і, за позитивного результату, — декодувати вбудоване повідомлення. У випадку виявлення ЦВЗ і/або повного розкриття змісту повідомлення при застосуванні деякої з множини атак тесту, досліджуваний алгоритм позначається як такий, що не пройшов даний тип атаки (зазвичай, у відповідність до цієї атаки ставиться значення «1», у протилежному випадку — «0»). Відсоток безпомилково виявлених при цьому ЦВЗ (кількість пройдених атак, віднесена до загальної їх кількості) є показником ефективності, який використовується для порівняння відносної ефективності алгоритмів стеганографії.

Даючи змогу виявити існуючі слабкі місця алгоритмів вбудовування ЦВЗ (переважно це стосується геометричних спотворень [3,6]), дані програми мають безліч недоліків, що ускладнюють або ж взагалі унеможливлюють прийняття безпомилкового і всебічно виваженого рішення щодо ефективності того чи іншого алгоритму.

Основним недоліком є те, що не береться до уваги імовірність "помилкової тривоги" (імовірність виявлення ЦВЗ у пустому контейнері). Таким чином, для двох алгоритмів, що мають однакову імовірність "пропуску цілі" (імовірність невиявлення ЦВЗ у заповненому контейнері), але різні імовірності "помилкової тривоги", буде винесене однакове рішення стосовно їхньої ефективності. Крім того, не проводиться відокремлена оцінка якості стеганодетектора і декодера, а помилково видобуте повідомлення розглядається як помилково виявлений ЦВЗ, що, безперечно, викривлює результати. Також, при оцінці

стійкості алгоритмів до конкретних атак, програмами використовуються один і той самий ключ. Проте, оскільки результати встановлення наявності ЦВЗ є залежними від ключа, очевидно, що для одержання більш точної характеристики якості виконання детектора і декодера повинна використовуватися велика кількість ключів. Ще одним недоліком можна назвати відсутність оцінки часу вбудовування і виявлення/видобування ЦВЗ. Зрештою, оцінки ефективності, одержані для різносторонніх атак, при формуванні загального показника ефективності об'єднуються як такі, що мають однакову вагу, — інакше кажучи, робиться припущення, що на практиці всі атаки і контейнери мають однакову імовірність появи. Втім, у багатьох практичних випадках такий підхід є помилковим, оскільки деякі види атак (напр., компресія із втратами) можуть здійснюватися набагато частіше за інші (напр., дзеркальне відображення).

Окрім *ефективності стеганодетектора і декодера* визначальними є й інші дві характеристики стеганосистем: обмеженими для певних видів атак є пропускна здатність і гранична стійкість до трансформації [3,4]. *Пропускна здатність* (ПЗ) — максимально можлива усереднена кількість інформації, що може бути вбудована до одного елементу контейнера (напр., пікселя або часового відліку) і надійно видобута згодом — безпомилково або ж із відсотком помилкових біт (BER — *Bit Error Rate*), що не перевищує встановленого порогу. *Гранична стійкість алгоритму до атаки* при трансформації контейнера (напр., JPEG-компресії) визначає межу перетворень структури контейнера або найбільш важку атаку, яку може витримати алгоритм, за умови подальшого надійного виявлення/видобування повідомлення.

## Постановка завдання

Метою роботи є представлення нового протоколу оцінки якості реалізації відомих і прогнозування ефективності розроблюваних алгоритмів комп'ютерної стеганографії, в якому усунуто недоліки існуючих тест-систем. Головну увагу слід зосередити на представленні повного набору тестів, що повинні бути виконані для одержання наочної, однозначної і надійної характеристики ефективності досліджуваного стеганоалгоритму. Також необхідно представити методику узагальнення окремих результатів для більш компактного відображення загальної ефективності методів стеганографії.

