Pedram // 31st International Conference on Distributed Computing Systems Workshops. Minneapolis, USA, 2011. P. 1-6.

Надійшла до редколегії 14.09.2015

Рецензент: д-р техн. наук, проф. Безрук В.М.

Скулиш Марія Анатоліївна, канд. техн. наук, доцент Національного технічного університету України "Київський політехнічний інститут". Наукові інтереси: біллінг, датацентри, хмарні обчислення, розподілені системи, SDN. Адреса: Україна, 01033, Київ, пров. Індуструальний, 2, тел. +38(044)4068299.

Суліма Світлана Валеріївна, аспірантка Національного технічного університету України "Київський політехнічний інститут". Наукові інтереси: мобільні мережі, NFV. пров. Адреса: Україна, 01033, Київ, пров. Індуструальний, 2, тел. 0666245361.

Skulysh Mariia Anatoliivna, PhD., associate professor, associate professor at National technical university of Ukraine "Kiev Polytechnic Institute". Billing, data centers, cloud computing, distributed systems, SDN. Address: Ukraine, Kyiv, pr. Industrialnyy, 2, mob. +38(044)4068299.

Sulima Svitlana Valeriivna, Ph.D. student at National technical university of Ukraine "Kiev Polytechnic Institute". Mobile networks, NFV. Address: Ukraine, Kyiv, pr. Industrialnyy, 2, mob. 0666245361.

УДК 004.056.5:004.7

АНАЛІЗ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ У КОНТЕЙНЕРИ РІЗНИХ ФОРМАТІВ

ЮДІН О.К., ЗЮБІНА Р.В., ФРОЛОВ О.В.

Аналізуються існуючі стеганографічні методи. Визначаються основні поняття цифрової та комп'ютерної стеганографії. Доводиться, що цифрова стеганографія використовує методи приховування контейнера у дані, які мають аналогову природу. Показується, що комп'ютерна стеганографія вивчає способи приховування інформації за рахунок певних властивостей файлових систем, файлів різних форматів, виконуваних файлів. Пропонується структурна схема та математична модель типової стеганосистеми. Аналізується питання стійкості стеганосистем залежно від розміру та класу обраного контейнера. Визначаються показники оцінки якості стеганосистем та вводиться детальна класифікація стеганографічних методів за форматом контейнера.

Ключові слова: стеганографія, стеганоаналіз, контейнер, відеодані, аудіодані, цифрова стеганосистема.

1. Вступ

Питання збереження конфіденційності інформаційних потоків під час їх передачі каналами зв'язку займає провідну позицію у процесі забезпечення інформаційної безпеки особистості, суспільства та держави. На даний час найбільш поширеними технологіями захисту інформації в процесі передачі даних по відкритих каналах зв'язку є процедури поєднання криптографічних та стеганографічних методів (комбіновані). В процесі розвитку інформаційних систем стеганографія вийшла на принципово новий рівень, названий комп'ютерною стеганографією (КС).

Метою роботи є аналіз та класифікація існуючих методів стеганографічного захисту інформації залежно від класу та типу контейнерів.

2. Основні поняття комп'ютерної стеганографії

Основні поняття комп'ютерної стеганографії були визначені у 1996 р. на 1-й міжнародній конференції по приховуванню даних (Information Workshop on Information Hiding '96).

У понятті комп'ютерної стеганографії виділяють більш вузьке поняття – цифрової стеганографії (ЦС). В той час як цифрова стеганографія має на увазі приховування одних даних у інші, такі що мають аналогову природу (медіа, аудіофайлах тощо), то КС вивчає способи приховування інформації за рахунок певних властивостей файлових систем, файлів різних форматів, виконуваних файлів. Набір методів та засобів, що використовуються для створення непомітного (прихованого) каналу передачі даних, називається стеганографічною системою, або стеганосистемою [1]. При побудові стеганосистеми мають враховуватися такі положення:

– стеганосистема повинна мати прийнятну складність обчислення реалізації (тобто прийнятну кількість арифметико-логічних дій для вбудовування повідомлення у стеганоконтейнер та відтворення даних із цього ж контейнера);

– при виявленні факту існування вбудованого повідомлення порушник не повинен мати можливості дістати це повідомлення або відтворити відкритий текст;

– методи приховування мають забезпечити цілісність вбудованого повідомлення для одержувача;

– повинна забезпечуватись необхідна пропускна здатність стеганоконтейнера та каналу зв'язку;

– при проектуванні системи слід використовувати модель потенційного порушника такого рівня, що може мати повне уявлення про існування і функціонування стеганосистеми, але йому не повинно бути відомо про місце знаходження, вид і розмір ключа, за допомогою якого можна визначити факт присутності повідомлення (відкритого тексту) та його зміст;

– порушник має бути позбавлений будь-яких (технічних та будь-яких інших) переваг.

Сьогодні стеганографічні системи активно використовуються для вирішення таких задач захисту інформаційних ресурсів:

– обхід засобів моніторингу;

– захист авторських прав на інтелектуальну власність (ЦВЗ);

– захист конфіденційної інформації від НСД;

– приховування певних програм (таких як віруси);

– викрадення інформації (створення невідомих для власника каналів витоку інформації) тощо.

