УДК 004.056.5:004.7

СИСТЕМАТИЗАЦІЯ ТА КЛАСИФІКАЦІЯ НАЯВНИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

О. В. Весельська, Р. В. Зюбіна, О. В. Фролов

Національний авіаційний університет

kszi@ukr.net

Проведено аналіз наявних способів класифікації стеганографічних методів, обробка та систематизування цих методів. Визначено, що, окрім загальновідомих методів стеганографічного захисту, окремим розділом стеганографії можна винести мережеву стеганографію, де в якості носіїв секретних даних використовуються мережеві протоколи еталонної моделі OSI. Створено оптимальну систему класифікації всіх методів стеганографії. Визначено, що для більшості сучасних методів, використовуваних для приховання повідомлення в цифрових контейнерах, має місце експоненційна залежність надійності системи від обсягу вбудовуваних даних. Дана залежність показує, що при збільшенні обсягу вбудовуваних даних знижується надійність системи (при незмінності розміру контейнера). Таким чином, використовуваний в стегосистемі контейнер накладає обмеження на розмір вбудовуваних даних.

Ключові слова: стеганографія, мережева стеганографія, стеганосистема, контейнер.

The existing ways of classification of steganography methods, processing and their systematization were analysed. In addition to well-known methods of steganographic protection, as a separate section of steganography can be defined network steganography, whereas the secret data carriers, use network protocols OSI, were determined. The optimal system of classification of all methods of steganography was created. Determined that the most current methods, for hiding messages in digital containers, are using the exponential dependence of reliability of system of the volume of embedded data. This dependence shows that by increasing the volume of embedded data decrease the reliability of the system (at constant size of the container). Thus, used in stegosystem container imposes restrictions on the size of the embedded data.

Keywords: steganography, network steganography, steganosystem, container.

Вступ

На сучасному етапі розвитку інформаційної системи у цілому, та її засобів безпеки, існує потреба надійно застосовувати криптографічні та стеганографічні методи.

Сьогодні вже існують певні технологій приховування даних. Проте, в основі багатьох підходів до вирішення задач стеганографії лежить загальна з криптографією теоретична база.

Аналізуючи процес розвитку комп'ютерної стеганографії можна сказати, що в найближчі роки інтерес до розвитку її методів буде посилюватися дедалі більше і більше. Актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З іншого боку, бурхливий розвиток інформаційних технологій забезпечує можли-вість реалізації цих нових методів захисту.

Стеганографічні методи, поряд з криптографічними, займають важливе місце серед методів захисту інформації.

Але якщо в криптографії наявність шифрованого повідомлення само по собі привертає увагу зловмисника, то в стеганографії прихований зв'язок залишається непомітним, що робить організацію цього процесу досить актуальною.

Спільною рисою стеганографічних методів є те, що приховане повідомлення, або додаткова інформація, вбудовуються в деякий нешкідливий, не звертаючи на себе увагу об'єкт або контейнер, результатом чого є стеганоповідомлення, яке потім відкрито транспортується адресату по каналу зв'язку або зберігається в такому вигляді.

Мета статті — аналіз наявних способів класифікації стеганографічних методів, оброблення та їх систематизування.

Аналіз існуючих способів класифікації стеганографічних методів

У праці [1] запропоновано поділ стеганографії на технологічну та інформаційну (рис. 1).

У сучасній літературі найчастіше виділяють чотири напрями стеганографії [2]:

1. Класичний.
2. Цифровий.
3. Лінгвістичний..
4. Квантовий.