## Виклад основного матеріалу дослідження

**Параметри протоколу.** Вхідною інформацією пропонованої тест-системи є програмні засоби вбудовування, виявлення і видобування ЦВЗ. Результатом тестування є числові показники і діаграми, що відображують ефективність досліджуваного стеганоалгоритму по відношенню до різних видів атак. Параметри системи тестування ефективності наступні:

— множина всіх контейнерів $\mathbf{C}^* = \{ c_j^*,\ j = \overline{1, N_{C^*}} \}$;

— множина ключів вбудовування ЦВЗ $\mathbf{W} = \{ w_t,\ t = \overline{1, N_W} \}$;

— множина повідомлень $\mathbf{M} = \{ m_i,\ i = \overline{1, N_M} \}$;

— множина атак $\mathbf{A} = \{ a_n,\ n = \overline{1, N_A} \}$;

— множина вагових коефіцієнтів $\mathbf{K} = \{ k_l,\ l = \overline{1, N_K} \}$;

— множина порогових значень ефективності $\mathbf{V} = \{ v_e,\ e = \overline{1, N_V} \}$;

— множина вимог до якості стеганосистеми $\mathbf{Q} = \{ q_r,\ r = \overline{1, N_Q} \}$.

*Контейнери*, що застосовуватимуться у тест-системі, повинні бути різноманітними за розміром і спектральним складом, оскільки саме ці два показники впливають на характеристики стеганографічних систем. Крім того, типи контейнерів в існуючій їх множині (цифрові фотографії, комп'ютерна графіка, фотознімки поверхні Землі з космосу, музичні записи тощо) повинні бути узгодженими з використовуваними у прикладних задачах.

Ключовим параметром тест-системи є потужність множини *ключів*, оскільки від ключа вбудовування ЦВЗ залежить ефективність алгоритмів багатьох стеганометодів. Потужність

множини *повідомлень*, навпаки, не є критичною, — ефективність стеганодекодера більшою мірою визначається можливістю достовірного виявлення ЦВЗ, а не вбудованого повідомлення.

Множина *атак* повинна містити всі види атак, що можуть бути здійснені будь-яким з відомих типів порушників з метою модифікації або "стирання" ЦВЗ [3]. Також повинні бути враховані всі спотворення, що виникають під час: *а)* використання мультимедійного контейнера за його прямим призначенням (напр., в результаті масштабування або переквантування); *б)* передавання; *в)* зберігання і т.п.

Множина *вагових коефіцієнтів* використовується для одержання загальної ефективності стеганосистеми шляхом представлення зваженої комбінації показників ефективності та діаграм (яка є результатом певного сполучення характеристик алгоритму, контейнеру й атак). Дані коефіцієнти повинні відбивати імовірнісний характер подій висування вимог до якості, використання контейнерів або здійснення атак, виходячи з конкретних обставин.

Для можливості проведення оцінки помітності ЦВЗ і якості сприйняття контейнера із вбудованим ЦВЗ повинна використовуватися об'єктивна міра *якості*. Найбільш доцільним є використання показника максимального відношення сигнал/шум (PSNR — *Peak Signal-to-Noise Ratio*), оскільки, не зважаючи на деякі недоліки показника (зокрема, слабку корельованість із сприйманою якістю контейнера [3]), поки що не запропоновано жодної задовільної міри якості, однаково ефективно застосовної для будь-якого типу медіаконтейнера. Що стосується вбудовування ЦВЗ, — може використовуватися множина показників PSNR: напр., 26 дБ для значного, 32 дБ для середнього і 38 дБ для малого об'єму вбудовування. При цьому повинні досліджуватися всі показники якості у даній множині.

**Елементи протоколу.** Тест-система об'єднує у собі модулі вбудовування, атаки, виявлення ЦВЗ / видобування повідомлення, а також модуль оцінки ефективності (**рис.1**).

*Модуль вбудовування* ЦВЗ використовує програмні засоби вбудовування, вхідними даними яких є множини **C**, **W**, **M** і **Q**. Функція прямого стеганоперетворення $\boldsymbol{E}$ вбудовує ЦВЗ $w_i$ та повідомлення $m_i$ до контейнера $c_j$ з урахуванням задоволення вимог до якості $q_r$ заповненим контейнером: $\boldsymbol{E}$: $\mathbf{C} \times \mathbf{W} \times \mathbf{M} \times \mathbf{Q} \rightarrow \mathbf{C}^W$. Дана процедура повторюється для всіх елементів множин **C**, **W**, **M** і **Q**, результатом чого є множина заповнених контейнерів $\mathbf{C}^W$. Потужність множини $\mathbf{C}^W$ дорівнює $N_C \times N_W \times N_M \times N_Q$. Також проводиться оцінка часу, необхідного для вбудовування ЦВЗ і повідомлення до кожного контейнера $c_j$.