3. Схема типової стеганосистеми

Основними поняттями у стеганографії є повідомлення та контейнер. Повідомлення $m \in M$ – певна закрита інформація, яку необхідно приховати. $M = \{m_1, m_2, ...m_n\}$ - множина всіх повідомлень, що формуються в стеганосистемі.

Контейнер $c \in C$ – множина відкритих даних, яка використовується для вбудовування закритої інформації; $C = \{c_1, c_2, ..., c_q\}$ – множина всіх контейнерів, причому $q >> n$.

Порожній контейнер – контейнер c, який не містить закритої інформації. Заповнений контейнер – такий контейнер, який містить приховану інформацію (C_m). Заповнений контейнер не повинен візуально відрізнятися від порожнього.

Контейнери бувають двох типів: потокові та фіксовані (рис.1). Потокові контейнери – це послідовність бітів, яка постійно змінюється. Повідомлення вбудовується у нього в реальному режимі часу, тому заздалегідь невідомо, чи вистачить розміру даного контейнера для передачі повідомлення повністю. Фіксовані ж контейнери мають фіксований розмір, тому є можливість обрати оптимальний контейнер для передачі повідомлення. Розмір контейнера повинен, принаймні, у декілька разів перевищувати розмір повідомлення, і, чим більше дане співвідношення, тим надійніше приховане повідомлення. Для підвищення рівня захищеності секретної інформації повідомлення можна попередньо зашифрувати стійким криптографічним алгоритмом. Також часто використовується завадостійке кодування.

4. Математична модель типової стеганосистеми

Процес звичайного стеганографічного перетворення описується такими залежностями:

$$E : C \times M \to S; \quad (1)$$

$$D : S \to M, \quad (2)$$

де $S = \{(c_1, m_1), (c_2, m_2), ..., (c_q, m_q)\} = \{s_1, s_2, ...s_q\}$ – множина заповнених контейнерів (стеганограм).

Залежність (1) описує процес приховування інформації, залежність (2) – витягування прихованої інформації. Однією із обов'язкових умов при цьому є відсутність «перетину», тобто якщо $m_a \neq m_b$ (причому $m_a, m_b \in M$, а $(c_a, m_a), (c_b, m_b) \in S$), то $E(c_a, m_a) \cap E(c_b, m_b) = \varnothing$.

В загальному випадку стеганосистему можна представити як сукупність $\sum(C, M, S, E, D)$ – контейнерів, повідомлень та перетворень, що їх зв'язують. Завжди контейнери с обираються таким чином, щоб заповнений контейнер майже не відрізнявся від порожнього контейнера. Стеганосистема може вважатися надійною, коли $sim[c, E(c, m)] = 1$ (де sim – функція подібності). Контейнер може обиратися двома способами: довільно (сурогатний метод) та підбором найбільш придатного у конкретному випадку контейнера, який зміниться найменше при перетворенні. В останньому випадку контейнер обирається виходячи із умови:

$$c = \max \text{sim}[x, E(x, m)]. \quad (3)$$

В будь-якому випадку пряме та зворотне перетворення (E та D) мають відповідати одне одному та підлягати умові, що незначне викривлення контейнера (на величину δ) не має призводити до викривлення прихованої інформації:

$$E(c, m) \approx E(c + \delta, m) \text{ або}$$

$$D[E(c, m)] \approx D[E(c + \delta, m)] = m. \quad (4)$$

5. Стійкість стеганографічних систем

Всі описані вище способи використання стеганографії для формування контейнерів мають у необхідних умо-

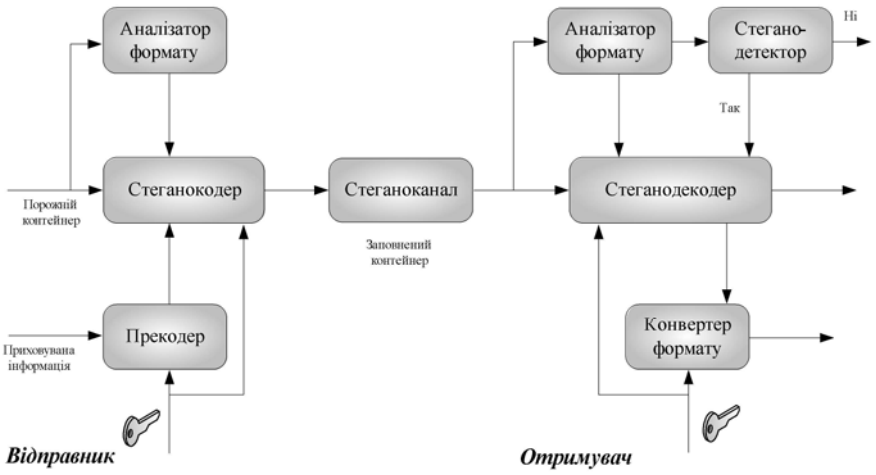

Рис. 1. Структурна схема типової стеганосистеми

вах певний розмір повідомлення та значення надійності його приховування. Оскільки при збільшенні об'єму повідомлення збільшуватиметься, розмір стеганоконтейнера, файл, який виконує роль контейнера, викликатиме певні підозри. Отже, існує залежність надійності приховування від об'єму повідомлення, яка продемонстрована на графіку (рис. 2).