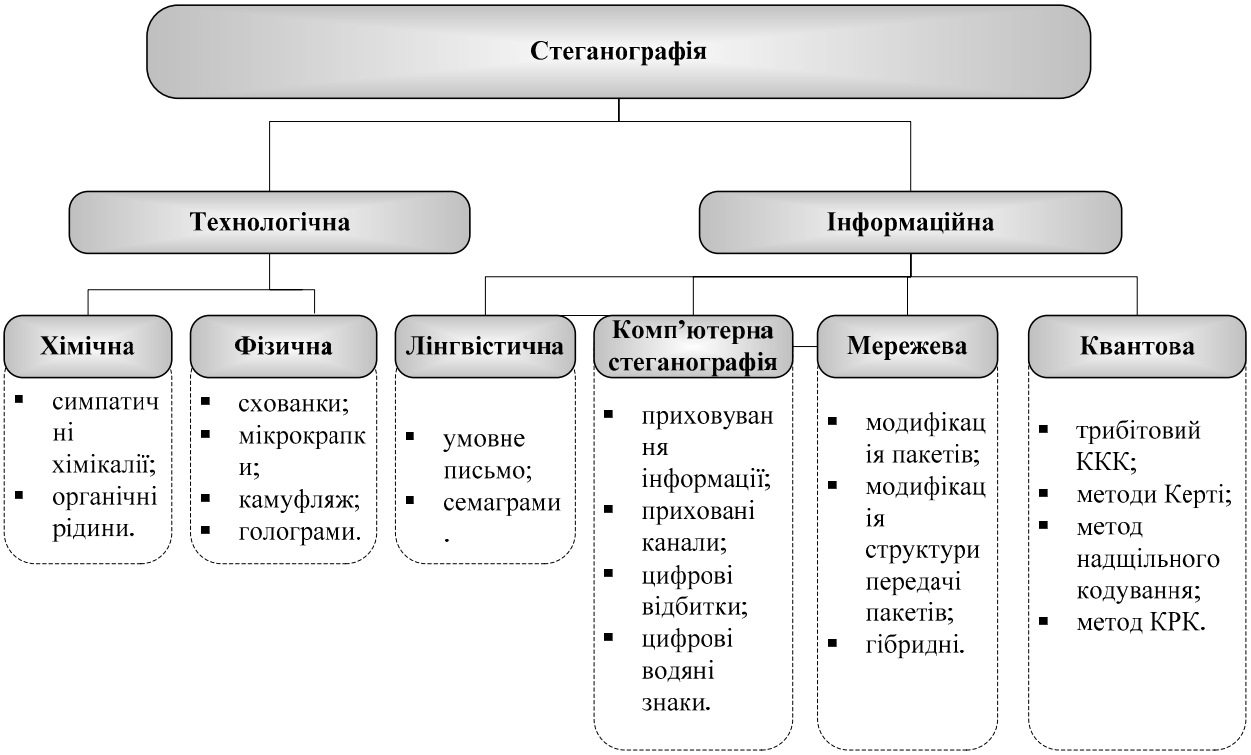

Рис. 1. Класифікація стеганографії. Поділ на технологічну та інформаційну

Щодня передача інформації відкритими каналами зв'язку відкриває безліч можливостей для прихованої комунікації. Секретні повідомлення можуть бути вбудовані не тільки в звичайних відкритих повідомленнях, як у традиційній стеганографії, а також в елементи управління протоколами зв'язку і в результатах зміни логіки протоколу.

Аналізуючи літературу [2], можна впевно виділити ще один окремий напрям стеганографії — мережеву стеганографію, де як носії секретних даних використовують мережеві протоколи еталонної моделі OSI.

До методів *технологічної стеганографії*, а саме класичної, відносять методи, які засновані на використанні хімічних або фізичних властивостей різних матеріальних носіїв інформації.

Хімічні методи стеганографії зводяться практично до застосування органічних рідин і симпатичних хімікаліїв.

До *фізичних методів* відносять мікрокрапки, голограми, різного виду сховища і методи камуфляжу.

До *інформаційної стеганографії* відносять методи лінгвістичної, комп'ютерної, мережевої та квантової стеганографії.

Лінгвістичні методи стеганографії поділяють на дві основні категорії:

- умовні листи;
- семаграми.

Існують три види умовного листа: жаргонний код, порожній шифр і геометрична система.

У жаргонному коді зовні безневинне слово має зовсім інше реальне значення, а текст складається так, щоб він виглядав якомога більш невинно і правдоподібно. При застосуванні порожнього шифру в тексті мають значення лише деякі певні букви або слова. Порожні шифри зазвичай виглядають ще більш штучно, ніж жаргонний код. Третім видом умовного листа є геометрична форма. При її застосуванні мають значення слова, що розташовуються на сторінці в певних місцях або в точках перетину геометричної фігури заданого розміру.

Другу категорію лінгвістичних методів становлять семаграми — таємні повідомлення, в яких шифропозначеннями є будь-які символи, крім літер і цифр. Ці повідомлення можуть бути передані, наприклад, у малюнку, що містить крапки і тире для читання за кодом Морзе.

