внутрішнього апаратного контролю. Алгоритм 1 доцільно використовувати для контролю і діагностики автономних схем ШПФ, алгоритм для перевірки схем ШПФ у складі системи.

2. Застосування підходу за алгоритмом 2 дає змогу:

- виявити помилки у роботі з точністю до функціонального вузла, конструктивні та технологічні помилки під час проектування цифрових вузлів тощо;
- перевірити правильність функціювання і рівень шумів зовнішніх відносно ПОС пристроїв;
- оцінити вплив різних типів вагових функцій на значення вихідного сигналу;
- перевірити в режимі реального часу значення інформації, що надходить на вхід системи опрацювання;
- перевірити точностні параметри роботи процесорів;
- перевірити реакцію ПОС на надходження збійної інформації.

1. Jun-Fu Li, Cheng-Wen Lu. Efficient FFT network testing and diagnostic schemes // IEEE Trans. VLSI Syst. – June 2002. – Vol. 10. – P. 267–278, 2. Jun-Fu Li, Shyue-Kung Lu, Shih-Arn Hwang, Cheng-Wen Lu. Easily Testable and fault-tolerantt FFT butterfly network // IEEE Trans or circuits and systems. – Sept. 2000. – Vol. 47. – P. 919–929. 3. Бондарев В.Н., Трестер Г., Чернега В.С. Цифровая обработка сигналов: методы и средства: Учеб. пособие для вузов. – 2-е изд. – Харьков: Конус, 2001. – 398 с. 4 . Jain V.K., Al-Arian S.A., Landis D.L., and Nienbaus H.A. Fully parallel and testtable WSI architecture for an FFT-processor // Intern. Jorn. Of Computer Aided VLSI Design. – 1991. – Vol. 3. – P. 113–135. 5. Oh C.G., Youn H.Y., and R.aj. V.K. An efficient algoritm-based concurrent error detection for FFTnetwork // IEEE Trans Computer. – Sept. 1995. – Vol. 44. – P. 1157–1162. 6. .Yamashita K., Kanasugi A., and Goto G. A wafe-scale 100 000-gate FFT processor with built-in test circuit // IEEE Jorn.of Solid-State Citcuits. – 1988. – Vol. 23. – P. 336–342, 7. Antola A., Sami M.G., Sciuto D. Testing approaches for flowgraph-derived FFT arrays // Int.Conf. jn Systolic Arrays, KillarneyIreland. – 1989. – P. 325–334.

УДК 621.383

Є.Я. Ваврук, Є.Г. Міюшкович
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ДЕЯКІ АСПЕКТИ ФІЛЬТРАЦІЇ СТЕГОЗОБРАЖЕНЬ В КОМП’ЮТЕРНИХ МЕРЕЖАХ

Описано розроблені структурні схеми системи стегофільтрації цифрових зображень.

Developed structures of digital images stegofiltering system is circumscribed.

1. Постановка проблеми. Однією із складових політики інформаційної безпеки в сучасній обчислювальній системі є виявлення та ліквідація прихованих каналів витоку інформації. Згідно з [1] ефективним шляхом утворення прихованих каналів передачі даних є використання комп’ютерної стеганографії, методами та засобами якої забезпечується непомітна передача одних бітових послідовностей (файлів, секретних повідомлень) в інших бітових послідовностях (файлах-носіях, контейнерах).

Протилежним за метою, напрямком є стегоаналіз, головними завданнями якого є виявлення, читання, модифікація або знищення секретного повідомлення в об’єкті-контейнері.

Як контейнери в комп’ютерній стеганографії найчастіше застосовують об’єкти, що мають аналогову природу – оцифровані зображення, звук та відео. Тут під поняттям контейнера будемо

розуміти лише оцифровані зображення. Вибір напрямку досліджень пов'язаний з широкою присутністю цього типу контейнерів у мережі Інтернет, що підтверджується [1, 3, 6, 7].

