Інститут кібернетики імені В. М. Глушкова
Національної академії наук України
Кам'янець-Подільський національний університет
імені Івана Огієнка

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

Серія: Технічні науки

Збірник наукових праць

Випуск 5

Кам'янець-Подільський національний університет
імені Івана Огієнка
2011

УДК 004.94:53.072
ББК 30
М34

Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 14522-3493Р від 25.06.2008 р.

Збірник наукових праць включено до Переліку наукових фахових видань України з технічних наук (постанова Президії ВАК України від 27 травня 2009 р. № 1-05/2, Бюлетень ВАК України №8, 2009)

Друкується згідно з рішенням вченої ради Кам'янець-Подільського національного університету імені Івана Огієнка, протокол № 7 від 30 червня 2011 року.

М34 Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. праць / Інститут кібернетики імені В. М. Глушкова Національної академії наук України, Кам'янець-Подільський національний університет імені Івана Огієнка ; [редкол.: Ю. Г. Кривонос (відп. ред.) та ін.]. — Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2011. — Вип. 5. — 224 с.

У збірнику друкуються результати досліджень, що стосуються проблем застосування математичних моделей в різних галузях людської діяльності.

Для наукових та інженерно-технічних працівників, докторантів, аспірантів, студентів вищих навчальних закладів.

УДК 004.94:53.072
ББК 30

УДК 004.056:621.397

В. Ю. Корольов*, канд. техн. наук,
В. В. Поліновський**, канд. техн. наук,
В. А. Герасименко*, молодший науковий співробітник,
М. Л. Горінштейн*, молодший науковий співробітник

*Інститут кібернетики НАН України, м. Київ,
**Вищий навчальний заклад «Відкритий міжнародний університет розвитку людини «Україна», м. Київ

КОМПЛЕКС СТАТИСТИЧНИХ ДОСЛІДЖЕНЬ ДЛЯ СТЕГОАНАЛІЗУ

Запропоновано концепцію нової інформаційної технології стегоаналітичних досліджень методів стеганографії та сформульовано вимоги до таких систем. Показано, що розроблене програмне забезпечення дозволяє отримати комплексну оцінку можливостей методів приховування даних у зображеннях. Результати роботи програмного комплексу показано на прикладі RS-стеганоаналізу для НЗБ-алгоритмів приховування даних.

Ключові слова: *стеганографія, RS-стегоаналіз, інформаційні технології.*

Вступ

Комп'ютерна стеганографія і стегоаналіз (СА) розвиваються паралельно вже понад 20 років. Як відомо, на відміну від криптографічного захисту інформації стеганографічні програмні засоби [1; 2] намагаються в першу чергу приховати сам факт передачі даних, використовуючи для цього психовізуальну надлишковість зображень або мультимедійних файлів (контейнери). В той же час, сучасна стеганографія використовує методи криптографії для шифрування інформації перед її вбудовуванням в контейнер, що з точки зору статистики еквівалентно внесенню у контейнер стохастичного збурення.

Спрощення використання методів приховування інформації та можливість передачі інформації по відкритим цифровим каналам передачі даних зробили доступними стеганографічне програмне забезпечення пересічному користувачу персонального комп'ютера з доступом до мережі Інтернет. Сьогодні на ринку програмного забезпечення існує багато пропозицій стеганографічних програмних додатків, у тому числі й на безоплатній основі.

Зрозуміло, що засоби стеганографії можуть використовуватись як законослухняними громадянами, так і кримінальними або шпигунськими структурами. Тому активно розвиваються відповідні методи протидії — стегоаналіз, які покликані виявити приховану у контейнері інформацію або встановити сам факт прихованої передачі даних.

Дослідження стійкості методів приховування даних до стегоаналізу дозволяє перевірити надійність стеганографії, а також зробити вагомий внесок в інформаційну безпеку держави.

Аналіз останніх досліджень і публікацій

За останні 15 років створено багато методів приховування інформації у різних типах і форматах файлів, а також методів виявлення вбудованих даних. Найбільшого поширення набули методи приховування даних у цифрових фотографіях за методом приховування у найменш значимих бітах байт кольорових каналів зображень (НЗБ-стеганографія) і, відповідно, найбільше методів стегоаналізу розроблено для виявлення саме НЗБ-стеганографії [1—14]. Крім того, такі методи найбільш прості в реалізації. Тому більшість комерційних і вільних програм приховування даних мають у своєму складі додатки НЗБ-стеганографії. Одним з найбільш точних сучасних методів виявлення прихованих даних у зображеннях є RS-стегоаналіз [3—14].

Зазначимо, що однією з тенденцій останніх двох років сучасного стегоаналізу [12—14] є використання методів інтелектуального аналізу даних (ІАД — Data Mining). З цією метою з декількох методів стегоаналізу і математичної статистики виділяють групи ознак для виявлення прихованих даних, які потім аналізуються системами ІАД.

Слід зауважити, що НЗБ-стеганографія передбачає приховування даних у байтах кольорів зображень, тобто збережених у форматі BMP та його похідних. Проте абсолютна більшість сучасних цифрових фотографій зберігається у форматі JPEG, оскільки у ньому найкраще реалізовано стиск зображень при мінімумі втрат візуальної якості. Висока продуктивність JPEG-алгоритмів ґрунтується на швидких перетвореннях, у яких обмежується інтенсивність високочастотних складових зображень. Цим пояснюється, що безпосереднє застосування методів НЗБ-стеганографії до зображень у форматі JPEG достатньо просто може бути виявлено [3], оскільки суттєво спотворює співвідношення чисел зображення у такому форматі і тому використання форматів збереження цифрових фотографій крім JPEG для передачі або демонстрації аматорських фотографій через Інтернет одразу стає підозрілим з позиції стегоаналітика.

