ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 681.511:3

ПРЕДСТАВЛЕННЯ І ПРОГНОЗУВАННЯ ЕФЕКТИВНОСТІ НОВОГО ПРОТОКОЛУ ОЦІНКИ ЯКОСТІ РЕАЛІЗАЦІЇ РОЗРОБЛЮВАНИХ АЛГОРИТМІВ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Навроцький Д. О., Дюжаєв Л.П., Пузиренко О.Ю.,

Представлено протокол оцінки якості реалізації відомих і прогнозування ефективності розроблюваних алгоритмів комп'ютерної стеганографії. Пропоновану концепцію дослідження можна використати для моніторингу стеганоалгоритмів.

Вступ. Постановка задачі

Питання 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. В такій ситуації особлива увага має бути надана превентивному створенню інформаційних систем, які були б надійно захищеними від різноманітних загроз. Одним з альтернативних засобів захисту інформації є *комп'ютерна стеганографія* [1,2]. 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, що, таким чином, спричинило потребу в наявності методики наочної оцінки відносної ефективності зазначених алгоритмів проти різноманітних видів атак на стеганосистеми.

В роботі представлено новий протокол оцінки якості реалізації відомих і прогнозування ефективності розроблюваних алгоритмів комп'ютерної стеганографії, в якому усунуто недоліки існуючих тест-систем. Головну увагу зосереджено на представленні повного набору тестів, що мають бути виконані для одержання наочної, однозначної і надійної характеристики ефективності досліджуваного стеганоалгоритму. Крім того, слід надати методику узагальнення окремих результатів для більш компактного відображення загальної ефективності методів стеганографії.

Опис протоколу

Вхідною інформацією запропонованої тест-системи є програмні засоби вбудовування, виявлення і видобування цифрового водяного знаку (ЦВЗ). Результатом проведених тестувань є числові показники і діаграми, що відображують ефективність досліджуваного стеганоалгоритму по відношенню до різних видів атак. Параметри пропонованої системи:

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

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

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

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

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

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

— множина вимог до якості стеганосистеми 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, 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 [1]. 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, оскільки, не зважаючи на деякі недоліки показника (зокрема, слабку корельованість із сприйманою якістю контейнера [1]), поки що не запропоновано жодної задовільної міри якості, однаково ефективно застосовної для будь-якого типу медіаконтейнера. Що стосується вбудовування ЦВЗ, — може використовуватися множина показників відношення сигнал/шум: 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 і 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 E вбудовує ЦВЗ w_t та повідомлення m_i до контейнера c_j з урахуванням задоволення вимог до якості q_r заповненим контейнером: $E: C \times W \times M \times Q \to C^W$. Дана процедура повторюється для всіх елементів множин C, W, M і Q, результатом чого є множина заповнених контейнерів C^W. Потужність множини 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.

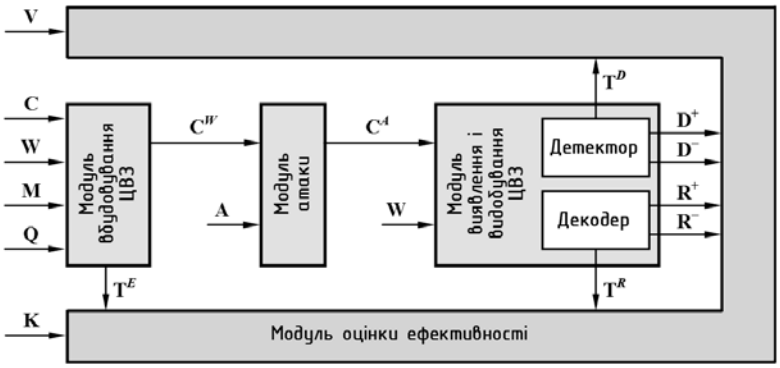

Рис.1. Блок-схема системи тестування

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

Модуль виявлення і видобування ЦВЗ використовує відповідні досліджувані програмні засоби, вхідними даними яких є множини C^A і W. Виконується виявлення ЦВЗ за правильним (w_x) і помилковим $(w_y,\ y \neq x)$ ключами, а також видобування визначених цими ЦВЗ вбудованих повідомлень $\tilde{m} \in M$ з усіх контейнерів множини C^A. Як наслідок, з кожного атакованого контейнера множини C^A видобувається дві пари вихідних даних детектора і декодера, що зумовлені використанням правильного і помилкового ключів вбудовування ЦВЗ. Нехай D^+ і R^+ — відповідні множини вихідних даних детектора і декодера при використанні для їх отримання правильного ключа, а D^- і 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: наприклад, «1»—ЦВЗ виявлено, «0»—ЦВЗ не виявлено (рішення є результатом порівняння статистики, що лежить в основі критерію для перевірки гі-