2. Сучасні методи приховування та виявлення інформації у зображеннях. Вичерпну класифікацію методів стеганографії зображень наведено в [2]. Всі існуючі методи за способом вкладення секретних повідомлень у зображення можна поділити на такі основні групи:

1) методи, що модифікують зображення у просторовій області (прямі методи);

2) методи, що модифікують трансформовані зображення;

3) методи, що використовують фрактальне кодування зображень;

4) методи, що використовують специфічні особливості формату файла зображення;

Всі ці методи пов'язані з різними способами кодування зображення.

2.1. Прямі методи. Орієнтовані на растрові формати представлення зображень (bmp, gif). Типовими представниками цієї групи є методи модифікації найменш значущих біт зображення (LSB методи). Головною перевагою цих методів є простота застосування, можливість приховувати порівняно великі повідомлення (до 1/8 об'єму контейнера) та наявність в Інтернеті безкоштовних утиліт (S-Tools, Steganos for Win95, Contraband). Стійкість прямих методів до виявлення, модифікації та знищення повідомлення є низькою. Для виявлення цих методів застосовуються:

1. "Візуальна атака" – використання спеціального фільтра, який будує зображення на основі молодших розрядів кольорів. Оскільки між молодшими бітами зображень існують кореляційні зв'язки (особливо це стосується штучних зображень), то спостерігач може легко виявити факт вкладення.

2. Атака "ксі квадрат" (chi-square attac) запропонована Вестфельдом (Westfeld), базується на статистичному аналізі першого порядку. Оригінальна версія атаки [3] виявляє послідовно вкладені повідомлення. В [4, 5] вона була узагальнена для виявлення випадково розміщених повідомлень.

3. Метод PQR [6], запропонований Фрідріч (Fridrich). Обчислюються статистичні характеристики підозрілого зображення, здійснюється вкладення тестового прихованого повідомлення та проводиться повторне обчислення статистик. Якщо результати близькі між собою, то найімовірніше підозри були виправданими. Як статистичні характеристики використовується кількість близьких пар кольорів, яка значно зростає при вкладенні повідомлення.

Методи знищення повідомлень у зображеннях є тривіальними – це може бути або проста підстановка псевдовипадкової величини замість молодших бітів зображення, або застосування процедури стискання/розтискання з втратами (наприклад JPEG).

До прямих також належать методи модифікації палітри. Характерною ознакою використання цих методів є наявність у зображенні нестандартно впорядкованих палітр або палітр з аномальним набором кольорів. Для знищення повідомлення у більшості випадків достатньо відкрити та зберігти файл у будь-якому стандартному редакторі растрових зображень, що призведе до перевпорядкування палітр.

2.2. Методи на основі трансформації зображень. У цих методах інформація вбудовується у набір коефіцієнтів, які є результатом певного перетворення вихідного зображення. При застосуванні формату JPEG модифікуються коефіцієнти дискретного косинусного перетворення (ДКП), при JPEG2000 – коефіцієнти вейвлітного перетворення. У [2] розглядається можливість використання інших перетворень – Фур'є, Карунена – Лоєва, сингулярного розкладу, але вони мають швидше теоретичне значення, оскільки ці перетворення не використовуються у розповсюджених форматах зберігання зображень.

Методи на основі трансформації зображень характеризуються підвищеною, порівняно з попередніми, стійкістю до виявлення та спотворення вкладеної інформації.

Зважаючи на розповсюдженість формату JPEG, зупинимося на ньому детальніше.

Станом на 2003 р. відомі декілька основних методів вкладення секретних повідомлень у зображення в форматі JPEG [7]. Це J-Steg, JPHide/JPSeek, F5 та OutGuess. Всі вони застосовують маніпуляції з квантованними значеннями коефіцієнтів ДКП. J-Steg та JPHide/JPSeek безпосередньо

розміщають повідомлення у молодших бітах коефіцієнтів і тому виявляються за допомогою простої або модифікованої атаки "ксі-квадрат". Алгоритми F5 та Outguess зберігають статистики першого порядку і тому проти них застосовується статистичний аналіз вищих порядків [7, 8].

