УДК 004.056.(0.45)

МЕТОДИ ПІДВИЩЕННЯ СТІЙКОСТІ СТЕГАНОСИСТЕМ ДО НЕСАНКЦІОНОВАНОГО ДОСТУПУ

А. В. Чунарьова, канд. техн. наук, доц.; ***Є. О. Потапенко***

Національний авіаційний університет

Yevgeniy_Potapenko@bigmir.net

Проведено системний аналіз існуючих на сьогодні методів підвищення стеганографічної стійкості систем до різних видів атак, яким може піддаватися стеганографічний контейнер у каналі передачі інформації. Проведено систематизацію моделі порушника стегосистеми, а також відповідно до цього виконано класифікацію видів атак. Наведено найбільш дієві методи захисту стеганографічних даних та загальні рекомендації щодо їх використання.

Ключові слова: стеганографічна система, модель порушника, стійкість, активні атаки, пасивні атаки, стеганографічний контейнер.

In this paper, an analysis system currently existing steganographic methods for improving the stability of different types of attacks, which can be subjected to steganographic container in a channel of information transfer. An offender stegosystem systematization model and, according to this, a classification of types of attacks. As a result, given the most effective methods to protect steganographic data, and general guidelines for their use.

Keywords: steganography system model intruder, stability, active attacks, passive attacks, steganographic container.

Вступ

На сьогодні, у зв'язку з бурхливим розвитком інформаційних технологій та розгалужених інформаційних систем, гостро постала проблема захисту інформації від несанкціонованого доступу. Питаннями захисту інформації переважно займаються криптографія та стеганографія.

Перша наука проводить захист інформації шляхом перетворення відкритого тексту в набір шифрованого тексту, а друга — вбудовуванням відкритих даних в інший набір даних (зображення, заголовки файлів тощо).

Ураховуючи, що наука, «стеганографія» сформувалася досить недавно, то й відповідно надає значно більше можливостей для вдосконалення та створення нових методів порівняно із криптографією, розвиток якої здебільшого йде в напрямку збільшення довжини ключів, і відповідно цим самим підвищення ступеня захисту інформації.

Постановка проблеми

Сучасні методи стеганографії полягають у тому, що останні, використовуючи нові досягнення в області криптографії, цифрової обробки інформації, дозволяють не тільки приховано передавати дані, але й цілком успішно розв'язувати задачі, пов'язані з завадостійкою аутентифікацією, захистом інформації від несанкціонованого копіювання, відслідковувати поширення інформації системами зв'язку.

Стеганоконтейнери (відкриті файли, які містять у собі приховані стеганографічним методом конфіденційні дані) під час передачі по відкритих каналах зв'язку можуть піддаватись різного роду атакам (як активним, так і пасивним), і відповідно до цього, необхідно, при обранні стеганографічного алгоритму приховування даних брати до уваги методи підвищення стійкості стеганоконтейнерів до даних атак, які безпосередньо розглядаються в цій статті.

Мета роботи — аналіз та систематизація існуючих методів підвищення стійкості стеганоконтейнерів до активних та пасивних атак.

Основна частина

Всі існуючі нині стеганографічні системи захисту інформації можна умовно поділити на три групи [1], які включають у себе теоретично стійкі системи, тобто ті, абсолютна теоретична надійність яких доведена математично в повному обсязі.

Дані системи під час приховування інформації використовують лише ті проміжки стеганоконтейнера, зміна яких не призведе до щонайменшої зміни статистичної функції контейнера. Відповідно до цього, в даних стеганографічних системах необхідна функція попереднього обрахування статистичних характеристик контейнера на основі обраних його частин, в які буде виконуватись стеганоприховування.

Другу групу формують практично стійкі стеганографічні системи. Дані системи відрізняються від попередніх тим, що для приховування використовують також ті проміжки (біти) контейнера, зміна яких може бути виявлена, але за умови, якщо відомо, що на даний час не існує таких методів, які б могли виявити ці зміни.

У цих системах також необхідним є використання статистичної функції, але на відміну від функції, яка використовується в теоретично стійких системах, значення даної функції не повинно перевищувати деякої наперед відомої величини. Тобто, під час зміни деяких бітів контейнера його статистична функція може змінювати своє значення, але воно повинне попадати в попередньо заданий діапазон. Нарешті, до третьої групи, відносять нестійкі стеганографічні системи, тобто ті, що проводять процес приховування інформації, і при цьому не звертають своєї уваги на будь-які зміни статистичної функції. Під час стеганоаналізу таких контейнерів факт наявності прихованих даних з'ясовується досить швидко.