Множина форматів RAW, у якому зберігають зображення професійні і напів-професійні дзеркальні фотокамери, має високу інформаційну надлишковість і тому рідко використовується для передачі даних. Цифрові фотографії у RAW форматі мають розміри десятки мегабайт, що обумовлює їх повільну передачу електронною поштою або обмежує її (для випадку поштових веб-сервісів). Крім того, цей

формат не підтримуються більшістю інтернет-браузерів для відображення на веб-сайтах.

При створенні методів стегоаналізу розробники виходять з того, що користувачі будуть фотографувати об'єкти або сцени фотокамерами середнього або високого класу, або братимуть цифрові фотографії з тематичних сайтів у мережі Інтернет.

Проте зображення може бути оброблене власником фотографії (обробка зображення для демонстрації в Інтернет) або самим користувачем для того щоб унеможливити для стегоаналітика отримання точного оригіналу.

Постановка завдання

Як було зазначено вище, планування статистичних досліджень для RS-стегоаналізу і подібних методів є актуальною науковою проблемою, одним із завдань якої є дослідження стійкості методів приховування даних до стегоаналізу. У роботі викладено результати понад шести років науково-прикладних досліджень авторів роботи в області НЗБ-стеганографії, які можуть бути застосовані як для приховування в контейнерах у форматі JPEG, так і для методів, які є подальшим розвитком RS - WS-стегоаналіз [3].

Основна частина.
Етапи стегоаналітичного дослідження

Досвід авторів у проведенні стегоаналітичних досліджень показує, що розробники методів стегоаналізу (СА) і автори наукових робіт, які намагаються знайти в цих методах слабкі сторони і виявити їх обмеження, приділяють не достатньо уваги формуванню колекції файлів з якими виконуються дослідження. Як правило, з мережі Інтернет для статистичних досліджень беруть набори фотографій (кількістю 150—450 файлів) які, на думку авторів методів, не оброблені цифровими фільтрами і не містять вбудовування знаків захисту авторського права (ЦВЗ).

У нашому циклі робіт було показано [7—10], що такий підхід приводить до перебільшення можливостей методу стегоаналізу. Крім того, на результати статистичних досліджень впливає не тільки ступінь зашумлення зображення, але і геометричний розмір та розрізнення фотографії. Так для зображень більшого формату без вбудованих стеганографічних даних характерно менше значення хибно позитивно визначених стегобіт (ХПВС) [9] — величина прихованих даних за методом RS-стегоаналізу.

У відповідності до теорії планування експерименту на початковому етапі досліджень, коли немає відомостей про вплив параметрів

на вихідну статистику, необхідно виконати відсіювальні експерименти для виявлення параметрів, які суттєво не впливають на статистичні дані або породжують аномальні відгуки, що рідко зустрічаються на практиці. Відсіювання несуттєвих факторів дозволяє знизити трудомісткість задач СА.

Тому, на думку авторів, план стегоаналітичних досліджень повинен складатись з наступних етапів.

1. Дослідження необроблених фотографій (оригіналів). Мета досліджень полягає у визначенні межі точності СА з мінімізацією несуттєвих для дослідження факторів впливу. Для досягнення цієї мети пропонується побудувати тематичні колекції фотографій над якими не виконувались перетворення. Найкраще групі дослідників самостійно сфотографувати набір сцен, об'єктів, пейзажів, тощо при варіації експозицій (значення витримки, діафрагмами, чутливості та глибині різкості) на декількох камерах, оскільки обробка зображень суттєво впливає на статистичні значення СА.

Результатом першого етапу є оцінка величини хибно позитивно виявлених прихованих даних (ХПВС) для оригіналів та характерних діапазонів значень для СА, визначення параметрів експозиції, які суттєво не впливають на отриманий результат та породжених ними вибірок, а також відсіювання з вибірок фотографій з аномально високими значеннями СА.

2. Дослідження впливу фільтрів і їх комбінацій на результати СА. Отриману на першому етапі структуровану множину фотографій обробляють цифровими методами, типовими для демонстрації зображень в мережі Інтернет або друку. Метою другого етапу досліджень є виявлення впливу типових методів цифрової обробки фотографій на результати СА. Результатом другого етапу є величина ХПВС для перетворених фотографій.

3. Дослідження можливостей методу СА у виявленні прихованих даних. Сучасна стеганографія використовує методи криптографії для шифрування файлів перед вбудовуванням у контейнер, тому моделюванням стеганографічного захисту шифрованих даних є приховання у фотографії масиву випадкових біт. Метою третього етапу є дослідження відповідності об'єму прихованих і виявлених даних за методом СА і оцінка точності та чутливості, а також виявлення типів зображень для яких додавання прихованих даних аномально високо підвищує СА процент виявлення або цей вплив є незначним, тобто не відповідає об'єму прихованих даних.