Зараз ведеться активна розробка т. зв. "сліпих" методів стегоаналізу [9–11, 13], які потенційно спроможні виявити секретні повідомлення, незалежно від застосованого методу їх вкладення. У цих методах "сліпий" детектор вивчає зображення у багатовимірному просторі ознак. Згодом проводиться навчання детектора для виявлення розбіжностей між ознаками зображень-контейнерів та стегозображень.

Запропоновані Фарідом (Farid) 72 характерні ознаки обчислюються в результаті вейвлітного перетворення стегозображення [10]. Для класифікації зображень використовується метод машинного навчання на основі опорних векторів (Support Vector Machine).

Об'єднавши підхід Фаріда із власним методом характерних статистик [8], Фрідріч запропонувала новий метод аналізу на основі каліброваних ознак, що обчислюються у просторі коефіцієнтів ДКП [11]. Тут застосовується метод машинного навчання під назвою лінійний дискримінант Фішера (Fisher Linear Discriminant classifier).

Цоппе (Tzschoppe) [12] запропонував метод вкладення повідомлень у JPEG зображення, який принципово не виявляється схемою Фаріда, хоча і детектується на основі однієї скалярної ознаки – каліброваної просторової блоковості.

Відома також спроба побудови сліпого детектора заміною машини опорних векторів у методі Фаріда генетичнми алгоритмами [13], але повідомлень про успішне закінчення розробки наразі немає.

2.3. Методи, що використовують фрактальне кодування зображень. Ідея методів цього класу полягає у конструюванні для зображення його фрактального коду таким чином, щоб декодоване зображення вже містило вбудовану інформацію. На сьогодняшній день ці методи мають більше теоретичне значення, що зумовлене обмеженим використанням фрактальних методів стиску зображень.

2.4. Методи на основі особливостей форматів файла зображення. Для вкладення повідомлень використовуються зарезервовані поля у форматах, можливість додавання коментарів до файлів та інші подібні підходи. Повідомлення легко виявляються та знищуються, оскільки для цього достатньо проаналізувати та обнулити ці поля даних.

3. Постановка задачі. Вище було відзначено, що прихований канал у межах легального каналу може бути утворений зловмисником із використанням методів стеганографії зображень (рис. 1). Оскільки стандартні засоби мережевого моніторингу неспроможні виявити факт вкладення повідомлень, задача розробки спеціалізованого фільтра є актуальною.

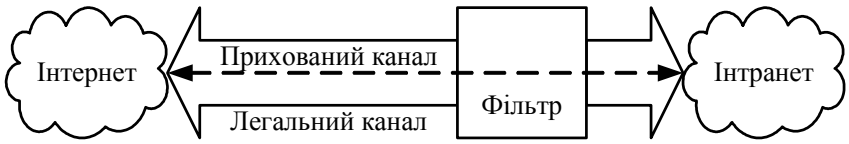

Рис. 1. Схема утворення прихованого каналу

4. Опис структури стегофільтра. Узагальнену структурну схему системи фільтрації стегоповідомлень у мережевому графіку наведено на рис. 2.

Схема сортування виділяє з вхідного трафіку мережі потенційні об'єкти-контейнери (в нашому випадку – файли із зображеннями), які направляються на подальший аналіз. Решта вхідних даних буферизується до закінчення процесу стегофільтрації контейнерів. Стегофільтр виявляє та знищує приховані повідомлення у об'єктах-контейнерах. Вихідний мультиплексор з буферизованих даних формує вихідний трафік, заміняючи при потребі підозрілі контейнери на очищені стегофільтром варіанти.