потези, з порогом прийняття рішень), або ж безпосередньо статистику, що лежить в основі критерію, у вигляді дійсних (не двійкових) чисел [1,3]. 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 (D^+ і D^-) і декодера (R^+ і R^-), множини T^E, T^D і T^R проміжків часу виконання кожної з операцій (вбудовування, виявлення і видобування), а також множина вагових коефіцієнтів K. Вихідні дані модуля — якісні оцінки і діаграми, що характеризують відносну ефективність 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 необхідно визначити імовірності "помилкової тривоги" і "пропуску цілі". Імовірністю "помилкової тривоги" (помилки 1-го роду) p_α є імовірність виявлення ЦВЗ у пустому контейнері або у контейнері, заповненому ЦВЗ з іншим ключем. У даному випадку p_α встановлюється здійсненням виявлення з помилковим ключем, оскільки це є еквівалентним найбільш несприятливому варіанту. Імовірністю "пропуску цілі" (помилки 2-го роду) p_β є імовірність не виявлення ЦВЗ у заповненому ним контейнері.

Якщо *дані з виходу детектора є недвійковими*, можлива оцінка емпіричного розподілу, який може бути апроксимований теоретичним розподілом $f(u)$. У відповідності з цим, результатом множин D^+ і 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_α і p_β [4]:

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

Використовуючи (1), визначимо робочу характеристику детектора (*DOC — Detector Operating Characteristic*) — залежність імовірності p_α від імовірності p_β, шляхом оцінки для будь-якого порогового значення V площ під $f^+(u)$ і $f^-(u)$ відповідно ліворуч (p_β) і праворуч (p_α) від порогу (рис.2) [5]. Криві *DOC* обчислюються для кожного контейнера з множини C^A. Крім того, криві *DOC* можуть бути визначені безпосередньо з емпіричних розподілів:

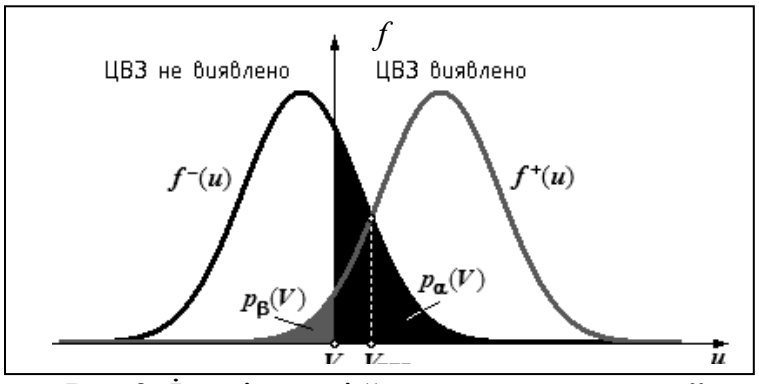

Рис.2. Імовірності "помилкової тривоги" і "пропуску цілі"

$$p_\alpha(V) = \left|\mathrm{D}_V^-\right| \Big/ \left|\mathrm{D}^-\right|;\ p_\beta(V) = \left|\mathrm{D}_V^+\right| \Big/ \left|\mathrm{D}^+\right|,$$

де $\mathrm{D}_V^- = \left\{u_i > V / u_i \in \mathrm{D}^-\right\}$; $\mathrm{D}_V^+ = \left\{u_i < V / u_i \in \mathrm{D}^+\right\}$; запис $|D|$ розуміє під собою потужність множини 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*, можна оцінити критерії ефективності (рис.3):

— імовірність p_β (p_α) для фіксованого значення p_α (p_β);

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

— так звану глобальну оцінку ефективності (площу під кривою *DOC*), S_{DOC}.