У загальному випадку *мережева стеганографія* є підвидом цифрової стеганографії, але останнім часом набули популярності методи, коли прихована інформація передається через комп'ютерні мережі з використанням особливостей роботи протоколів передачі даних. Такі методи отримали назву «мережева стеганографія». Типові методи мережевої стеганографії містять зміни властивостей одного з мережевих протоколів. Крім того, може використовуватися взаємозв'язок між двома або більше різними протоколами з метою більш надійного приховання передачі секретного повідомлення. Мережева стеганографія уже охоплює широкий спектр методів,

тому її виділимо, як окремий незалежний напрям стеганографії.

Мережева стеганографія — вид стеганографії, де як носії секретних даних використовують мережеві протоколи еталонної моделі OSI.

Передачу прихованих даних у мережевій стеганографії здійснюють через приховані канали. Прихований канал може існувати в будь-якому відкритому каналі, у якому існує деяка надмірність.

Приховані дані називаються *стеганограмою*. Вони розташовуються в певному носії (*carrier*). У мережевій стеганографії роль носія виконує переданий по мережі пакет.

Основні параметри мережевої стеганографії — це пропускова здатність прихованого каналу, імовірність виявлення і стеганографічна вартість. Пропускова здатність — обсяг секретних даних, який може бути відправлений за одиницю часу. Імовірність виявлення визначається за можливістю виявлення стеганограми в певному носії. Найбільш популярний спосіб виявити стеганограму — це аналіз статистичних властивостей отриманих даних і порівняння їх з типовими значеннями для цього носія. Стеганографічна вартість характеризує ступінь модифікації носія після впливу на нього стеганографічного методу.

Методи мережевої стеганографії можна поділити на три групи:

1. Методи, сутність яких полягає в зміні даних у полях заголовків мережевих протоколах і в полях корисного навантаження пакетів;

2. Методи, у яких змінюється структура передачі пакетів, наприклад, змінюються послідовності передачі пакетів або навмисне введення втрат пакетів при їх передачі;

3. Змішані (гібридні) методи, при застосуванні яких змінюється вміст пакетів, терміни доставки пакетів і порядок їх передачі.

Кожен з цих методів поділяється ще на кілька груп. Методи модифікації пакетів містять три різних методи:

1. Методи зміни даних у полях заголовків протоколу: вони засновані на модифікації полів заголовків IP, TCP, SCTP і так далі;

2. Методи модифікації корисного навантаження пакета; в цьому випадку застосовуються алгоритми водяних знаків, мовних кодеків і інших стеганографічних технік з приховування даних;

3. Методи змішаних технік.

Методи модифікації структури передачі пакетів містять:

1. Методи, у яких змінюється порядок послідовності пакетів;

2. Методи, що змінюють затримку між пакетами;

3. Методи, сутність яких полягає у введенні навмисної втрати пакетів шляхом пропуску порядкових номерів у відправника.

Змішані (гібридні) методи стеганографії використовують два підходи:

1. Методи втрати аудіопакетів (LACK)

2. Ретрансляція пакетів (RSTEG).

Квантова стеганографія [4] аналогічно традиційним методам має за мету підвищення рівня секретності шляхом приховування самого факту передачі інформації. Подібно до класичної цифрової стеганографії, у квантовій інформації приховується через вкладення повідомлення у надлишкову частину середовища покриття (контейнер). Квантова стеганографія ще не вийшла на рівень практичної реалізації, але досить часто пропонуються теоретичні моделі стегосистем, що використовують властивості квантових станів. Даний напрям є синтезом класичної та квантової інформатики та ґрунтується на спільному використанні законів квантової фізики та класичної теорії інформації.

На даний час запропоновано три основних методи квантової стеганографії:

1. Приховування у квантовому шумі;

2. Приховування із застосуванням квантових завадостійких кодів;

3. Приховування у форматах даних, протоколах.

У межах комп'ютерної стеганографії розглядаються також питання, пов'язані з приховуванням інформації, яка зберігається на носіях або передається по мережах телекомунікацій, з організацією прихованих каналів у комп'ютерних системах і мережах з технологіями цифрових водяних знаків і відбитків пальців.

Існують певні відмінності між технологіями цифрових водяних знаків і відбитками пальців, з одного боку, і власне стеганографічна технологія приховування секретної інформації для її подальшого передавання або зберігання. Найголовніша відмінність — це те, що цифрові водяні знаки і відбитки пальців мають на меті захист самого цифрового об'єкта (програми, зображення, музичного файлу), куди вони впроваджуються, і забезпечують доказ прав власності на даний об'єкт.