*Модуль атаки* використовується для внесення спотворень до всіх заповнених контейнерів з множини $\mathbf{C}^W$ шляхом застосування всіх атак з множини **A**. Результатом є множина $\mathbf{C}^A$ атакованих контейнерів, яка містить $N_C \times N_W \times N_M \times N_Q \times N_A$ елементів.

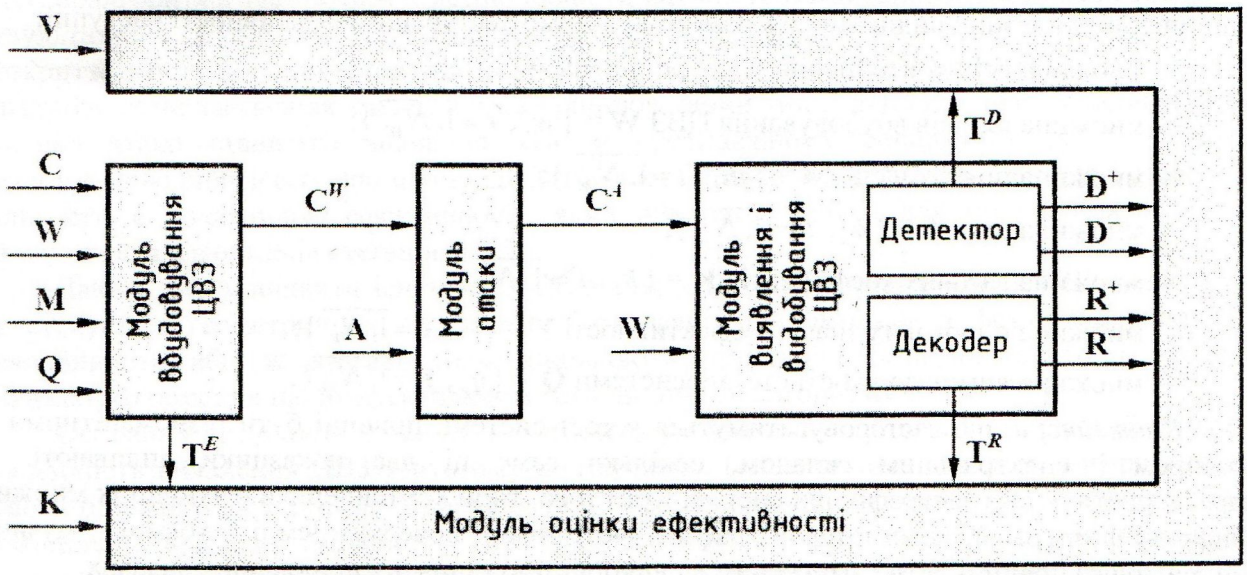


**Рис.1. Блок-схема системи тестування ефективності стеганоалгоритмів**

*Модуль виявлення і видобування ЦВЗ* використовує відповідні досліджувані програмні засоби, вхідними даними яких є множини $\mathbf{C}^A$ і $\mathbf{W}$. Виконується виявлення ЦВЗ за правильним ($w_x$) і помилковим ($w_y$, $y \neq x$) ключами, а також видобування визначених цими ЦВЗ вбудованих повідомлень $\tilde{m} \in \mathbf{M}$ з усіх контейнерів множини $\mathbf{C}^A$. Як наслідок, з кожного атакованого контейнера множини $\mathbf{C}^A$ видобувається дві пари вихідних даних детектора і декодера, що зумовлені використанням правильного і помилкового ключів вбудовування ЦВЗ. Нехай $\mathbf{D}^+$ і $\mathbf{R}^+$ — відповідні множини вихідних даних детектора і декодера при використанні для їх отримання правильного ключа, а $\mathbf{D}^-$ і $\mathbf{R}^-$ — відповідні множини вихідних даних, одержані при використанні помилкового ключа. Як і у випадку вбудовування, здійснюється оцінка і збереження значень часу, що витрачається на операції виявлення/видобування.