4. Дослідження можливостей СА у виявленні прихованих даних після застосування до них типових перетворень. Метою четвертого етапу є виявлення впливу застосування до зображень типових цифро-

вих фільтрів і перетворень на результат виявлення вбудованих даних у зображення. Для цього над зображеннями виконуються перетворення, додають у них приховані дані і роблять СА. Метою четвертого етапу є визначення перетворень, які зменшують результат СА до рівня, характерного для оригіналів.

5. Дослідження зображень з мережі Інтернет. Зрозуміло, що кількість фотографій, зроблених дослідниками або таких, над якими гарантовано не виконувались перетворення, є обмеженою. З іншого боку, користувачі для приховування даних у фотографіях можуть брати їх з мережевих колекцій та обробити для того, щоб унеможливити отримання оригіналу стегоаналітиком. При дослідженні зображень з Інтернет слід враховувати, що вони можуть бути перетворені користувачем або самим сервісом з метою покращення візуальної якості, у фотографіях можуть бути вбудовані цифрові водяні знаки для захисту авторських прав на фотографію тощо. Зображення також мають статистичну природу і складну систему зв'язків між фоном і об'єктами сцени передбачити вплив на які перетворень можливо тільки для простих випадків.

Оскільки, стеганографічний захист інформації носить статистичний характер, перелічені перетворення можуть суттєво впливати на результат СА, що потрібно визначити. Методи досліджень аналогічні для чотирьох попередніх етапів.

6. Перевірка гіпотез обходу СА. За результатами виконання СА колекцій зображень дослідники вже мають достатньо повне уявлення про слабкі сторони методу і мають ідеї їх використання як алгоритм протидії стегоаналізу та основу для створення нових та модифікацій розроблених методів стеганографії.

7. Суміжні дослідження. СА використовує методи багатьох областей для виявлення прихованих даних. Після накопичення великого масиву результатів статистичних випробувань отримані дані і напрацьовані методики можуть бути використані у суміжних з СА напрямках досліджень [9].

8. Створення тегів для зображень. Мета восьмого етапу полягає в семантичному описі змісту кожного зображення з досліджуваної колекції для передачі його в систему інтелектуального аналізу даних (ІАД — Data Mining).

9. Застосування методів ІАД для виявлення закономірностей не помічених дослідниками СА. Одним з найбільш відомих програмних комплексів ІАД є програмний комплекс фірми Oracle.

З урахуванням вищезазначеного, перед кожним дослідженням необхідно сформувати вибірку зображень. Представимо у концептуальному вигляді механізми роботи користувача для синтезу задач СА (рис. 1).

Концепція побудови інформаційної технології для стеганографічних досліджень

Очевидно, що велика кількість параметрів фотографій, фільтрів для перетворень зображень, методів стеганографії та стеганоаналізу набувають вигляду громіздких ієрархічних моделей і ускладнюють аналітикам сприйняття задачі та побудову функціональних залежностей і визначення кореляцій між параметрами.

Характеристики і параметри зображень та описи вибірок пропонується подавати у вигляді хмарин тегів. Такий підхід дозволить автоматизувати дослідження за допомогою систем ІАД. Кожен з цих параметрів або елементів переліку належить до відповідного масиву (хмарин) тегів. Отже, маємо чотири таких хмарин: хмара тегів параметрів зображень та опису змісту сцени, хмара тегів фільтрів і перетворень, хмара тегів стегоалгоритмів та хмара тегів стегоаналізу (рис. 1).

Варто зазначити, що в більш загальному вигляді три останні хмаринки являють собою результуючу хмару синтезу задач (див. рис. 1). Зрозуміло, що аналітику незручно працювати одночасно з всіма трьома хмаринками тегів «задач», тому в цій хмарі виділено абстрактну сутність — хмарину обраних тегів, яка в будь-який момент часу може бути повною реплікацією однієї з трьох хмаринок (Ф, С, Са) за вибором оператора. Тобто аналітик працює тільки з однією хмаринкою вибору тегів (рис. 1).

Такий підхід є практичним, особливо для розподіленої роботи та паралельних обчислень. Більш детально механізм синтезу задач стеганоаналізу та обробки зображень розглянемо нижче, а зараз покажемо як формуються вибірки (див. рис. 1).

Аналітик (на рис. 1, позначений А), звертається до хмари тегів зображень з якої він обирає необхідні параметри для проведення досліджень, далі запускається механізм відбору зображень. Відповідний додаток звертається до банку фізичного збереження фотографій та формує віртуальну вибірку зображень за обраними параметрами. Такий механізм дозволяє сформувати декілька суттєво відмінних вибірок, які використовуватимуться для вирішення різних задач стегоаналізу, обробки зображень та статистичних досліджень. Потім для кожної вибірки синтезується власний або однаковий перелік задач для стеганоаналізу або обробки зображень, що є раціональним для розподіленої роботи та паралельних обчислень.

Побудуємо концептуальну модель процесу синтезу задач стеганоаналізу або обробки зображень та їх реалізації (рис. 2). Як і було зазначено вище, аналітик (на рис. 2, позначений А), звертається до хмари задач, а саме до хмари «***0***`», з якої по зазначеному вище спосо-

бу починає формувати послідовність задач (від 1 до m, див. рис. 2), які необхідно буде виконати для проведення стеганоаналізу або обробки зображень. Для кожної з цих задач, оператор може задати певні параметри (див. рис. 2). Сукупність задач та їх параметрів формують певний робочій простір, зазначеному на рис. 2 — як Wf, для обробки зображень що містяться у віртуальній виборці. Зрозуміло, що навіть не запускаючи ніяких обчислювальних процесів користувач може заздалегідь створити декілька Wf, і вже після цього запустити процес обробки зображень, що дозволить природно використовувати розподілені роботи та паралельні обчислення.