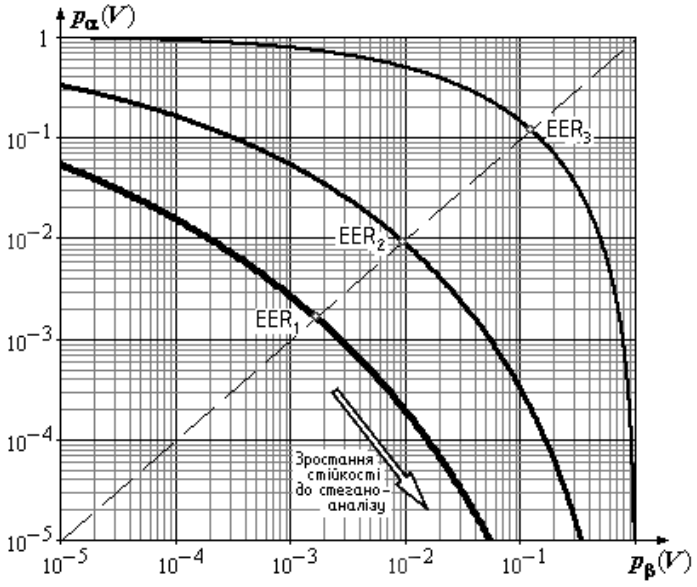

Рис. 3. Робочі характеристики стеганодетекторів

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

Регулювання порогу чутливості V у розробленій системі дозволяє гну-

чко настроювати її до вимог безпеки. При цьому, як було встановлено, слід брати до уваги, що збільшення стійкості стеганосистеми до аналізу (і, як наслідок, зниження імовірності p_α) супроводжується зростанням часу виявлення прихованих даних і підвищенням імовірності p_β [1].

Якщо *дані з виходу детектора є двійковими*, криві *DOC* одержати неможливо. У цьому випадку можна оперувати кількістю помилково виявлених у пустому контейнері ЦВЗ (N_α) і кількістю пропущених ЦВЗ (N_β): $p_\alpha = N_\alpha / |\mathrm{W}|;\ p_\beta = N_\beta / |\mathrm{W}|$. Як критерій ефективності нами була використана зважена сума $p = k_\alpha p_\alpha + k_\beta p_\beta$, де k_α, k_β — вагові змінні, що обираються відповідно 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 ($N_M{}^+$).

За допомогою одержаних результатів для кожного елементу C^A ми змогли побудувати графіки залежностей N_{BER} і $N_M{}^+$ від порогу V (або, що те саме, як функції відповідної імовірності $p_\alpha(V)$). Критеріями ефективності ми могли обрати значення N_{BER} або $N_M{}^+$ при $p_\alpha(V) = const$.

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

Висновки

Представлений новий протокол оцінки ефективності відомих і розроблюваних стеганоалгоритмів вільний від недоліків 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"

Література

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: "МК-Пресс", 2006. — 288 с.

2. Хорошко В.О., Азаров О.Д., Шелест М.Є., ін. Основи комп'ютерної стеганог-

рафії. Вінниця: ВДТУ, 2003. 143 с.

3. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: "Солон-Пресс", 2002. — 272 с.

4. Вентцель Е.С., Овчаров В.А. Теория вероятностей и её инженерные приложения. Уч. пос. для ВУЗов. — М.: "Академия", 2003. — 464 с.

5. Скляр Б., Цифровая связь: Теоретические основы и практическое применение. М.: "Вильямс", 2003. — 1104 с.

Навроцкий Д.О., Дюжаев Л.,Пузиренко О.Ю

Представление и прогнозирование эффективности нового протокола оценки качества реализации разрабатываемых алгоритмов компьютерной стеганографии

Представлен протокол оценки качества реализации известных и прогнозирование эффективности разрабатываемых алгоритмов компьютерной стеганографии. Предложенную концепцию можно использовать для мониторинга стеганоалгоритмов.

Navrotskiy D.O.,Dyuzhayev L.,Puzirenko O.Yu

Representation and forecasting of efficiency of the new protocol of an estimation of quality of realization of developed algorithms computer steganography

There is represented the protocol quality rating of realization and technologic forecasting of efficiency of well-known and developed algorithms of computer stenography. The proposed concept can be used for the monitoring of steganoalgorithms, which are used for copyright protection.