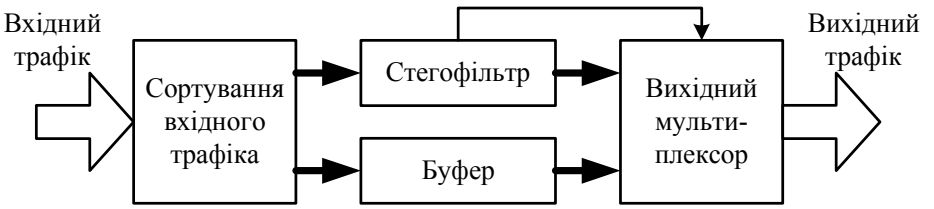

Рис. 2. Структурна схема системи стегофільтрації

Загальна часова затримка системи стегофільтрації T_{filt} визначається виразом (1):

$$T_{filt} = T_{sort} + T_{stg} + T_{mux}\,, \tag{1}$$

де T_{sort} , T_{stg} , T_{mux} – відповідно час роботи схеми сортування, стегофільтра та вихідного мультиплексора.

Беручи до уваги, що $T_{mux} << T_{sort} << T_{stg}$, отримуємо таке співвідношення:

$$T_{filt} \approx T_{stg}\,. \tag{2}$$

Отже, загальна пропускна здатність системи стегофільтрації переважно визначається продуктивністю стегофільтра, яка, в свою чергу, залежить від варіантів його реалізації та застосованих технологій.

Основними складовими стегофільтра є стегодетектор та стерилізатор. Стегодетектор виявляє факт наявності прихованих повідомлень у мережевому трафіку, а стерилізатор знищує ці повідомлення.

На структурну реалізацію стегофільтра впливає інтенсивність потоку даних, що надходять на обробку та продуктивність обчислювальних вузлів системи.

При низькій інтенсивності надходження підозрілих контейнерів операції детектування та знищення повідомлень можна здійснювати послідовно, використовуючи для цього один універсальний обчислювач. Цей підхід орієнтований на програмну реалізацію стегофільтра у складі мережевого екрана (типу brandmauer).

Схему послідовного стегофільтра наведено на рис. 3.

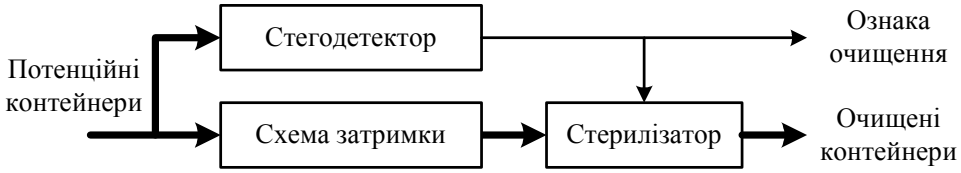

Рис. 3. Схема послідовного стегофільтра

Вузол затримки призначений для зберігання досліджуваного контейнера під час роботи стегодетектора, що дає змогу організувати потокову обробку.

Часові параметри послідовного стегофільтра визначаються співвідношенням (3):

$$T_{stg} = T_{det} + T_{cln}\,, \tag{3}$$

де T_{det} – час виявлення прихованих повідомлень стегодетектором; T_{cln} – час очищення контейнера від повідомлень стерилізатором.

При зростанні інтенсивності мережевого трафіку ефективнішою є паралельна схема стегофільтра (рис. 4), яка характеризується підвищеними апаратними витратами.

При такому підході здійснюється примусове формування очищених контейнерів, а стегодетектор лише визначає необхідність їх використання.

Часові параметри паралельного стегофільтра визначаються співвідношенням (4):

$$T_{stg} = \max\,(T_{det}\,,\, T_{cln}\,) \tag{4}$$

Рис. 4. Схема паралельного стегофільтра

У випадку обробки великих потоків даних часу на стегоаналіз може просто не залишитися. Тоді єдиним виходом є примусове очищення та заміна всіх потенційних контейнерів. Це пояснюється тим, що час виконання процедури очищення є значно меншим від часу, який необхідний для проведення стегоаналізу (див. п. 2). Такі самі заходи можуть бути рекомендовані за необхідності отримати гарантоване подавлення стегоповідомлень.