Оскільки найбільший інтерес на даному етапі розвитку інформаційних технологій становить комп'ютерна стеганографія, тому більшість авторів класифікують лише методи, які можна реалізувати за допомогою комп'ютерних технологій.

У науковій праці, розглядають два основні напрями розвитку методів комп'ютерної стеганографії:

- використання спеціальних властивостей комп'ютерних форматів;
- надлишковість аудіо- та візуальної інформації.

Спеціальні властивості форматів обирають з урахуванням захисту приховуваного повідомлення від безпосереднього прослуховування, перегляду або зчитування. Проте більш широко використовують методи засновані на використанні надлишкової інформації аудіо та візуальної інформації. Цифрові фотографії, цифрова музика, цифрове відео являють собою матрицю чисел, які кодують інтенсивність у дискретні моменти в просторі і/або в часі. Цифрова фотографія — це матриця чисел, що являють собою інтенсивність світла в певний момент часу. Цифровий звук — це матриця чисел, що являє собою інтенсивність звукового сигналу в послідовно слідкуючі моменти часу. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку і візуального образу. Їх заповнення відчутно не впливає на якість сприйняття, що й дає можливість для приховування додаткової інформації.

Графічні кольорові файли зі схемою змішування RGB кодують кожну точку зображення трьома байтами. Кожна така точка складається з адитивних складових: червоного, зеленого та синього. Зміна кожного з трьох найменш значущих біт призводить до зміни менше 1 % інтенсивності даної точки. Це дозволяє приховувати в стандартній графічній картинці об'ємом 800 Кбайт близько 100 Кбайт інформації, що не помітне при перегляді зображення.

Такий підхід є досить простим і зрозумілим, проте він упускає багато важливих моментів при виборі необхідного способу приховування даних.

Такі недоліки були частково враховано в праці [5; 6], де методи комп'ютерної стеганографії поділено за певними критеріями.

- За способом обрання контейнера:
  - сурогатні (ерзацметоди);
  - селективні (методи відбраковування);
  - конструюючі (методи імітації).
- За способом доступу до інформації:
  - потокові;
  - фіксовані.
- За способом організації контейнера:
  - систематичні;
  - несистематичні.
- За способом видобування повідомлення:
  - з оригіналу;
  - без оригіналу контейнера;
  - за фрагментом оригіналу контейнера.
- За принципом приховування:
  - безпосередньої заміни;
  - спектральні.
- За форматом контейнера:
  - текстові;
  - аудіо;
  - графічні;
  - відео.
- За призначенням:
  - захист конфіденційних даних;
  - захист авторських прав;
  - автентифікація даних.

Аналізуючи існуючі на даному етапі способи класифікації стеганографічних методів слід зазначити, що всі вони лише частково відображають ту ситуацію, яка склалася з стрімким розвитком стеганографії як науки. Немає повного відображення всіх особливостей, які необхідно враховувати для ефективного використання прихованої передачі повідомлень, з дотриманням основних положень сучасної стеганографії [8]:

1. Методи приховування повинні забезпечувати автентичність і цілісність файлу.

2. Передбачається, що порушнику повністю відомі можливі стеганографічні методи.

3. Безпека методів ґрунтується на збереженні стеганографічним перетворенням основних властивостей відкритого файлу.

4. Навіть якщо факт приховування повідомлення став відомий зловмиснику, то виокремлення самого секретного повідомлення є складною обчислювальною задачею.

Систематизація та класифікація стеганографічних методів

Основним визначальним моментом у стеганографії є стеганографічне перетворення. До недавнього часу стеганографія, як наука, переважно вивчала окремі методи приховування інформації і способи їх технічної реалізації. Різноманітність принципів, закладених у стеганографічних методах, по суті гальмувала розвиток стеганографії як окремої наукової дисципліни і не дозволила їй сформуватися у вигляді сучасної науки зі своїми теоретичними положеннями і єдиною концептуальною системою, яка забезпечила б формальне отримання якісних і кількісних оцінок стеганометодів.