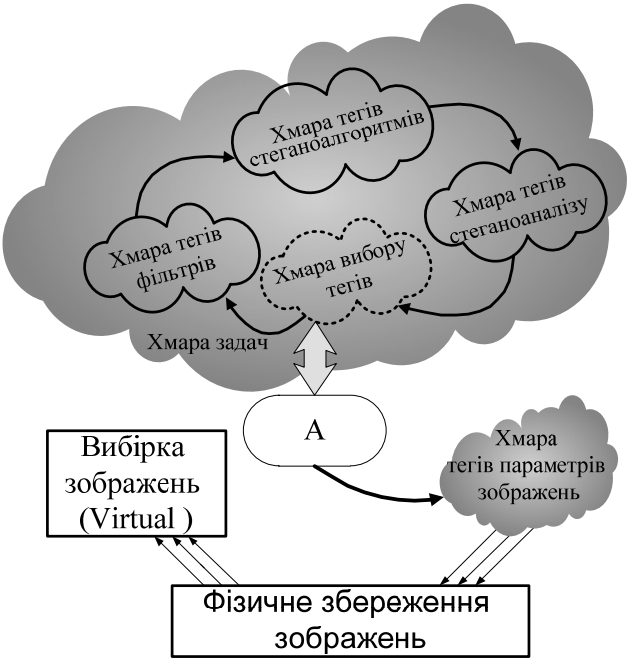

Рис. 1. *Модель синтезу задачі стеганоаналізу*

Результати руху зображень через робочий простір, тобто послідовна обробка кожного зображення задачами від 1 до m з певними параметрами, будуть записані в базу даних (**db_{res}**). При цьому, варто зазначити, що ця **db_{res}** містить в собі три пов'язані між собою бази даних db_{wf} — база даних, що містить інформацію про кожний з робочих просторів, у яких виконувалися дослідження, db_{is} — база даних, що містить статистичну інформацію (кількісну характеристику), db_a — база даних, що містить інформацію про результати певних подій. Деталі роботи буде пояснено нижче.

При формуванні робочого простору Wf, важливим є не тільки вид задач та з якими параметрами входять до нього, а й послідовність виконання цих задач, оскільки перетворення даних у стегоаналізі не є комутативними операціями. Крім того, обробка кожного з зображень віртуальної вибірки певними алгоритмами стеганоаналізу або фільтрації та приховування інформації в них за стеганографічними алгоритмами споживають багато обчислювальних ресурсів. Тому актуальною науково-прикладною задачею є оптимізація механізмів руху масивів даних через робочий простір при дослідженнях зображень методами стеганографії, стеганоаналізу або обробки зображень.

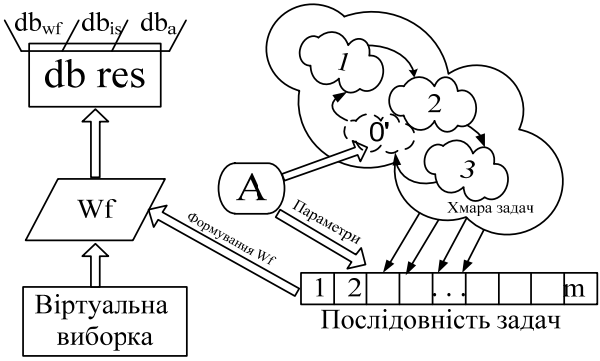

Рис. 2. *Модель синтезу задач для стеганоаналізу або обробки зображень*

Розглянемо концепцію оптимізації більш детально: маємо віртуальну вибірку і сформований робочий простір Wf, тобто оператор може запустити процес дослідження. Згідно з попередньою схемою дослідження (рис. 2) проходило б над усіма зображеннями, причому, якщо до цієї вибірки додати декілька зображень (порівняно з попереднім дослідженням), то все одно всі операції перетворень для кожного з зображень пройшли би повний цикл згідно Wf. При цьому нових даних в $\mathbf{db_{res}}$ майже не потрапить, а обчислювальні навантаження будуть колосальні, тож такий варіант є неефективним.

Один із варіантів вирішення цієї задачі показано на рис. 3. Коли оператор запускає процес досліджень формується «віртуальна вибірка`» та Wf`, яка є описовими відображеннями реальних даних. Далі проводяться віртуальні дослідження без будь-яких обчислювальних перетворень над зображеннями, тобто для кожного з зображень створюється формальне (індексне) представлення, з переліком які саме перетворення над ним буде проведено і які дані після цього будуть отримані. Отримані дані записуються в поля бази даних $\mathbf{R_a}$. Після проведення запланованих віртуальних досліджень база даних $\mathbf{R_a}$ порівняється з $\mathbf{db_{res}}$ (рис. 3). На основі результатів порівняння і форму-

ється оновлений робочий простір Wf* та оновлена «віртуальна вибірка*», які не містять зайвих (дубльованих) результатів досліджень. Потім виконуються перетворення зображень з «віртуальної вибірки*» згідно Wf* (див. рис. 3).