Ураховуючи вказану вище класифікацію стеганографічних систем, найбільш дієвими методами підвищення стійкості до стеганоаналізу є використання в якості контейнера такої послідовності даних, приховування інформації в яких взагалі не буде вносити ніяких змін, а також, зменшення діапазону зміни статистичної функції. Перший варіант можливо реалізувати, за умови введення такої функції залежності [2]:

$$y = f(x), \qquad (1)$$

де y — послідовність бітів обраного контейнера; $f(x)$ — конфіденційна інформація, що підлягає захисту.

Відповідно до виразу (1), обрання контейнера повинно відбуватись за умови відомих приховуваних даних. Тобто, наприклад, на вхід системи подається конфіденційна інформація, після цього стеганосистема проводить пошук у своїй базі контейнерів, того, структура якого повністю відповідає приховуваним даним і лише після цього відбувається стеганоприховування. Тим не менш, даний варіант не є досить практичним, оскільки для його реалізації потрібна наявність великої кількості стеганоконтейнерів, щоб підібрати для приховування інформації той контейнер, який повністю відповідає приховуваним даним.

На практиці більш оптимальним є другий варіант, коли величина зміни статистичної функції не повинна перевищувати певного порогового значення, наперед заданого для конкретної стеганографічної системи. У цьому випадку, перед стеганоприховуванням, також відбувається пошук найбільш оптимального контейнера, але тим не менш, він не повинен повністю відповідати приховуваним даним. Якщо ж говорити про стійкість стеганосистеми, з урахуванням виду порушника, який може впливати на стеганографічний канал, то тут переважно виділяють три ієрархічні рівні правопорушника [1].

До першого рівня відносять пасивного порушника, який здатний лише виявити стеганографічний канал обміну інформацією, і ніяким чином не може впливати на нього.

До другого рівня відносять активного правопорушника, який на відміну від пасивного, окрім виявлення стеганоканалу спроможний також його перекривати, тобто руйнувати стеганоконтейнери.

Третій рівень правопорушника є найбільш небезпечним, оскільки тут він може не лише руйнувати стеганоканал, а також може носити певні зміни в стеганоконтейнер, цим самим створювати канал дезінформації між відправником та отримувачем стеганоповідомлень.

У загальному випадку, в процесі зламу стеганосистеми можна виділити такі етапи [3]:

1) визначення факту прихованих даних;
2) вилучення прихованих даних;
3) модифікація прихованих даних;
4) встановлення заборони пересилання будь-яких даних.

Пасивний порушник в основному реалізує лише перший етап зламу стеганографічної системи, тим не менш у працях [3; 5] також зазначається, що до даного рівня порушника також може відноситись і другий етап.

До активного порушника відносять третій та четвертий етап, оскільки для їх реалізації необхідні найбільші можливості, котрі відповідно має даний рівень порушника.

Кожен рівень правопорушника реалізує свій рівень загроз відповідно до його можливостей. Виходячи із цього, існує два рівня атак, спрямованих проти стеганорафічної системи: активні та пасивні атаки. Стійкість стеганосистеми до пасивних атак в основному ґрунтується на тому, що пасивний правопорушник для виявлення стеганографічного каналу обміну інформацією користується різного роду статистичними функціями, які здатні виявляти певні неоднорідні ділянки стеганоконтейнера (наприклад, неоднорідність бітів зображення), ділянки з досить великою зашумленістю та інші специфічні для кожної стеганосистеми ознаки. У результаті, пасивний порушник зі своєї сторони створює статистичну функцію, яка здатна після пропускання через себе заповненого контейнера дати відповідь про наявність чи відсутність прихованих даних.

Загалом, дану функцію можна подати в такому вигляді[4]:

$$Q = f(m) = \begin{cases} 1, \text{ якщо є приховані дані} \\ 0, \text{якщо нема прихованих даних} \end{cases} \qquad (2)$$

У формулі (2) під $f(m)$ мається на увазі статистична функція, прийняття рішення про наявність прихованих даних; m — двійкові дані стеганоконтейнера.

Структурний вигляд детектора прихованих повідомлень, який використовується зловмисником, подано на рис. 1.