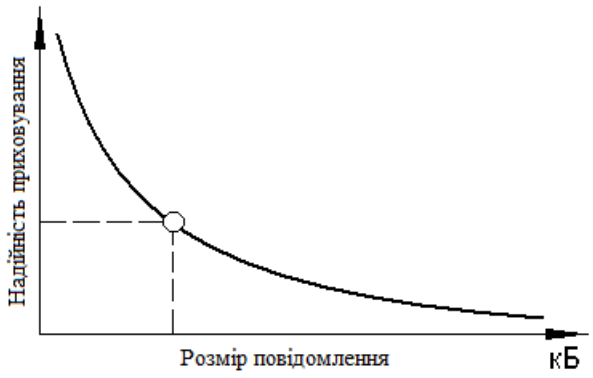

Рис. 2. Графік залежності надійності приховування даних від розміру повідомлення

Шляхом зміни певних якостей стеганоконтейнера можна досягти високої надійності приховування повідомлення або його великого обсягу, але ні в якому випадку не обох показників одночасно, тому що ріст одного із цих значень неминуче призводить до зменшення іншого. Таким чином, існує перспектива прийняття оптимального рішення при виборі між об'ємом даних та стійкістю системи до стеганоаналізу.

6. Стеганографічний аналіз

Основою стеганографічного аналізу є моделювання та дослідження стеганографічних систем для виявлення їх вразливих місць та визначення їх надійності. Термінологія стеганоаналізу майже ідентична термінології криптоаналізу, але є деякі відмінності. Криптоаналіз призначений для розшифровування криптограм, в той час як стеганоаналіз використовується для виявлення прихованої інформації і відтворення відкритого тексту.

За рівнем секретності стеганосистеми ділять на теоретично стійкі, практично стійкі та нестійкі.

Теоретично стійкі стеганосистеми проводять приховування інформації у тих частинах повідомлення, значення елементів яких не перевищує рівня шумів або певних помилок, і при цьому теоретично доведено, що неможливо створити стеганоаналітичний метод виявлення прихованої інформації.

Практично стійкі стеганосистеми виконують таку модифікацію фрагментів контейнера, що виявлення прихованої інформації можливе, але відомо, що у порушника подібні стеганоаналітичні методи відсутні.

Нестійкі стеганосистеми перетворюють контейнер таким чином, що існуючими стеганоаналітичними системами можна виявити секретну інформацію. В даному випадку стеганоаналіз дозволяє виявити слабкі місця такої системи для подальшої її модифікації до теоретично стійкої або, принаймні, до практично стійкої стеганосистеми.

7. Атаки на стеганографічну систему

Стеганографічна система вважається зламаною, якщо порушник зміг довести факт існування прихованого повідомлення у перехопленому контейнері. Передбачається, що порушник може використовувати будь-який вид атак та має необмежені обчислювальні можливості. По аналогії із криптоаналізом виділяють такі види атак на стеганосистеми:

– на основі відомого заповненого контейнера;

– на основі відомого вбудованого повідомлення;

– на основі обраного прихованого повідомлення;

– на основі обраного заповненого контейнера;

– на основі відомого порожнього контейнера (не має аналогу у криптоаналізі);

– на основі обраного порожнього контейнера (не має аналогу у криптоаналізі);

– на основі відомої математичної моделі контейнера або його частини (не має аналогу у криптоаналізі).

8. Оцінка якості стеганосистеми

Кількісна оцінка стійкості стеганографічної системи до зовнішніх впливів є доволі складною задачею, яка зазвичай реалізується методами системного аналізу, математичного моделювання або експериментального дослідження.

Надійна стеганосистема вирішує дві основні задачі:

– приховування самого факту існування повідомлення (перший рівень захисту);

– запобігання НСД до інформації шляхом вибору відповідного методу приховування інформації (другий рівень захисту).

Можливе існування третього рівня захисту – попередній криптографічний захист повідомлення (шифрування).

Модель аналізу загроз та оцінки стійкості стеганосистеми представлена на рис.3.

Оцінка рівня прихованості забезпечується шляхом проведення аналітичних досліджень та випробувань. Надійність стеганосистеми визначається, в основному, можливостями обчислювальної системи.

9. Стеганографічні методи приховування даних

Більшість методів КС базуються на двох принципах:

– файли, що не потребують абсолютної точності, можуть бути видозмінені (певною мірою) без втрати функціональності;

– органи відчуттів людини не здатні розрізнити зміни в модифікованих таким чином файлах та відсутній спеціальний інструментарій для цього.

Рис. 3. Модель аналізу загроз та оцінки стійкості стеганосистеми

Відповідно до існуючих методів комп'ютерної стеганографії, запропоновано класифікацію, зображену на рис. 4. За способом вибору контейнера вирізняють сурогатні, селективні та конструюючі методи. В сурогатних методах стеганографії можливість вибору контейнера відсутня, обирається перший наявний контейнер, який, у більшості випадків, не є оптимальним. Селективні методи дозволяють обирати оптимальний контейнер. Для цього генерують велику кількість альтернативних контейнерів, певна хеш-функція яких порівнюється із хеш-функцією повідомлення. В конструюючих методах контейнер генерується сам.