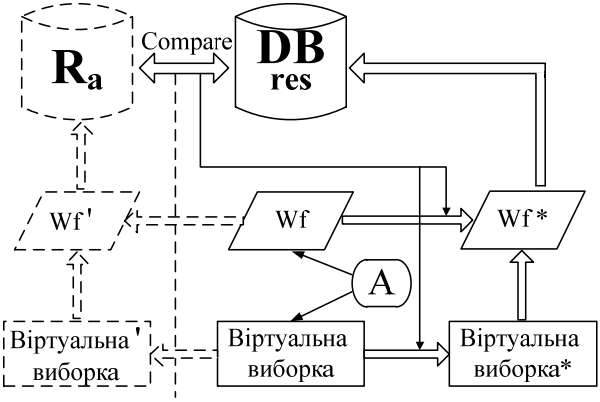

Рис. 3. *Модель раціоналізації обчислювальних процесів дослідження фотографій методами стеганоаналізу та перетворення зображень*

Архітектура програмного комплексу аналізу зображень

Для досліджень характеристик масивів зображень за різними методами було розроблено універсальний комплекс аналізу зображень з модульною архітектурою, який дозволяє додавати нові формати файлів зображень та алгоритмів їх аналізу, а також виконувати обробку без зміни самого комплексу. Головним завданням, яке ставилось при розробці комплексу стегоаналізу, була потреба виконання досліджень не лише оригінальних масивів зображень, а й певним чином модифікованих версій у процесі обробки зображень, наприклад – результати фільтрації за обраними оператором-аналітиком алгоритмами. Крім того, необхідно виконувати аналіз зображень різними алгоритмами, тобто в загальному випадку над зображеннями необхідно виконати задану послідовність операцій фільтрації та аналізу. Кожна операція повинна мати можливість налаштування, тобто завдання параметрів фільтрації та аналізу.

Отримані масиви статистик зберігаються в базі даних, структура якої дозволяє зберігати та отримувати статистику оброблену іншими модулями аналізу даних. Також комплекс має досить широкі можливості вибірки та аналізу накопичених даних. За переліченими характеристиками комплекс стегоаналітичних досліджень суттєво відрізняється від наявних рішень, більшість з яких є вузькоспеціалізованими і виконують аналіз зображень лише одного типу та одним алгоритмом, результати обробки також представляються в своєму форматі.

Серед прототипів комплексу можна назвати комплекси MGEBO [12] та **Digital Invisible Ink Toolkit** [13], а серед аналогів — додатки розроблені лабораторією проф. Д. Фридрич [14].

Для вирішення поставленої задачі була реалізована модульна архітектура комплексу, яка передбачає реалізацію фільтрів та аналізаторів в окремих модулях-розширеннях комплексу. Це дозволяє додавати такі модулі без зміни основного комплексу. Фільтр та аналізатор в цій архітектурі визначаються як програмні інтерфейси (набір методів з визначеними сигнатурами), що використовуються основним комплексом при обробці файлів. Модулі-розширення представляють собою звичайні dll-бібліотеки, що містять один чи декілька класів, які реалізують ці інтерфейси.

На рис. 4 наведена діаграма класів поточної версії комплексу, яка включає інтерфейси фільтру та аналізатору, а також декілька класів, що реалізують ці інтерфейси. Кожен з цих класів реалізований в окремому проекті dll-бібліотеки.

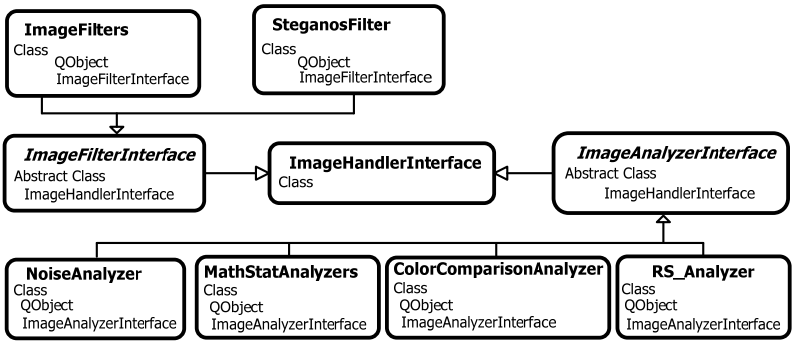

Рис. 4. *Діаграма класів фільтрів та аналізаторів*

Крім інтерфейсів на діаграмі наведені 2 класи фільтрів та 4 класи аналізаторів:

- ImageFilters — реалізує набір стандартних графічних фільтрів: GaussianBlur, Defocus, Highlight, Sharpen, BigEdge, Emboss, EmbossColor, EdgeDetect, Negative, RemoveChannel, Punch;
- SteganosFilter — реалізує фільтри приховування даних, які базуються на алгоритмі НЗБ;
- MathStatAnalyzers — виконує аналіз зображень методами математичної статистики, повертає середнє значення, середньоквадратичне відхилення та медіану для декількох характеристик з різних кольорових просторів;
- RS-Analyzer — виконує RS-аналіз зображення та повертає набір відповідних коефіцієнтів;

- ColorComparisonAnalyzer — виконує порівняння кольорових складових пікселів зображення (R, G, B) та повертає статистику по співвідношенням між ними;
- NoiseAnalyzer — повертає дві шумові характеристики для різних кольорових просторів.