Стеганодетектор реалізує тестову функцію, яка видає або дворозрядні рішення про наявність/відсутність ЦВЗ у досліджуваному контейнері: напр., «1» — ЦВЗ виявлено, «0» — ЦВЗ не виявлено (рішення є результатом порівняння статистики, що лежить в основі критерію для перевірки гіпотези, з порогом прийняття рішень), або ж безпосередньо статистику, що лежить в основі критерію, у вигляді дійсних (не двійкових) чисел [3,5]. Вихідними даними стеганодекодера є оцінка вбудованого повідомлення (остання виконується лише за умови надходження від детектора позитивного результату виявлення).

*Модуль оцінки ефективності* використовується для одержання кількісних оцінок або діаграм ефективності досліджуваного алгоритму. Первинними даними є множини вихідних даних детектора ($\mathbf{D}^+$ і $\mathbf{D}^-$) і декодера ($\mathbf{R}^+$ і $\mathbf{R}^-$), множини $\mathbf{T}^E$, $\mathbf{T}^D$ і $\mathbf{T}^R$ проміжків часу виконання кожної з операцій (вбудовування, виявлення і видобування), а також множина вагових коефіцієнтів $\mathbf{K}$. Вихідні дані модуля — якісні оцінки і діаграми, що характеризують відносну ефективність тестованого алгоритму або його придатність для виконання конкретних задач.

**Оцінка ефективності.** За результатами виконання операцій "вбудовування-атака-виявлення-видобування" одержують вихідні дані з декодера і детектора (для правильних і помилкових ключів ЦВЗ), а також тривалості виконання операцій вбудовування, виявлення і видобування. Використовуючи ці основні дані, здійснюють оцінку ефективності алгоритму як по відношенню до атак, здійснюваних на відповідну йому стеганосистему, так і виходячи з часу виконання основних етапів алгоритму.

Для оцінки **стійкості стеганоалгоритму до атак** повинні бути визначені імовірності "помилкової тривоги" і "пропуску цілі". Імовірністю "помилкової тривоги" (помилки 1-го роду) $p_\alpha$ є імовірність виявлення ЦВЗ у пустому контейнері або у контейнері, заповненому ЦВЗ з іншим ключем. У даному випадку $p_\alpha$ встановлюється здійсненням виявлення з помилковим ключем, оскільки це є еквівалентним найбільш несприятливому варіанту. Імовірністю "пропуску цілі" (помилки 2-го роду) $p_\beta$ є імовірність невиявлення ЦВЗ у заповненому ним контейнері.

Якщо *вихідні дані з виходу детектора є недвійковими*, можлива оцінка емпіричного розподілу, який може бути апроксимований теоретичним розподілом $f(u)$. У відповідності з цим, результатом множин $\mathbf{D}^+$ і $\mathbf{D}^-$ є два розподіли: $f^+(u)$ і $f^-(u)$. Нехай $V_{\min}$ і $V_{\max}$ — мінімальне і максимальне середнє значення цих розподілів. Тоді для кожної порогової величини $V \in [V_{\min}, V_{\max}]$ можуть бути обчислені імовірності $p_\alpha$ і $p_\beta$ [7]:

$$p_\alpha(V) = \int_V^\infty f^-(u)\,\mathrm{d}u, \qquad p_\beta(V) = \int_{-\infty}^V f^+(u)\,\mathrm{d}u. \tag{1}$$

Використовуючи (1), визначимо робочу характеристику детектора (DOC — *Detector Operating Characteristic*) — залежність імовірності $p_\alpha$ від імовірності $p_\beta$. Це може бути зроблено шляхом оцінки для будь-якого порогового значення $V$ площ під $f^+(u)$ і $f^-(u)$