За способом доступу до інформації, що приховується, розрізняють методи для потокових та фіксованих контейнерів.

За способом організації контейнера бувають систематичні та несистематичні методи КС. У систематичних методах можна точно сказати, де в контейнері знаходяться інформаційні біти, а де – біти шуму. У несистематичних методах для виділення повідомлення доводиться обробляти всю стеганограму.

За принципом приховування даних є методи безпосередньої заміни та спектральні методи. Методи безпосередньої заміни використовують надлишок інформації у малозначних частинах контейнера для вбудовування повідомлення. Спектральні ж методи використовують спектральні представлення елементів контейнера для приховування повідомлення. В основному в стеганографії використовується саме надлишковість файлу-контейнера.

Варто також виділити методи, що використовують спеціальні властивості форматів файлів:

– зарезервовані поля форматів файлів, які зазвичай заповнюються нулями і не враховуються програмами;

– спеціальне форматування даних (зсув слів, речень, абзаців або шаблонний вибір символів);

– використання незадіяних частин оптичних та магнітних носіїв.

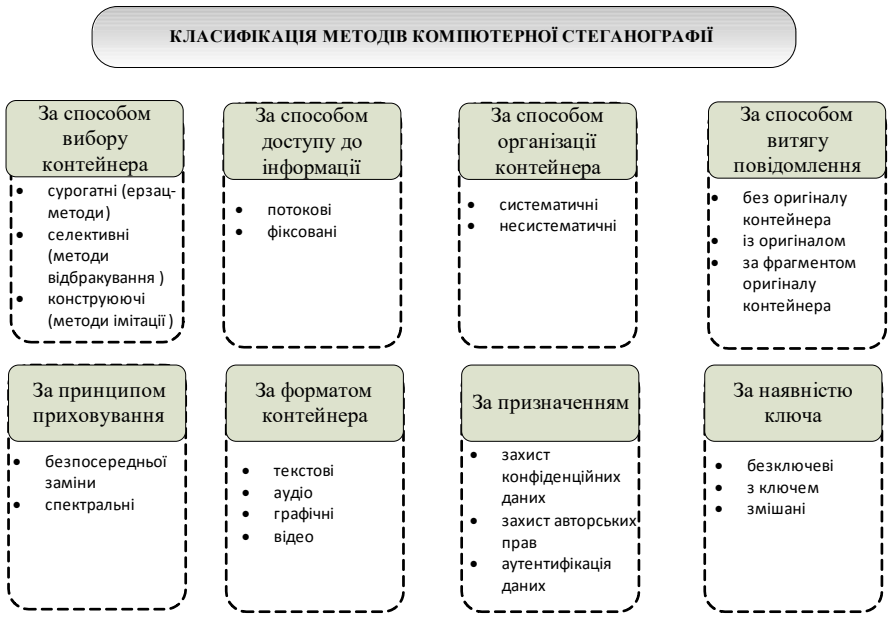

Рис. 4. Класифікація методів КС

Але для таких методів характерні низька пропускна здатність, низькі надійність та рівень прихованості.

За призначенням розрізняють методи для прихованої передачі даних (або прихованого зберігання) та методи для приховування даних цифрових об'єктів з метою захисту авторських прав на них.

За типами контейнера виділяють стеганографічні методи із текстовими, графічними, аудіо- та відеофайлами-контейнерами.

За наявністю ключа виділяють безключові, з ключем та змішані стеганосистеми.

Для функціонування безключової стеганосистеми, крім алгоритму графічного перетворення, відсутня необхідність в додаткових даних, на зразок стеганоключа.

Таким чином, безпека безключової стеганосистеми базується тільки на секретності використовуваних стеганографічних перетворень.

Ключова стеганосистема поділяється на системи з відкритим та закритим ключами. Система з відкритим ключем передбачає наявність закритого каналу зв'язку для передачі стеганоключа і забезпечує вищий рівень захисту повідомлення порівняно з безключовою, однак потребує затрат на передачу ключа. Стеганосистема з відкритим ключем працює по аналогії з криптографічними алгоритмами, однак потрібно зазначити, що стеганоключ не шифрує дані, а приховує місце їх вбудовування в контейнері.

Змішані стегосистеми використовують як відкритий, так і секретний ключ.

Провівши загальну класифікацію методів комп'ютерної стеганографії, детально розглянемо методи стеганографічного приховування інформації залежно від формату використовуваного контейнера.

10. Приховування даних у тексті

Для приховування інформації у тексті (лінгвістична стеганографія) використовується звичайна надлишковість письмової мови або формати представлення тексту.

Найскладнішим об'єктом для приховування є електронна версія тексту, тому що його друкована версія може бути зображенням в електронному вигляді, обробленим відповідними методами. Ця складність в основному обумовлена відносним дефіцитом у тексті надлишковості, на відміну від зображення або аудіофайлу. В той час як існує можливість внести невидимі для ока модифікації у зображення або не відчутні для слухової системи людини (ССЛ) зміни у звучанні аудіофайла, будь-яка зайва літера, зайвий символ або зайвий знак пунктуації може бути виявлений випадковим читачем.