Надалі кількість таких класів фільтрації та аналізу буде розширюватись для підтримки нових методів та алгоритмів. Робота з комплексом розбивається на декілька етапів:

1. Вибір файлу бази даних, в якому буде зберігатись статистика.
2. Додавання папок із зображеннями, які необхідно обробити. При цьому підтримується рекурсивна обробка піддиректорій та завдання списку масок файлів для обробки.
3. Завдання послідовності екземплярів фільтрів та аналізаторів, якими будуть оброблятись та досліджуватись фотографії. Фільтр — це модуль, який змінює зображення, наприклад, виконує його фільтрацію чи приховування даних певним алгоритмом. Аналізатор повертає певний набір статистики. Для модулів обох типів може задаватися набір специфічних для них параметрів (наприклад, коефіцієнти роботи алгоритмів фільтрації та аналізу) — таким чином створюються екземпляри фільтрів та аналізаторів, які і додаються в послідовність.
4. Запускається на виконання завдання обробки файлів по даним попередніх етапів. Реалізація обробки виконана по схемі робочих потоків, які незалежно оброблюють файли зображень, завдяки чому підвищено ефективність паралельної обробки на SMP-системах. Підтримка розподілених систем планується в наступних версіях комплексу.
5. Після закінчення обробки накопичена статистика доступна для вибірок та експорту у вигляді звітів трьох типів (рис. 5).

Статистика по зображенням дозволяє отримати результати аналізу зображень по кожному файлу окремо. При цьому можна вибрати необхідний набір даних, які будуть виводитись для зображень, а також задати умову фільтрації по ним, наприклад: ([Ширина] > 1000) and ([Висота] > 1000) and ([Ім'я] like 'nature%'). На другій вкладці можна вибрати набір даних статистики, яку необхідно вивести. Набір доступних даних статистики відображається у вигляді дерева, яке містить послідовності екземплярів фільтрів та аналізаторів з вкладеними списками статистики, яку можна включити в звіт. За даними статистики також можна виконувати фільтрацію, задаючи потрібним колонкам символічні імена та використовуючи їх у виразі фільтру, наприклад: ([a1] > 90) and ([a2] > 40). Після завдання параметрів звіту можна переглянути результат на третій вкладці. Його можна експор-

тувати в csv-файл для подальшої обробки в табличному процесорі типу Майкрософт Ексель.

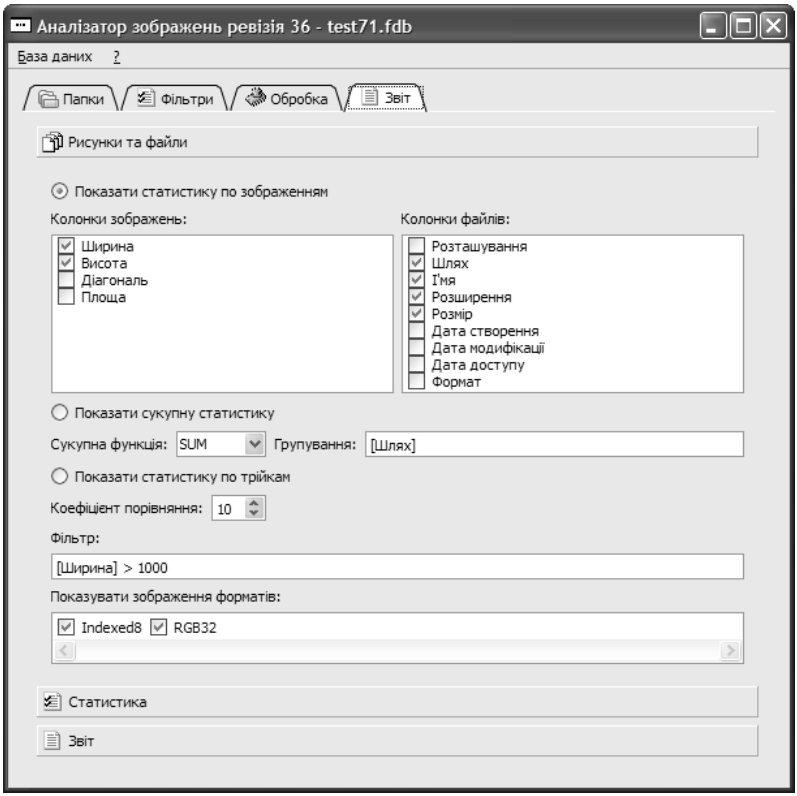

Рис. 5. *Параметри отримання звіту зі статистикою*

Другий варіант статистики — сукупний. Він дозволяє виводити агреговану вибраною функцією (мінімум, максимум, сума, кількість та середнє значення) статистику по вибраним даним, згруповану по відповідним колонкам. Наприклад, можна отримати сумарну статистику окремо по всім папкам, в яких знаходяться оброблені зображення. Третій варіант статистики дозволяє отримати частоти появи трійок, що відображають співвідношення трьох вибраних величин.