Сучасний інтерес до стеганографії, як сукупності методів приховування інформації, виник завдяки інтенсивному впровадженню і широкому розповсюдженню засобів обчислювальної техніки в усі сфери діяльності людини. У межах обчислювальних мереж виникли досить широкі можливості з оперативного обміну різною ін-

формацією у вигляді текстів, програм, звука, зображень між будь-якими учасниками мережевих сеансів незалежно від їх територіального розміщення. Це дозволяє активно застосовувати всі переваги, які дають стеганографічні методи захисту.

Стеганографія знаходить все більше застосування в оборонній та комерційній сферах діяльності через легку адаптованість при вирішенні завдань захисту інформації, а також відсутності явно виражених ознак засобів захисту, використання яких може бути обмежено або заборонено (як, наприклад, криптографічних засобів захисту).

Проаналізувавши існуючі на даному етапі методи прихованої передачі інформації можна запропонувати новий підхід для класифікації методів комп'ютерної стеганографії. Доповнивши та скомпонувавши всі методи розглянуті вище, можна згрупувати їх за ознаками: вибір контейнера, призначення, наявність ключа, а також спосіб приховування даних (рис. 2).

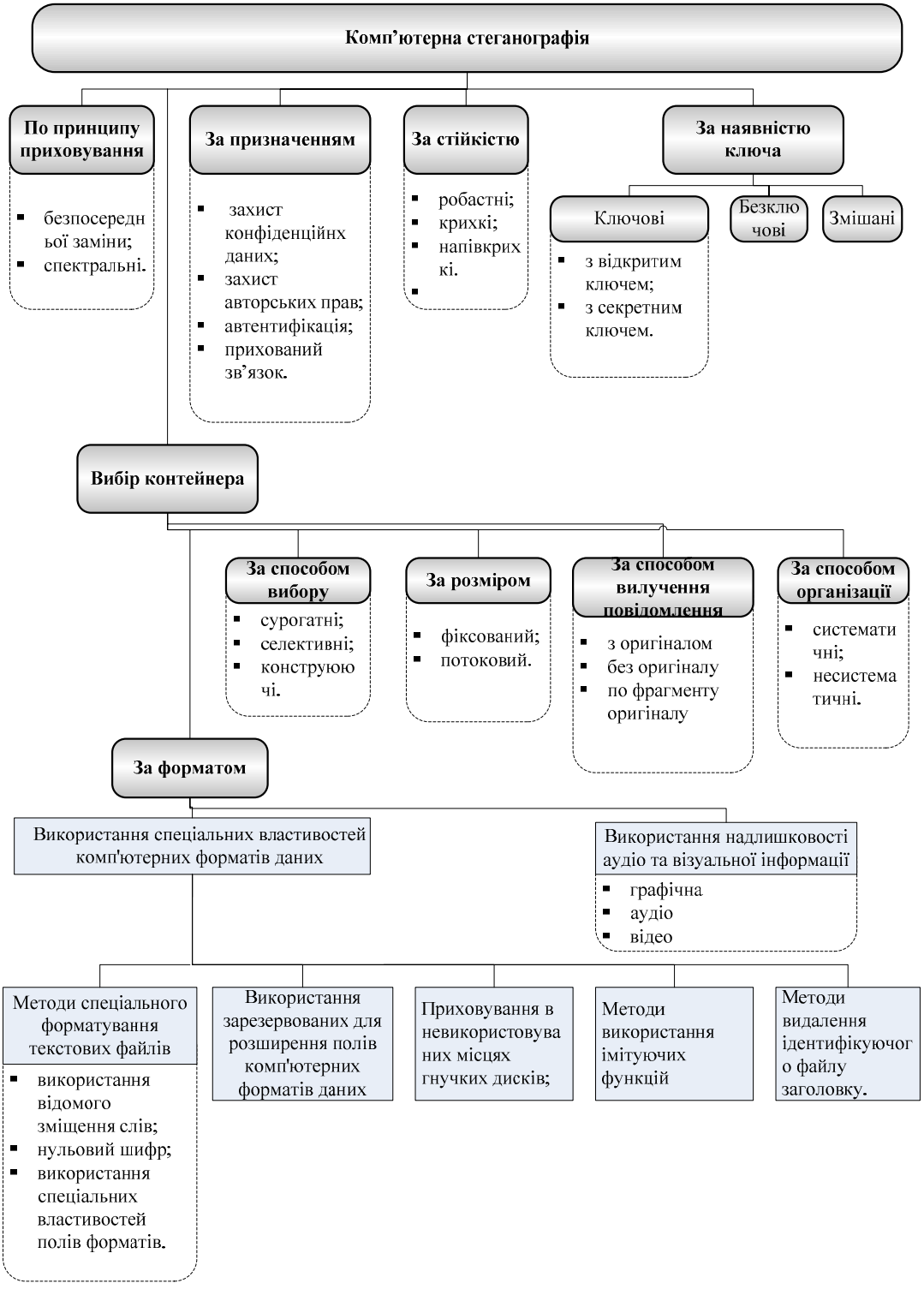

Рис. 2. Новий спосіб класифікації стеганографічних методів

Проведемо детальніше огляд кожної ознаки.

Вибір контейнера можна поділити за п'ятьма напрямами.

1) Вибір контейнера за форматом:

Методи використання спеціальних властивостей комп'ютерних форматів даних:

- використання зарезервованих для розширення полів комп'ютерних форматів даних. Поля розширення є в багатьох мультимедійних форматах, вони заповнюються нульовою інформацією і не враховуються програмою.

Методи спеціального форматування текстових файлів:

(1) Методи використання відомого зміщення слів, речень, абзаців. Методи засновані на зміні положення рядків і розстановки слів у реченні, що забезпечується вставкою додаткових пробілів між словами.

(2) Методи вибору певних позицій букв (нульовий шифр). Акровірш — окремий випадок цього методу (наприклад, початкові літери кожного рядка утворюють повідомлення).

(3) Методи використання спеціальних властивостей полів форматів, які не відображаються на екрані. Методи засновані на використанні спеціальних «невидимих», прихованих полів для організації виносок і посилань (наприклад, використання чорного шрифту на чорному тлі).