Рис. 1. Структурна схема детектора стеганограм

Виходячи із сказаного вище та беручи до уваги відомості із теорії зв'язку, в системі виявлення прихованого стеганоканалу може відбутись два типи помилок: «хибна тривога» (помилка першого роду) та «пропущення цілі» (помилка другого роду) [4]. Перша помилка полягає в тому, що система порушника повідомляє йому про те, що в контейнері є приховані дані, коли насправді вони там відсутні, а друга помилка — в тому, що система повідомляє про відсутність стеганоданих, коли вони насправді присутні. Дані типи помилок, зв'язані пропорційно між собою, тобто збільшення ймовірності появи однієї веде до зменшення ймовірності появи іншої.

Отже, одним із методів підвищення ступеня захисту стеганографічних систем до пасивних атак, є підвищення ймовірності виникнення помилки другого роду (ідеально, коли вона дорівнює одиниці), і відповідно до цього помилка першого роду, в свою чергу буде прямувати до нуля.

Якщо ж говорити про стійкість стеганографічних систем до активних атак, то варто відзначити, що навіть за умови, що порушник не може прочитати приховані стеганографічні дані, то в нього завжди зберігається можливість простого їх руйнування. Враховуючи, що стеганоконтейнери досить чуттєві навіть до незначних змін, то порушнику достатньо навіть просто внести будь-який довільний шум, і дані зруйнуються, а якщо у випадку контейнера використовується наприклад зображення, то достатньо просто змінити його формат, або навіть застосувати будь-який простий фільтр для зображення. При цьому приховані дані не обов'язково піддаються повній руйнації, для неправильного декодування прихованих даних достатньо найменшої зміни в заповненому контейнері [5]. Тим не менш, це питання належить більше до стійкості стеганографічних методів, а не до атак на систему.

Стійкість стеганографічної системи до активних атак виражається в тому, що прихована інформація не може бути змінена або видалена без суттєвих змін заповненого стеганоконтейнера. Тобто, якщо порушнику вдасться змінити приховані дані, то контейнер, в якому вони були приховані, не зможе надалі використовуватись у системі, оскільки приймаюча сторона одразу виявить такі зміни. Для підвищення стійкості стеганосистем може використовуватись, наприклад, завадостійке кодування. Але, у свою чергу, стійкі системи є ненадійними, що пояснюється великою надлишковістю приховуваного тексту при використанні того самого завадостійкого кодування [2]. Процес приховування інформації призводитиме до значних змін вихідного контейнера, і зловмисник досить просто зможе дізнатись про організований прихований стеганографічний канал.

Тим не менш, на практиці досить поширеним є створення стеганосистем, які стійкі лише до певного виду атак (наприклад, стиснення, фільтрація, зміна формату контейнера, внесення додаткових шумів і т. д.) [1].

Отже, перед проектуванням даних систем необхідний попередній аналіз усіх можливих атак, і подальша адаптація цих систем до конкретного профілю загроз. Недоліком даного методу можна назвати те що в процесі використання цієї системи можлива поява нових видів загроз, адаптація до яких взагалі неможлива у використовуваній системі, або ж вона призведе до значного зменшення ступеня захисту системи до раніше виявлених атак. У результаті необхідно буде знову формулювати новий профіль загроз, і створювати нову систему, що є досить довгим та коштовним процесом. Також під час розробки нового профілю захищеності стеганосистеми відпаде можливість обміну конфіденційними даними, що також є небажаним процесом. Після створення стеганографічної системи досить важливим етапом, що передує її безпосередньому впровадженню, є процес моделювання її роботи та оцінювання стійкості створеної стеганосистеми до різних видів атак. Загальна структура даного процесу показана на рис. 2.