Існують три основні методи приховування даних у тексті, що найширше розповсюджені:

– методи довільних інтервалів;

– синтаксичні методи;

– семантичні методи.

11. Методи довільного інтервалу

Дані методи виконують приховування даних за допомогою маніпулювання пропусками у тексті.

1) Метод зміни інтервалу між реченнями.

Повідомлення вбудовуються у двійковому форматі – після кожного символу завершення речення ставиться один або два пропуски, що відповідають бітам «1» та «0». Даний метод, хоч і дуже простий, але має багато недоліків:

– для приховування повідомлення невеликого об'єму потрібен контейнер значного розміру – при умові, що речення мають середньостатистичний вигляд (приблизно 2 рядки по 80 символів на кожен), 1 біт повідомлення приховується у 160 байтах текстового контейнера;

– можливість вбудовування повідомлення дуже залежить від структури текстового контейнера, наприклад, вірші, зазвичай, не мають однозначних знаків завершення повідомлення;

– існують текстові редактори, які самостійно вписують пропуск чи два після знаку закінчення речення (автозавершення);

– непослідовна поява пропусків у тексті може викликати підозри у читача.

2) Метод зміни кількості пропусків у кінці рядка.

Даний метод полягає у додаванні пропусків у кінці кожного рядка. Кількість пропусків залежить від значення біту, що вбудовується. Два пропуски кодують один біт на рядок, чотири пропуски – два біти на рядок, вісім пропусків – три біти на рядок і т.д. Такий підхід дозволяє значно збільшити кількість приховуваної інформації порівняно із попереднім методом. Додатковою перевагою даного методу є те, що його можна використати для будь-якого тексту, оскільки дані вільні місця будуть непомітними по відношенню до основного тексту. Недоліком даного методу (як і попереднього) є те, що деякі текстові редактори доставляють пропуски в кінці рядків. Також неможливе використання даного методу на папері у зв'язку із неможливістю розібрати кількість пропусків.

3) Метод зміни кількості пропусків між словами вирівняного по ширині тексту.

Даний метод додає пропуски між словами у тексті, який вирівняний по ширині. Один пропуск між словами інтерпретується як «0», два пропуски – як «1». В середньому даний метод дозволяє приховувати по декілька біт на рядок. Але враховуючи те, що не кожний пропуск між словами може використовуватись для вбудовування інформації, і для однозначного вирішення який пропуск є прихованою інформацією, а який є частиною оригінального тексту, використовують метод вбудовування, аналогічний манчестерсько-

му кодуванню, тобто комбінація бітів «01» вважається «1», а «10» - «0», пари ж «00» та «11» вважаються порожніми.

12. Синтаксичні та семантичні методи

До синтаксичних відносяться методи, які використовують для приховування інформації неоднозначності пунктуації у тексті, та методи зміни структури та стилю тексту. Наприклад, фрази «синій, зелений, червоний» та «синій, зелений та червоний» мають однаковий сенс, але зміна цих форм може бути поставлена у відповідність двійковому коду (форма із використанням сполучника «та» – «1», без сполучника «та» - «0»). Але даний метод необхідно використовувати з обережністю, бо в деяких випадках постійна зміна подібних форм може знизити сприймання даного тексту або отримання даним текстом діаметрально протилежного сенсу. Інколи краще використовувати методи, які змінюють стиль та структуру тексту. Наприклад, речення «Існує немало випадків, коли правила пунктуації є неоднозначними» можна сформулювати таким чином: «Правила пунктуації є неоднозначними у багатьох випадках». Такі методи є більш непомітними для читача, але можливість їх використання зникає у класичних текстах, в яких такі форми будуть незвичні для автора. Дані методи також дуже складні у автоматизації процесу вбудовування та витягу бітів повідомлення.

Семантичні методи подібні до синтаксичних, але замість вбудовування даних заміною двох неоднозначних граматичних форм вони використовують синоніми. Так, слово «але» може бути поставлене у відповідність «1», а слово «однак» – «0». Для цього необхідно мати таблицю синонімів. А враховуючи велику кількість синонімів до одного слова, існує можливість кодування одразу великої кількості біт.

13. Приховування даних у нерухомих зображеннях

В більшості випадків використовуються стеганографічні методи із графічними зображеннями в ролі контейнерів саме через такі причини:

– розповсюдження цифрових фотографій та відео, які необхідно захищати від протизаконного тиражування та розповсюдження;

– відносно великий об'єм графічних зображень, що дає широкий простір для приховування даних (великого розміру);

– розмір контейнера відомий заздалегідь, що дає змогу обирати оптимальний контейнер;

– відносно слабка чутливість людського ока до незначних змін у цифрових графічних зображеннях;

– добре розроблені, в останній час, методи цифрової обробки зображень.

14. Приховування даних у просторовій області

Загальний принцип таких алгоритмів полягає у заміні надлишкової, малозначної частини зображення бітами секретного повідомлення. Для витягу повідомлення необхідно знати алгоритм, по якому воно розміщувалося у зображенні.