Методи приховування в невикористовуваних місцях гнучких дисків. Інформація записується в зазвичай невикористовуваних місцях ГМД (наприклад, у нульовій доріжці).

Методи використання імітуючих функцій. Метод заснований на генерації текстів і є узагальненням акровірша. Для таємного повідомлення генерується осмислений текст, що приховує саме повідомлення.

Методи видалення ідентифікуючого заголовка. Приховуване повідомлення шифрується і у результаті видаляється ідентифікуючий заголовок, залишаючи тільки шифровані дані. Одержувач заздалегідь знає про передачу повідомлення і знає про заголовок файлу.

Використання надлишковості аудіо та візуальної інформації.

Молодші розряди цифрових бітів містять дуже мало корисної інформації. Їх заповнення додатковою інформацією практично не впливає на якість сприйняття, що і дає можливість приховування конфіденційної інформації.

*2. Вибір контейнера за способом вилучення інформації***:**

а) з оригіналом;

б) без оригіналу;

в) по фрагменту оригіналу.

3. Вибір контейнера за розміром:

а) потокові — до них відносять контейнери, розмір яких наперед невідомий і може змінюватись під час приховування інформації.

б) фіксовані — до них належать контейнери розмір яких наперед відомий і незмінний.

Оскільки контейнер відомий заздалегідь, є час оцінити його ефективність стосовно до обраного алгоритму приховування інформації. З іншого боку, контейнери фіксованої довжини мають обмежений обсяг і іноді вбудоване повідомлення може не поміститися у файл-контейнер.

Інший недолік полягає в тому, що відстані між прихованими бітами рівномірно розподілені між найбільш коротким і найдовшим заданими відстанями, в той час як справжній випадковий шум буде мати експоненційний розподіл довжин інтервалу. Звичайно, можна згенерувати псевдовипадкові експоненціально розподілені числа, але цей шлях зазвичай занадто трудомісткий.

Однак на практиці частіше за все використовуються саме контейнери фіксованої довжини, як найбільш поширені і доступні.

4. За способом вибору контейнера:

а) у сурогатних методах стеганографії повністю відсутня можливість вибору контейнера і для приховування повідомлення обирають будь-який контейнер;

б) у селективних методах комп'ютерної стеганографії заздалегідь визначається, що приховане повідомлення має відображати певні спеціальні статистичні характеристики шуму контейнера. У такому випадку створюють ряд альтернативних контейнерів з подальшим вибором найбільш підходящого для заданого повідомлення;

в) у конструюючих методах стеганографії контейнер створює сама стеганосистема.