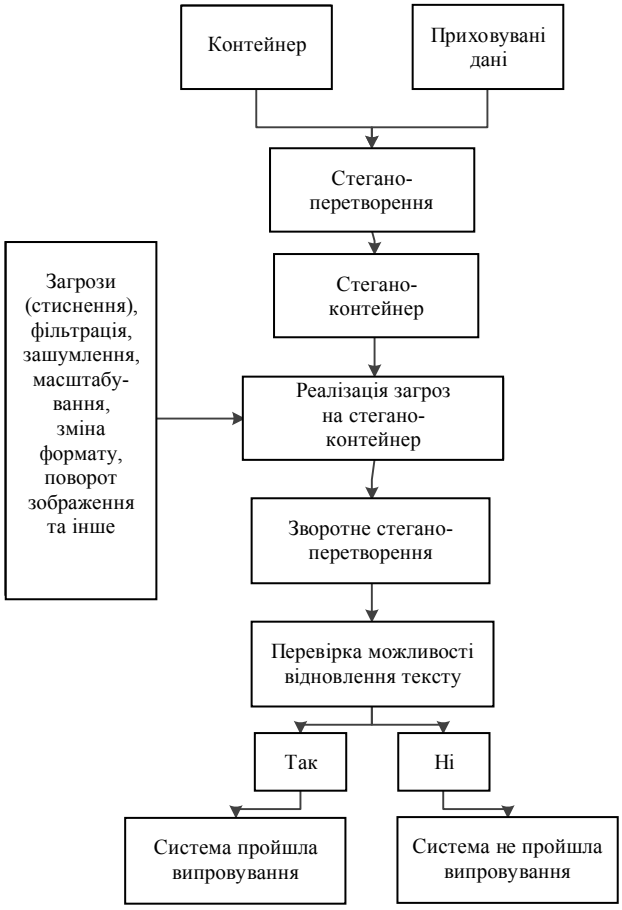

Рис. 2. Процес перевірки надійності стеганографічної системи

Аналізуючи сказане вище, можна зробити висновок, що підвищення стійкості стеганосистем до активних атак відбувається за такими напрямками:

1. Створення стеганографічних систем, які є стійкими до деякого наперед заданого профілю загроз;

2. Використовуване в системі стеганографічне приховування інформації повинно відбуватись у найбільш значущі області контейнера. Відповідно зміна або видалення інформації з даних областей призводить до значного або повного руйнування контейнера, після чого приймаюча сторона одразу виявить дії зловмисника (даний метод переважно використовується в системах вбудовування ЦВЗ);

3. Реалізовані стеганографічні перетворення повинні бути оберненими відносно до можливих модифікацій, тобто у випадку, коли порушник модифікував певну частину стеганограми, приймаюча сторона повинна мати можливість відновити первинні дані.

Прикладом цього може служити метод «афінного кодування даних» [1], котрий передбачає оцінку параметрів виконаного зловмисником перетворення, оцінку зміни форми заповненого контейнера та його складових, а також оцінку деяких розмірів та напрямків кодових послідовностей у контейнері.

Як зазначається в праці [3], теоретично надійна стеганографічна система повинна реалізовувати трирівневу модель захисту інформації:

– перший рівень — стеганографічне приховування конфіденційної інформації;

– другий рівень — унеможливлення несанкціонованого ознайомлення із прихованою інформацією, що полягає у виборі конкретного стеганографічного методу;

– третій рівень — перед приховуванням інформації відбувається попереднє криптографічне шифрування.

Висновки

У даній статті було розглянуто трирівневу модель класифікації стеганографічних систем захисту інформації, в якій основним критерієм виступає ступінь захисту інформації. Встановлено, що для створення надійної системи необхідно, щоб контейнер для приховування інформації являв деяку функцію залежності від приховуваного тексту, що є вхідним параметром для цієї функції. Розглянуто модель порушника, і відповідно до цього види загроз, яким може піддаватись стеганографічний контейнер у процесі передачі через незахищений канал. Встановлено загальні вимоги до системи щодо протидії активним та пасивним атакам. Було розглянуто методи підвищення захисту стеганосистеми на процесі її проектування та введення в дію.

ЛІТЕРАТУРА

1. *Основи* комп'ютерної стеганографії: навч. посіб. / В. О. Хорошко, О. Д. Азаров, М.Є. Шелест, Ю. Є. Яремчук. — Вінниця : ВДТУ, 2003.

2. *Барсуков В. С.* Компьютерная стеганография: вчера, сегодня, завтра. Технологии информационной безопасности XXI века / В. С. Барсуков, А. П. Романцов // Матеріали Internet-ресурсу «Специальная техника» (http://st.ess.ru/).

3. *Грибунин В. Г.* Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : Солон-Пресс, 2002.

4. *Конахович Г. Ф.* Компютерна стеганографії. Теорія та практика / Г. Ф. Конахович, А. Ю. Пузиренко. — Мк-прес, 2006, 288 с.

5. *Барсуков В. С.* Стеганографические технологии защиты документов, авторских прав и информации / В. С. Барсуков // Обзор специальной техники. — 2000. — № 2. — С. 31–40.

Стаття надійшла до редакції 08.04.2014.