Висновки. Тут проаналізовані сучасні методи стеганографії та стегоаналізу цифрових зображень. Запропоновано узагальнену схему системи фільтрації стегоповідомлень та три підходи до реалізації стегофільтрів, наведені якісні оцінки їх пропускної здатності.

Область застосування запропонованих рішень не обмежується лише протидією стегоканалам на основі цифрових зображень. Зміною алгоритмів стегоаналізу та стерилізації можна створити ефективні фільтри для інших типів мультимедійних даних (цифрове аудіо та відео). Але, зважаючи на розповсюдженість цифрових зображень у інтернет-контенті, стегофільтрація цифрових зображень є пріоритетним напрямком.

На сьогодні найреальнішим є тотальне очищення зображень, оскільки воно не вимагає проведення стегоаналізу. Практичну реалізацію запропонованих паралельної та послідовної схем стегофільтра стримує відсутність швидких та надійних стегоаналітичних методів.

Тому подальші дослідження будуть спрямовані на пошук таких методів та вдосконалення запропонованих структурних рішень.

1. Алексей Галатенко. О скрытых каналах и не только. – Jet Info, 2002. – № 11. (http://www.jetinfo.ru). 2. Городецкий В.И., Самойлов В.И. Стеганография на основе цифровых изображений. – 2002. (http://www.iias.spb.su). 3. Westfeld, A. and Pfitzmann, A. Attacks on Steganographic Systems. In: Pfitzmann A. (eds.): 3rd International Workshop. Lecture Notes in Computer Science, Vol. 1768. Springer-Verlag, Berlin Heidelberg New York, 2000. – P. 61−75 4. Westfeld A. Detecting Low Embedding Rates. In: Petitcolas, F.A.P. (ed.): Information Hiding. 5th International Workshop. Lecture Notes in Computer Science, Vol. 2578. Springer-Verlag, Berlin Heidelberg New York, 2002. – P. 324–339 5. Provos, N. and Honeyman, P. Detecting Steganographic Content on the Internet. CITI Technical Report 01–11 (2001). 6. Fridrich J., Du R., Meng L. Steganalysis of LSB Encoding in Color Images, ICME 2000, New York City, 31 July −2 August 2000. 7. Fridrich, J., Goljan, M., Hogea, D., and Soukal, D. Quantitative Steganalysis: Estimating Secret Message Length. ACM Multimedia Systems Journal. Special issue on Multimedia Security. – 2003. – Vol. 9(3). – P. 288–302. 8. Fridrich J., Goljan M., Hogea D.: New Methodology for Breaking Steganographic Techniques for JPEGs, Proc. EI SPIE Santa Clara, CA, Jan 2003. – P. 143–155. 9. Avcibas I., Memon N., Sankur B.: Steganalysis using Image Quality Metrics // SPIE Security and Watermarking of Multimedia Contents II, Electronic Imaging, San Jose, CA, Jan. – 2001. 10. Farid H., Siwei, L. Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines. In: Petitcolas, F.A.P. (ed.): Information Hiding. 5th International Workshop. Lecture Notes in Computer Science, Vol. 2578. Springer-Verlag, Berlin Hei-delberg New York, 2002. – P. 340–354. 11. Fridrich, J. Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes, Proc. 6th Information Hiding Workshop, Toronto, Canada, 23–25 May 2004. 12. Tzschoppe, R., Bäuml, R., Huber, J.B., Kaup, A. Steganographic System based on Higher-Order Statistics. Proc. EI SPIE Electronic Imaging. Santa Clara. – 2003. – P. 156–166. 13. Jackson J., Gunsch G., Claypoole R., Lamont G. Blind Steganography Detection Using a Computational Immune System: A Work in Progress // International Journal of Digital Evidence, Winter 2003, Issue 1, Volume 4 (www.ijde.org).