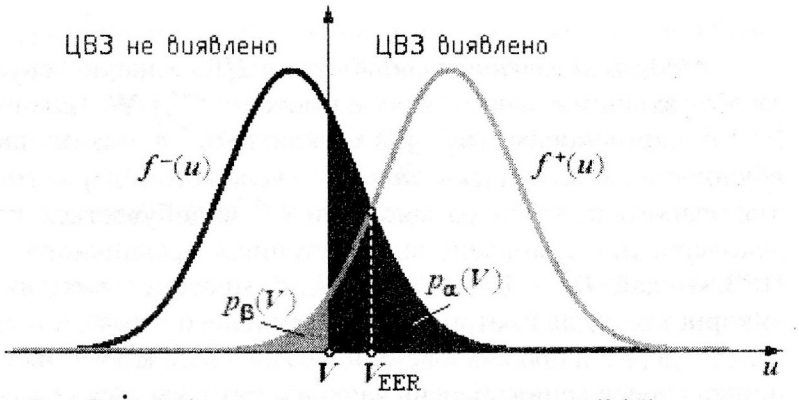


**Рис.2. Імовірності "помилкової тривоги" і "пропуску цілі"**

відповідно ліворуч ($p_\beta$) і праворуч ($p_\alpha$) від порогу (**рис.2**) [8]. Криві DOC обчислюються для кожного контейнера з множини $\mathbf{C}^A$.

Крім того, криві DOC можуть бути визначені безпосередньо з емпіричних розподілів:

$$p_\alpha(V) = \left|\mathbf{D}_V^-\right| / \left|\mathbf{D}^-\right|; \qquad p_\beta(V) = \left|\mathbf{D}_V^+\right| / \left|\mathbf{D}^+\right|, \tag{2}$$

де $\mathbf{D}_V^- = \{u_i > V / u_i \in \mathbf{D}^-\}$; $\mathbf{D}_V^+ = \{u_i < V / u_i \in \mathbf{D}^+\}$; запис $|\mathbf{D}|$ розуміє під собою потужність множини $\mathbf{D}$. Але при цьому, для того щоб мати точність порядку $10^{-N}$, необхідно використовувати як мінімум $10^N$ ключів.

Завдяки найбільш повній характеристиці ефективності алгоритму з точки зору стійкості останнього, крива DOC може розглядатися як міра стеганостійкості. Визначивши DOC, також можна оцінити наступні критерії ефективності (**рис.3**):

— імовірність $p_\beta$ ($p_\alpha$) для фіксованого значення $p_\alpha$ ($p_\beta$);

— коефіцієнт рівної імовірності помилок 1 і 2-го роду (EER — *Equal Error Rate*);

— площу під кривою DOC (т. зв. глобальну оцінку ефективності), $S_{DOC}$.

На підставі критеріїв EER та $S_{DOC}$ можна зробити висновки про відносні переваги і недоліки різних алгоритмів — чим нижчими вони є, тим більш якісною і надійною буде стеганосистема.

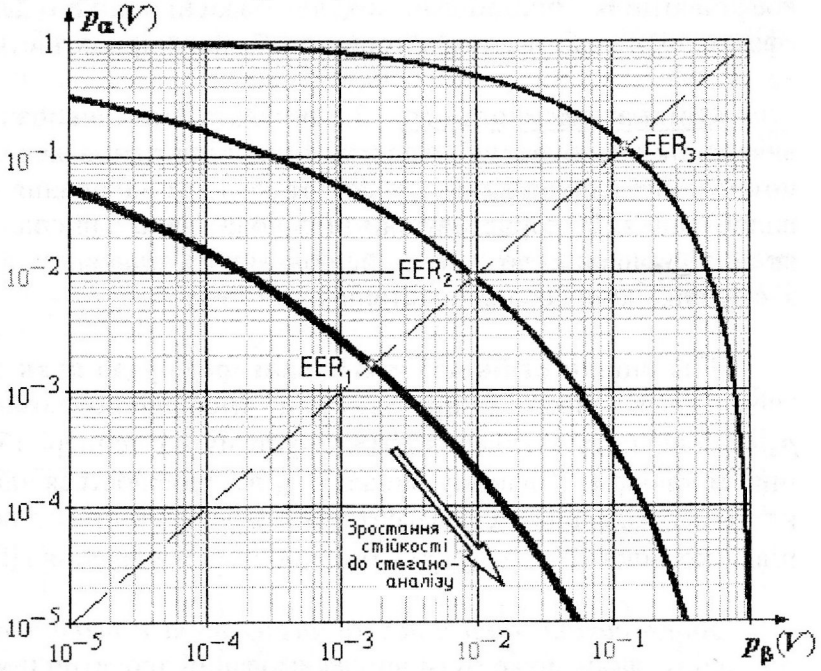


**Рис.3. Робочі характеристики стеганодетекторів**

Регулювання порогу чутливості $V$ у системі дозволятиме гнучко настроювати її у відповідності до вимог безпеки. При цьому слід брати до уваги, що збільшення стійкості стеганосистеми до аналізу (і, як наслідок, зниження імовірності $p_\alpha$) супроводжується зростанням часу виявлення прихованих даних і підвищенням імовірності $p_\beta$ [3].