1) Метод заміни найменш значущого біту.

Метод заміни найменш значущого біту (НЗБ, LSB – Less Significant Bit) - найбільш розповсюджений серед методів даного класу. НЗБ несуть у собі найменше інформації. Як відомо, людина, у більшості випадків, не може розрізнити інформацію у даних бітах. При цьому в чорно-білому зображенні (в якому кожен піксель кодується одним байтом) об'єм вбудованих даних може займати до 1/8 об'єму зображення-контейнера. Популярність даного методу обумовлена його простотою та можливістю приховувати доволі великі об'єми даних. В більшості випадків цей метод працює із растровими зображеннями, представленими у форматі без компресії даних (GIF, BMP).

Недоліком даного методу є його низька стійкість до викривлення контейнера внаслідок навіть незначних помилок у каналі передачі або активних і пасивних атак порушника. Для уникнення цієї проблеми використовують завадостійке кодування.

2) Метод псевдовипадкового інтервалу.

Даний підхід полягає у псевдовипадковому розподіленні бітів повідомлення по зображенню-контейнеру, внаслідок чого відстань між двома вбудованими бітами визначається псевдовипадково. Цей підхід ефективний у випадку, коли об'єм повідомлення набагато менший за контейнер. Недоліком такого методу є те, що біти повідомлення розподіляються по контейнеру у тому ж порядку, що і у самому повідомленні.

3) Метод псевдовипадкової перестановки.

Основою цього методу є генератор псевдовипадкових чисел (ПВЧ), який формує певну псевдовипадкову послідовність індексів $j_1, j_2, ... j_k$ і *k-ий* біт повідомлення зберігається у пікселі із індексом j_k.

Функція перестановки має бути псевдовипадковою і мати достатньо великий набір індексів, щоб жоден з них не повторився жодного разу і не відбулося «перетину».Цей метод забезпечує рівномірний розподіл інформаційних бітів по контейнеру. Імовірність перетину зменшується із зменшенням співвідношення (довжина повідомлення)/(довжина контейнера).

4) Метод блочного приховування.

При використанні даного методу зображення-контейнер розбивають на блоки, що не перетинаються між собою. Для кожного блоку визначають певний біт парності. В кожному блоці приховують один секретний біт. Якщо визначений біт парності не відповідає секретному біту, проводять інвертування НЗБ блоку, доки біт парності не буде, по суті, секретним бітом.

Цей метод, як і всі попередні, має низьку стійкість до викривлень, але він має свої переваги – існує можливість модифікувати такий піксель у блоку, щоб статистика контейнера була змінена якомога менше.

5) Метод заміни палітри.

Ще один метод приховування даних у зображенні – зміна палітри кольорів. Палітра кольорів зображення зберігається у вигляді списку пар індексів (i, A_i), який визначає відповідність між індексом і та його вектором кольору. Кожному пікселю зображення ставиться у відповідність певний індекс у таблиці. Оскільки порядок кольорів у палітрі не важливий для відновлення зображення, конфіденційна інформація може бути прихована шляхом перестановки кольорів у палітрі.

15. Приховування даних у частотній області зображення

Описані вище стеганографічні методи приховування даних у нерухомих зображеннях є нестійкими до більшості відомих видів спотворень. Наприклад, конвертування зображення у інший формат із компресією призводить до часткового або повного руйнування повідомлення. Більш стійкими до спотворень є методи, що використовують для приховування даних не просторову область контейнера, а частотну.

Найпоширеніші методи приховування даних у частотній області використовують вейвлет-перетворення та дискретно-косинусне перетворення (ДКП). Це пояснюється широким їх розповсюдженням у технологіях компресії цифрових зображень.

ДКП в цифровій обробці зображень використовується в такому вигляді:

$$\Omega(\upsilon,\nu) = \frac{\varsigma(\upsilon)\cdot\varsigma(\nu)}{\sqrt{2N}}\cdot\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(x,y)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right]; \quad (5)$$

де C(x,y) та S(x,y) - елементи оригінального та відновленого зображення розміром N*N; x,y – просторові координати пікселів зображення; $\Omega(\upsilon,\nu)$ – масив коефіцієнтів ДКП; υ,ν – координати у частотній області;

$\varsigma(\upsilon) = 1/\sqrt{2}$, якщо $\upsilon = 0$, та $\varsigma(\upsilon) = 1$, якщо $\upsilon > 0$.

1) Метод відносної заміни величин коефіцієнтів ДКП.

При використанні даного методу зображення розбивається на блоки 8x8 пікселів. До кожного з блоків застосовується ДКП, в результаті чого отримується матриця коефіцієнтів ДКП 8x8. Кожен блок призначений для приховування одного біту даних. Приховування проводиться заміною одного коефіцієнта у блоку.

2) Метод Бенгама-Мемона-Ео-Юнга.

Даний метод є модифікацією попереднього. Основною зміною є той факт, що при використанні даного методу секретна інформація приховується не в усіх блоках зображення, а тільки в обраних (найбільш підходящих).

3) Метод Фрідріх.