5. За способом організації контейнери можуть бути:

а) систематичними, у яких можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти контейнера, а де шумові біти, призначені для приховування інформації.

б) несистематичні, у яких все навпаки.

За наявністю ключа стеганосистеми поділяють на:

1. ключові;
2. безключові;
3. змішані.

Для функціонування безключових стеганосистем, крім алгоритму стеганографічного перетворення, немає необхідності в додаткових даних, а саме стеганоключа.

Ключові стеганосистеми поділяють на системи з секретним та відкритим ключами. Для систем з наявністю секретного ключа має використовуватись захищений канал передачі інформа-

ції. Стеганографічні системи з відкритим ключем не потребують використання захищеного каналу для передачі ключів. У разі використання стеганосистем з відкритим ключем необхідно мати два стеганоключа: один секретний, а інший — відкритий, його можна зберігати у відомому для всіх місці.

На практиці перевага надається безключовим стеганосистемам, хоча останні можуть бути розкриті в тому випадку, якщо порушник дізнається про метод стеганоперетворення, який при цьому був використаний. У зв'язку з цим у безключових системах часто використовують особливості криптографічних систем з відкритим і/або секретним ключем.

За призначенням стеганографічні методи можна розділити на такі області використання:

1. Захист від копіювання (електронна комерція, контроль за тиражуванням (DVD), розповсюдження мультимедійної інформації);
2. Прихована анотація документів (медичні знімки, картографія, мультимедійні бази даних);
3. Аутентифікація (системи відеоспостереження, електронної комерції, голосової пошти, електронне конфіденційне діловиробництво);
4. Прихований зв'язок (використання в воєнних розвідувальних цілях, а також у тих випадках, коли використовувати криптографію заборонено).

Використання стеганографічних систем є найбільш ефективною при вирішенні проблеми захисту інформації з обмеженим доступом. Так, наприклад, тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 біт у стереорежимі дозволяє приховати за рахунок заміни молодших розрядів на приховуване повідомлення близько 10 Кбайт інформації. При цьому зміна значень відліків становить менше 1 %. Така зміна практично не виявляється при прослуховування файлу більшістю людей.

Крім прихованої передачі повідомлень, стеганографія є одним з найбільш перспективних напрямів для аутентифікації й маркування авторської продукції з метою захисту авторських прав на цифрові об'єкти від піратського копіювання. На комп'ютерні графічні зображення, аудіопродукцію, літературні твори (програми в тому числі) наносять спеціальну позначку, яка залишається невидимою для очей, але розпізнається спеціальним програмним забезпеченням. Мітка містить приховану інформацію, що підтверджує авторство. Прихована інформація покликана забезпечити захист інтелектуальної власності. Як приховану інформацію можна використовувати дані про автора, дату і місце народження твору, номери документів, що підтверджують авторство, дату пріоритету і т. ін. Такі спеціальні відомості можуть розглядатися як доказ при розгляді суперечок про авторство або для доказу нелегального копіювання.

Як і будь-які інші інструменти, стеганографічні методи потребують до себе бережного ставлення, оскільки вони можуть бути використані і з метою захисту, і в протиправних цілях.

Наприклад, наприкінці 2001 року під пильною увагою преси виявилися відомості про те, що один з найнебезпечніших терористів світу Осам Бен Ладен і члени його угруповання широко використовують Інтернет для передачі повідомлень по організації терористичних акцій. Уряди деяких країн роблять кроки з метою приборкання такої загрози, намагаючись ввести обмеження на поширення програм, пов'язаних з криптографічними і стеганографічними методами. Однак стеганографічні методи успішно застосовуються для протидії системам моніторингу та управління мережевими ресурсами промислового шпигунства. За їх допомогою можна протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери управління локальних або глобальних обчислювальних мереж.

Нерідко методи стеганографії використовують для камуфляжу програмного забезпечення. У тих випадках, коли використання програм незареєстрованими користувачами є небажаним, воно може бути закамуфльоване під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховане у файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор). І, нарешті, стеганографічний підхід використовують при створенні прихованого каналу витоку чутливої інформації від санкціонованих користувачів.

За принципом приховування методи комп'ютерної стеганографії поділяють на два основні класи:

1. Безпосередньої заміни.
2. Спектральні методи.