Якщо *вихідні дані з виходу детектора є двійковими*, криві DOC одержати неможливо. У цьому випадку можна оперувати кількістю помилково виявлених у пустому контейнері ЦВЗ ($N_\alpha$) і кількістю пропущених ЦВЗ ($N_\beta$): $p_\alpha = N_\alpha / |\mathbf{W}|$; $p_\beta = N_\beta / |\mathbf{W}|$. Як критерій ефективності може бути використана зважена сума:

$$p = k_\alpha \cdot p_\alpha + k_\beta \cdot p_\beta, \quad (3)$$

де $k_\alpha$, $k_\beta$ — вагові змінні, що обираються в залежності від вимог до алгоритму.

Якщо алгоритмом передбачається можливість приховування повідомлення, *вихідними даними декодера* є повідомлення $\tilde{m}_i$, яке порівнюється з повідомленням-оригіналом $m_i$. У випадку *недвійкового характеру* вихідних даних детектора, для кожного значення порогу $V$ визначається:

— середня кількість помилкових біт у видобутих даних ($N_{BER}$) для ЦВЗ (правильних і помилкових), що перевищили поріг $V$ детектора (тобто для всіх виявлених ЦВЗ);

— кількість повідомлень, для яких були правильно видобуті усі біти первинного повідомлення ($N_M^+$). Як і у попередньому випадку — для всіх виявлених ЦВЗ.

За одержаними результатами для кожного елементу $\mathbf{C}^A$ будуються графіки залежностей $N_{BER}$ і $N_M^+$ від порогу $V$ (або, що те саме, як функції відповідної імовірності $p_\alpha(V)$). Критеріями ефективності можуть бути обрані значення $N_{BER}$ або $N_M^+$ при $p_\alpha(V) = const$.

Якщо вихідні дані детектора носять *двійковий характер*, маємо попередньо визначений поріг (а, отже, й задану точку на кривій DOC). При цьому, для будь-якого контейнеру з $\mathbf{C}^A$ можна однозначно встановити $N_{BER}$ і $N_M^+$, які й використовуються як критерії ефективності.

**Час виконання** операцій з вбудовування, виявлення і видобування даних визначається шляхом усереднення на множинах **W** і **M**.

Результатом виконання вищенаведених процедур є критерії ефективності для будь-якого контейнера з множини $\mathbf{C}^A$, одержані шляхом аналізу вихідних даних детектора, декодера і часу на виконання ключових операцій. Виходячи із значного обсягу даної інформації, результати доцільно представити у більш компактній і наочній формі. Наприклад, шляхом **зваженого об'єднання критеріїв-результатів**, що відповідають кожному контейнеру з $\mathbf{C}^A$. Вага того або іншого критерію повинна відповідати імовірності появи специфічного контейнера за конкретних обставин.

Для оцінки **пропускної здатності** стеганосистеми, формованої на основі досліджуваного алгоритму, до контейнера вбудовуються повідомлення зростаючої довжини і перевіряється значення показника BER, одержуваного за результатами видобування, на предмет перевищення ним заданого порогу $V_{BER}$. У випадку *недвійкового детектора*, BER визначається для кожного значення змінюваного порогу $V$ тестової статистики, тобто для кожного значення $p_\alpha$. В результаті оцінка ПЗ одержується для кожної комбінації "контейнер-якість". Оскільки поріг $V$ пов'язаний з відповідною парою імовірностей $p_\alpha$ і $p_\beta$, можна відтворити залежність ПЗ від $p_\alpha$ або $p_\beta$. Можливим критерієм ефективності при порівнянні алгоритмів є порівняння їх ПЗ, що відповідає фіксованому значенню $p_\alpha$. Якщо *детектор двійковий*, значення ПЗ визначається для заданого робочого стану стеганосистеми. Для одержання оцінки загальної ПЗ, забезпечуваної алгоритмом, окремі показники можуть бути об'єднані для кожної комбінації "контейнер-якість" аналогічно тому, як це робилося при оцінці стійкості алгоритму до атак.