Згідно з цим методом, який по суті є комбінацією двох алгоритмів, секретні дані вбудовуються в низькочастотні та середньочастотні коефіцієнти ДКП. Каскадне використання цих двох алгоритмів може дати непогані результати відносно стійкості стеганографічної системи до різних атак.

4) Методи розширення спектра.

Система зв'язку є системою із розширеним спектром, коли:

– смуга частот, яка використовується при передачі, значно ширша за необхідну для передачі повідомлення, внаслідок чого співвідношення сигнал/шум є доволі низьким, і повідомлення важко знайти у каналі (особливо для органів чуття людини);

– розширення спектра відбувається за допомогою так званого розширюючого сигналу, який не залежить від інформації, що передається. Присутність енергії сигналу в усіх частотних діапазонах робить радіосигнал

$$\Omega(\upsilon,\nu) = \frac{\varsigma(\upsilon)\cdot\varsigma(\nu)}{\sqrt{2N}}\cdot\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(x,y)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right], \quad (6)$$

стійким до завад, а інформацію, що знаходиться у контейнері, стійкою до її видалення.

– Відновлення первинної інформації відбувається шляхом зіставлення отриманого сигналу та синхронізованої копії кодового(розширюючого) сигналу.

16. Приховування даних у аудіосигналах

Особливий розвиток отримали стеганографічні методи приховування інформації у аудіосередовищі. Це охарактеризовано тим, що ССЛ працює у надширокому динамічному діапазоні і має доволі малий різницевий діапазон. Виходячи із цього, можна зробити висновок, що у аудіофайлах присутній широкий простір для приховування даних. Також ССЛ не здатна розрізняти абсолютну фазу, вирізняє лише відносну. Крім того, існують деякі види спотворень, викликаних зовнішнім середовищем, які можна використати для приховування даних.

1) Кодування найменш значущих бітів (часова область).

Даний метод є найпростішим серед методів приховування даних у аудіосигналах. Його суть полягає у заміні НЗБ у кожній точці вибірки із сигналу, представленого у двійковій послідовності. Використання даного методу обумовлює високу пропускну здатність каналу, платою за що є добре чутний низькочастотний шум. Дану проблему можна вирішити використанням записів, на яких присутній певний шум, наприклад, звук стадіону, під час концерту. Але як і у аналогічних методах приховування інформації у нерухомих зображеннях, заповнені контейнери є вразливими до сторонніх впливів, окрім випадків, коли секретна інформація вбудована із внесенням надлишковості. Однак останнє при збільшенні стійкості каналу зменшує швидкість передачі даних.

2) Метод фазового кодування (частотна область).

Основною ідеєю методу фазового кодування є заміна фази вихідного звукового сегмента на деяку опорну фазу, характер зміни якої і відражає повідомлення, яке необхідно приховати. При правильному використанні даний метод є найефективнішим для приховування даних у аудіосигналах, оскільки доки модифікація фази достатньо мала, наявність повідомлення може бути абсолютно не відчутно на слух (не враховуючи використання спецтехніки).

3) Метод розширення спектра (часова область).

Даний метод майже ідентичний методу приховування даних у нерухомих зображеннях шляхом розширення спектра. Секретне повідомлення розподіляється по частотах несучого сигналу рівномірно, так щоб співвідношення сигнал(повідомлення)/шум у каналі було дуже низьким і не виникло підозр щодо наявності повідомлення. Сигнал-контейнер, в даному випадку, обирається набагато більший за секретне повідомлення.

4) Приховування даних із використанням ехо-сигналу.

Даний метод вбудовує повідомлення у аудіосигнал-контейнер шляхом введення у нього ехо-сигналу. Дані приховуються зміною параметрів ехо-сигналу: початкової амплітуди, швидкості затухання та зсуву. Коли зсув між оригінальним сигналом та ехо-сигналом зменшується, починаючи з певного значення, ССЛ стає нездатною виявити різницю між двома сигналами, а ехо-сигнал сприймається лише як додатковий резонанс. Цей метод непростий у реалізації, тому що значення зсуву дуже важко визначити. Воно значною мірою залежить від якості початкового сигналу і, само собою, від слухача [2].

17. Приховування даних у відеоданих

Стеганографічні методи приховування рідше за все використовуються у відеоданих, оскільки даний файл складається з динамічних зображень (фреймів) та звукової доріжки. Для цих цілей найчастіше використовуються контейнери у форматах MPEG – 2, MPEG – 4 та AVI. Варто також зазначити, що досі не використовуються як контейнери одночасно аудіодоріжки та фрейми. Загальна схема вбудовування повідомлення у відеодані зображена на рис. 5.