Приклади результатів досліджень. Дослідження впливу цифрових фільтрів на значення ПВС

Відомо, що зображення з мереж загального доступу можуть мати цифрові водяні знаки, над ними можуть бути виконані операції покращення візуальної якості або спеціальні дизайнерські перетво-

рення типу підготовки до друку. Тому було взяти 1700 фотографій з аматорської колекції, зроблені мобільним телефоном та цифровою камерою, над якими гарантовано не виконували будь-які перетворення. Далі вибірка була оброблена існуючими фільтрами (посилення кольору, зменшення/збільшення різкості, замулення і т.п.) і було виконано RS-стегоаналіз результати якого наведено у табл. 1, 2.

Результатами експериментів показали, що більшість зображень можна розділити на три типи:

1) зображення, на які перетворення суттєво впливають в напрямку зменшення або збільшення ПВС;
2) зображення, ПВС яких мало змінюється в результаті застосування фільтрів та перетворень будь-яких типів;
3) зображення, ПВС яких змінюється при застосуванні одних перетворень і мало змінюється при використанні інших.

За впливом конкретного фільтру на вибірку можна виділи фільтри, що зменшують ПВС (табл. 2) та такі, що збільшують ПВС (табл. 1). Дослідження будуть продовжені в напрямку розширення номенклатури фільтрів і їх комбінацій, що будуть застосовуватись до вибірок цифрових фотографій.

Таблиця 1

Кількість зображень у групах, що відповідають фільтрам, які збільшують ПВС

Назва фільтру і класифікація операції	**Кількість зображень, %**				
		2% - max			
	0-2%	2% - max	2-5 %	5-10 %	10% - max
Оригінал	80,7	19	13	4,6	1,7
Multiply_15	74,2	26,8	19,2	4,6	2
Overlay_15	75	25	20	4	1
High Pass_15	78	22	13	7	2
Reduce_noise	80,9	19,1	14,4	3,6	1,1
AutoContrast+ FocusRestoration	3,1	96,9	12,5	19	65,4
Normalize	79,27	20,73	13,7	5,15	1,88
Blur_3+ Sharpen_40	73,6	26,4	16,9	6	3,5

Таблиця 2

Кількість зображень у групах, що відповідають фільтрам, які зменшують ПВС

Назва фільтру і класифікація операції	Кількість зображень, %			
	2% - max	2-5 %	5-10 %	10% - max
Оригінал	19	13	4,6	1,7
Медіанний	0,06	0,06	-	-
Гауссівський	0,35	0,35	-	-
Minimum_3x3	1,94	1,94	-	-
Average_3x3	2,12	2,12	-	-

Дослідження закономірностей у каналах. кольорових зображень за методом RS-стегоаналізу

В ході досліджень [7—10] авторами було виявлено нерівномірне співвідношення ХПВС по каналам кольорових зображень. Символами R, G, B позначено значення ХПВС, отриманого за RS-стегоаналізом для червоного, зеленого та синього каналів відповідно. За частотами співвідношень кольорів — нерівностями можна побудувати множину всіх можливих подій у вибірці. Елементарні події повної множини наведені на нижній строчці гістограми.

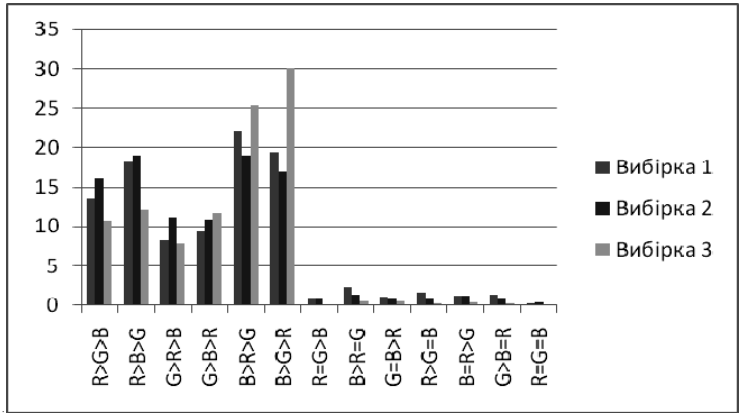

Рис. 6. *Співвідношення між ХПВС кольорових каналів*

Вибірка 1 — колекція з 41378 сучасних дизайнерських фотографій (DataCraft), Вибірка 2 — це набір тематично структурованих професійних цифрових фотографій, зроблених 10 років тому (8300 файлів), Вибірка 3 складається з 1700 фотографій і була зроблена співавтором Горінштейном М. цифровими фотоапаратами та камерами мобільних телефонів. Загальна кількість зображень склала 51378 файлів.

Висновки

1. Вперше запропоновано комплексну систему статистичних досліджень для методів стегоаналізу.
2. Розроблено нову модульну проблемно-орієнтовану архітектуру комплексу стегоаналітичних досліджень, яка дозволяє оператору гнучко змінювати напрямки збору статистики та експортувати отримані дані в додаток Майкрософт Ексель (електроні таблиці).
3. Завдяки створеному комплексу отримано нові результати в області приховування даних стеганографічними методами у зображеннях:
   - виявлено обмеження методу RS-стегоаналізу для багатьох класів зображень, доступних у мережі Інтернет;
   - запропоновано способи обходу методу RS-стегоаналізу;
   - показано, що для великих масивів зображень характерні залежності між статистичними характеристиками кольорових каналів з декількома максимумами.
4. Перспективними напрямками є дослідження нового методу WS-стегоаналізу та побудова аналогічного комплекса для стеганографії зображень у форматі JPEG, дослідження змін співвідношень між характеристиками кольорових каналів після фільтрації зображень та застосування методів ІАД до структурованої колекції зображень.