Для обраного критерію ефективності та за певних: якості, контейнера й атаки (у довільній комбінації) можна визначити **граничні рівні стійкості до атаки** досліджуваного алгоритму. Передбачено можливість покрокового підвищення рівня атаки (напр., підвищення ступеню JPEG-компресії з кроком 2%) до тих пір, поки дані на виході детектора не задовольнятимуть обраному критерію ефективності. Атака, для якої критерій ефективності алгоритму перевищив встановлений поріг, є *алгоритмічною межею* для обраного різновиду атак. Показники граничної стійкості для всіх контейнерів і певної пари "якість-атака" можуть бути зведені до відповідного цій парі загального показника граничного стійкості за методикою, аналогічною вищенаведеній.

Також є доцільною перевірка стеганоалгоритму на факт **задоволення вимогам певної прикладної задачі**. Для цього існуючі вимоги зводяться до відповідної множини вагових коефіцієнтів **K** (елементи якої беруть участь при визначенні показників ефективності в ході дослідження алгоритму) і множини порогових значень ефективності **V** (з елементами якої порівнюються одержані в ході дослідження показники ефективності).

**Висновки і перспективи дослідження**

В даній роботі представлено нестандартний протокол оцінки ефективності відомих і розроблюваних стеганоалгоритмів, в якому усунуто недоліки існуючих для даних цілей програм тестування. Тест-система, розроблена на основі даного протоколу, може бути використана для моніторингу ефективності алгоритмів, що використовуються для захисту авторського права, ідентифікації медіаконтенту цифровими "відбитками", контролю доступу до конфіденційної інформації тощо.

**Список літератури**

1. Internet-ресурс інформагентства Reuters (http://today.reuters.com/news/).
2. Internet-ресурс Цейтру дослідження проблем комп'ютерної злочинності — Computer Crime Research Center (http://www.crime-research.org/).
3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: "МК-Пресс", 2006. — 288 с.
4. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії. — Вінниця: ВДТУ, 2003. — 143 с.
5. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: "Солон-Пресс", 2002. — 272 с.
6. StirMark (http://www.petitcolas.net/fabien/watermarking/stirmark/index.html), UnZign (http://www.petitcolas.net/fabien/steganography/image_watermarking/unzign/).
7. Вентцель Е.С., Овчаров В.А. Теория вероятностей и её инженерные приложения. Изд. 3-е, перераб. и доп. Уч. пос. для ВУЗов. — М.: "Академия", 2003. — 464 с.
8. Б. Скляр, Цифровая связь: Теоретические основы и практическое применение. Изд. 2-е, исправл. — М.: "Вильямс", 2003. — 1104 с.

УДК 681.511.3

Кобозева А.А., Маракова И.И.

## МЕТОД ОЦЕНКИ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ К ВОЗМУЩАЮЩИМ ПРЕОБРАЗОВАНИЯМ

По мере развития современного общества проблема защиты информации становится все более актуальной, что приводит к резкому повышению интереса к исследованиям в области компьютерной стеганографии [1]. Толчком для развития этих исследований в последнее время послужило появление новых областей применения. Дополнительная информация ( ДИ ) встраивается в основное сообщение ( ОС ), в качестве которого может использоваться видео, изображение, аудиозаписи и т.д., причем дополнительная информация может быть как секретной, так и несекретной. Без потери общности для конкретизации исследований далее в качестве ОС будем рассматривать изображение.

Целью исследования является установление таких свойств произвольного изображения, наличие которых явилось бы достаточным условием устойчивости предлагаемого алгоритма стеганографического преобразования этого изображения и декодирования скрытой в нем информации к различного рода искажениям, а также нечувствительности задачи о декодировании ДИ к возмущениям в исходных данных.

Дадим определения используемым понятиям.

Стеганографическим преобразованием будем называть процесс погружения ДИ в основное сообщение.