На сьогодні існує три методи для приховування інформації у відеоданих , а саме:

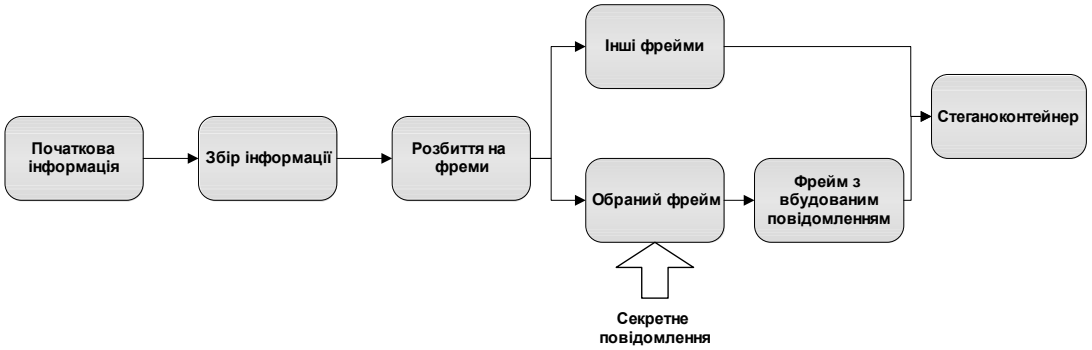

Рис. 5. Загальна схема вбудовування повідомлення у відеодані

Метод вбудовування на рівні коефіцієнтів – біти приховуваного повідомлення вбудовуються в коефіцієнти ДКП. Враховуючи, що використовуються алгоритми стиснення, основною проблемою стає накопичення зсуву та помилок. Для зменшення внесених змін використовують додатковий спеціальний сигнал. В зв'язку з обмеженням бітової швидкості при вбудовуванні змінюється лише 10-12% коефіцієнтів ДКП. При використанні даного методу приховувана інформація зберігається при фільтруванні, зашумленні (адитивним шумом) і дискретизації.

Метод вбудовування інформації на рівні бітової площини - відрізняється високою пропускною здатністю і легкими обчисленнями. Але є й істотний недолік: інформація, вбудована таким чином, може бути легко видалена. При повторному накладенні послідовності біт якість відео погіршиться, а приховувана інформація буде знищена.

Метод вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами - в основі лежить диференціальне вбудовування енергії. Цей метод може використовуватись для багатьох алгоритмів стиснення, не тільки для MPEG. Інформація вбудовується шляхом видалення декількох коефіцієнтів ДКП [3].

18. Висновки

Стеганографічні системи захисту інформаційних потоків під час їх зберігання та передачі займають провідні позиції у процесах забезпечення інформаційної безпеки.

Проведено аналіз існуючих стеганографічних методів. Визначено основні поняття цифрової та комп'ютерної стеганографії. Доведено, що цифрова стеганографія використовує методи приховування контейнера у дані, які мають аналогову природу. Показано, що комп'ютерна стеганографія вивчає способи приховування інформації за рахунок певних властивостей файлових систем, файлів різних форматів, виконуваних файлів. Представлено структурну схему та математичну модель типової стеганосистеми. Проаналізовано питання стійкості стеганосистем залежно від розміру та класу обраного контейнера. Визначено показники оцінки якості стеганосистем та введено детальну класифікацію стеганографічних методів за форматом контейнера.

Література: 1. *Юдін О.К., Конахович Г.Ф., Корченко О.Г.* Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. **2.** *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография //Теория и практика/Киев: МК-Пресс. 2006. **3.** *Моденова О. В.* Стеганография и стегоанализ в видеофайлах //Прикладная дискретная математика. Приложение. 2010. №. 3.

Надійшла до редколегії 10.09.2015

Юдін Олександр Костянтинович, доктор технічних наук, професор, директор інституту комп'ютерних інформаційних технологій Національного авіаційного університету. Наукові інтереси: комплексні системи захисту інформації. Захоплення та хобі: волейбол, морські прогулянки, серфінг. Адреса: Україна, Київ, пр. Космонавта Комарова, 1, тел. 097-707-77-37.

Зюбіна Руслана, викладач кафедри комплексних систем захисту інформації Національного авіаційного університету. Наукові інтереси: комплексні системи захисту інформації. Захоплення та хобі: волейбол, морські прогулянки, серфінг. Адреса: Україна, Київ, пр. Космонавта Комарова, 1, тел. 097-707-77-37.

Фролов Олег, здобувач кафедри комплексних систем захисту інформації Національного авіаційного університету. Наукові інтереси: комплексні системи захисту інформації. Захоплення та хобі: волейбол, морські прогулянки, серфінг. Адреса: Україна, Київ, пр. Космонавта Комарова, 1, тел. 097-707-77-37.

Yudin Alexander, Doctor of Technical Sciences, professor, Director of the Institute of Computer Information Technologies, The National Aviation University, Kyiv, Ukraine. Scientific interests: complex information security system. Interests and hobbies: volleyball, boating, surfing. Address: Kosmonavta Komarova ave.1, Kyiv, Ukraine, 097-707-77-37.

Zubina Ruslana, lecturer of the Department of complex information security systems, The National Aviation University, Kyiv, Ukraine. Scientific interests: complex information security system. Interests and hobbies: volleyball, boating, surfing. Address: Kosmonavta Komarova ave.1, Kyiv, Ukraine, 097-707-77-37.

Frolov Oleg, aspirant of the Department of complex information security systems, The National Aviation University, Kyiv, Ukraine. Scientific interests: complex information security system. Interests and hobbies: volleyball, boating, surfing. Address: Kosmonavta Komarova ave.1, Kyiv, Ukraine, 097-707-77-37.