Список використаних джерел:

1. Задирака В. К. Комп'ютерна стеганографія / В. К. Задирака, І. В. Серієнко, І. М. Коваленко, П. І. Андон та ін. // Стан та перспективи розвитку інформатики в Україні : монографія. — К. : Наук. думка, 2010. — С. 736—747.
2. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.
3. Buhme R. Advanced Statistical Steganalysis / R. Buhme. — Springer, 2010.
4. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fridrich. — Cambrige University Press, 2010.
5. Аграновский А. В. Стеганография, цифровые водяные знаки и стеганоанализ : монография / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин, С. А. Сапожников. — М. : Вузовская книга, 2009. — 220 с.
6. Fridrich J. Detecting LSB Steganography in Color and Gray-Scale Images / J. Fridrich, M. Goljan, R. Du // Magazine of IEEE Multimedia, Special Issue on Security. — 2001. — P. 22—28.
7. Королёв В. Ю. Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей / В. Ю. Королёв, В. В. Полиновский, В. А. Герасименко // Управляющие системы и машины. — № 1 (231). — 2011. — С. 79—87.
8. Корольов В. Ю. RS-стеганоаналіз. Принципи роботи, недоліки та концепція метода його обходу / В. Ю. Королёв, В. В. Полиновский, В. А. Герасименко // Вісник Вінницького політехнічного інституту. — 2010. — № 6. — С. 66—71.
9. Корольов В. Ю. Визначення можливостей RS-стегоаналізу для дослідження статистичних властивостей зображень / В. Ю. Корольов, В. В. По-

ЗМІСТ

Андрейцев А. Ю., Смирнов І. В., Чорний А. В.
Нагрів та плавлення частинок порошку в плазмовому струмені 3

Бомба А. Я., Савюк Є. В.
Метод фіктивної фільтрації моделювання процесів руху рідин у водоймах з урахуванням впливу джерел поповнення течії..... 10

Васильев А. В.
Математические модели ПИД-контроллеров динамических систем в различных базисах..... 24

Верлань А. Ф., Чмырь И. А., Фуртат Ю. О.
Логическая структура транзакции эротетического диалога 35

Верлань А. А.
Способ параметрического контроля численного моделирования динамических объектов..... 56

Верлань Д. А.
Апроксимація функцій двох змінних в задачах керування..... 62

Горошко І. О., Павленко В. Д.
Формування нелінійних динамічних моделей газотурбінних силових установок при розв'язанні задач параметричної ідентифікації 70

Гридасов И. А.
Об одном подходе к организации кибернетической производственной системы на основе математического моделирования..... 80

Іванюк В. А., Тихоход В. А., Протасов С. Ю.
Інтегральні моделі ірраціональних та трансцендентних ланок 90

Карпенко В. М., Нікорюк Н. С.
Формування керуючого впливу пуску двигуна постійного струму з послідовним збудженням 99

Карпенко Є. Ю.
Узагальнений принцип нев'язки при розв'язанні інтегральних рівнянь Фредгольма I роду методом усіченого SVD розкладу..... 108

Конет І. М., Ленюк М. П.
Моделювання дифузійних процесів в неоднорідних середовищах з м'якими межами методом гібридного диференціального оператора Бесселя—Лежандра—Фур'є на сегменті полярної осі 112

Корнєєв О. М., Федорчук В. А.
Квадратурний алгоритм розв'язування систем інтегральних рівнянь Вольтерри з виродженими ядрами 123

Корольов В. Ю., Поліновський В. В., Герасименко В. А., Горінштейн М. Л.
Комплекс статистичних досліджень для стегоаналізу.....134

Мосенцова Л. В.
О решении обратной задачи определения области размещения источника тепла при известных значениях внешней температурной аномалии в среде MatLab.....149

Окрепкий Б. С., Алілуйко А. М.
Осесиметрична контактна задача термопружності про тиск штампа, що обертається, на пружний трансверсально-ізотропний шар.....155

Положаенко С. А.
Синтез законов оптимального управления энергетическими объектами, характеризующимися выраженным запаздыванием.....171

Рябова Н. В., Козополянская А. А., Шубкина О. В., Гринев С. А.
Модель семантического репозитория текстовых документов для онтологического портала МОНУ.....177

Сытник А. А., Наконечная О. А.
Определение временных характеристик сигналов акустической эмиссии 185

Сопель М. Ф.
Анализ искажений дискретных сигналов в линиях связи АСУ.....196

Шаповалова С. І., Мажара О. О.
Програмний комплекс діагностики економічного стану підприємства 209

Інститут кібернетики імені В. М. Глушкова
Національної академії наук України
Кам'янець-Подільський національний університет
імені Івана Огієнка

НАУКОВЕ ВИДАННЯ

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

Серія: Технічні науки

Збірник наукових праць

Випуск 5

Підписано до друку 12.09.2011 р. Гарнітура «Таймс».
Папір офсетний. Друк різографічний.
Формат 60x84/16. Умовн. друк. арк. 13. Обл.-вид. арк. 11,7.
Тираж 100. Зам. № 478.

Кам'янець-Подільський національний університет імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.

Надруковано в Кам'янець-Подільському національному
університеті імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.