Якщо перша, використовуючи надлишок інформаційного середовища в просторовій або часовій області, полягає в заміні малозначущої частини контейнера бітами секретного повідомлення, то інші для приховування даних використовують спектральне представлення елемен-тів середовища, у яке вбудовують приховувані дані.

9. За стійкістю стеганосистеми можна виділити:

1. Робастні.
2. Крихкі.
3. Напівкрихкі.

Пояснити таку класифікацію можна за допомогою цифрових водяних знаків.

Під робастністю розуміють стійкість ЦВЗ до різного роду впливів на стегосистему. Робастності ЦВЗ присвячено більшість досліджень.

Крихкі ЦВЗ руйнуються за незначної модифікації заповненого контейнера. Їх використовують для підтвердження сигналів. Відмінність від засобів електронного цифрового підпису полягає в тому, що крихкі ЦВЗ все ж допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, так як законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність полягає в тому, що крихкі ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але також вид і місце розташування цієї зміни.

Напівкрихкі ЦВЗ стійкі відносно до одних дій і нестійкі відносно до інших. Майже всі ЦВЗ можуть бути віднесені до цього типу. Однак напівкрихкі ЦВЗ спеціально проектують так, щоб бути нестійкими щодо певного роду операцій.

Така класифікація найбільш широко відображає систему методів прихованої передачі інформації. Можливо хтось заперечить такий підхід і висловить своє заперечення такому підходу, адже в наведеній класифікації пропонується також класифікація стеганографічних систем, що є дещо суперечливим фактом. Проте це використано з такого погляду, що будь-який стеганографічний метод напрямлений на створення системи прихованої передачі інформації. Тому буде неправильно розглядати початковий етап — вибір контейнера під час класифікації даних методів, а водночас не надавати значення уже готовому продукту — стеганографічній системі. Цей спосіб класифікації не вказує на самі методи, тут немає жодної конкретної назви того чи іншого методу, проте тут відображені всі основні властивості, які необхідно враховувати при вирішенні того чи іншого завдання. З подальшим розвитком комп'ютерних технологій дану структуру можна доповнювати та поширювати відповідно до вимог, які необхідно забезпечити.

Висновки

У результаті аналізу наявних способів класифікації та систематизації стеганографічних методів, було створено оптимальну систему класифікації цих методів.

Необхідно враховувати, що створення стегосистеми потребує певного співвідношення між стійкістю вбудованого повідомлення до зовнішніх впливів (у тому числі і стегоаналізу) і розміром самого вбудованого повідомлення.

Для більшості сучасних методів, використовуваних для приховання повідомлення в цифрових контейнерах, має місце експоненційна залежність надійності системи від обсягу вбудовуваних даних. Дана залежність показує, що при збільшенні обсягу вбудовуваних даних знижується надійність системи (при незмінності розміру контейнера). Таким чином, використовуваний в стегосистеми контейнер накладає обмеження на розмір вбудовуваних даних.

Отже, на сьогодні розвиток стеганографічних методів захисту інформації набуває все більших обертів, створюється теоретичні основи, а також більш стійкі методи приховування повідомлень до різних впливів на стеганоконтейнер.

ЛІТЕРАТУРА

1. *Тарасов Д. О.* Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д. О. Тарасов, А. С. Мельник, М. М. Голобородько // Інформаційні системи та мережі. Вісник НУ «Львівська політехніка». — 2010. — № 673. — С. 365–374.

2. *Стасюк О. І.* та ін. Сучасні стеганографічні методи захисту інформації / О. І. Стасюк та ін. // Захист інформації. — 2011. — Т. 13. — № 1 (50).

3. *Пескова О. Ю.* Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет / О. Ю. Пескова, Г. Ю. Халабурда // Материалы научной конференции» Интернет и современное общество». — 2012. — С. 348–354.

4. *Конахович Г. Ф.* Сучасні методи квантової стеганографії / Г. Ф. Конахович // Захист інформації. — 2011. — Т. 13. — № 2 (51).

5. *Конахович Г. Ф.* Комп'ютерна стеганографія / Г. Ф. Конахович, О. Ю. Пузиренко //Теорія і практика. — К. : МК-Пресс. — 2006.

6. *Юдін О. К.* Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О. К. Юдін, Р. В. Зюбіна, О. В. Фролов // Радиоэлектроника и информатика. — Х. : НХНУРЕ, 2015. — № 3. — С. 24–31.

Стаття надійшла до редакції 30.05.2016