УДК 004:651.93

М.Є. Шелест, доктор технічних наук, професор
В.І. Андреев, кандидат технічних наук

КОМП'ЮТЕРНА СТЕГАНОГРАФІЯ ТА ЇЇ МОЖЛИВОСТІ

У статті узагальнюються сучасні уявлення про комп'ютерну стеганографію, проводиться аналіз принципів створення й функціонування стеганографічних систем, дається класифікація стеганографічних методів, в основі яких лежить цифрове представлення аналогового контейнера, наводяться підходи до формального опису моделей стеганографічних систем й одержання оцінок їхніх базових параметрів.

Ключові слова: *стеганографія, стегосистема, стеганаліз, стеганографічний контейнер, стеганографічне перетворення, захист інформації.*

В статье обобщаются современные представления о компьютерной стеганографии, проводится анализ принципов создания и функционирования стеганографических систем, дается классификация стеганографических методов, в основе которых лежит цифровое представление аналогового контейнера, даются подходы к формальному описанию моделей стеганографических систем и получению оценок их базовых параметров.

Ключевые слова: *стеганография, стегосистема, стеганализ, стеганографический контейнер, стеганографическое преобразование, защита информации.*

Modern views about computer steganography are generalized; analysis of the principles of steganographic systems creation and functioning is carried out, classification of steganographic methods, founded on the basis of the digital representation of the analogue container is given, approaches to the formal description of the models of steganographic systems and to estimation of their basic parameters are suggested.

Keywords: *steganography, steganographic system, steganographic analysis, steganographic container, steganographic transformation, information security.*

Стеганографія – наука про методи захисту інформації шляхом приховання факту її існування в тому або іншому середовищі має тисячолітню історію. Приховання факту існування таємного повідомлення завжди видавалося доцільним для його захисту, а наявність різних технічних, хімічних, фізичних і психологічних методів такого приховання забезпечувало можливість його реалізації. Сьогодні стеганографія являє собою сукупність методів і технічних рішень, що реалізують захист інформації, заснований на різних принципах. Однак в умовах стрімкого зростання інформаційно-телекомунікаційних технологій найбільш активно розвиваються комп'ютерні методи стеганографії й способи їхнього застосування в кібернетичному просторі.

В основі багатьох підходів до вирішення завдань стеганографії лежить спільна із криптографією методична й інструментальна база, закладена Шеноном при розробці загальної теорії секретного зв'язку. Це пов'язано з тим, що стеганографія

й криптографія розвивалися в рамках єдиної науки – тайнопису. Лише наприкінці XIX століття, після формулювання Кирхгофом базових законів криптографії, основний з яких полягав у тому, що стійкість криптографічного перетворення визначається таємністю ключа, криптографія відокремилася від стеганографії й стала розвиватися як самостійна наука. Визначальним моментом у стеганографії залишилося збереження в таємниці алгоритму стеганографічного перетворення.

У сучасній стеганографії можна виділити два напрями: технологічну стеганографію й інформаційну стеганографію. До технологічної стеганографії належать методи, які засновані на використанні хімічних або фізичних властивостей різних матеріальних носіїв інформації. Хімічні методи стеганографії зводяться майже винятково до застосування невидимого чорнила. До фізичних методів можна віднести мікрокрапки, різного виду схованки й методи камуфляжу. Крім цього, з'явився цілий ряд нових технологій, які, базуючись на традиційних підходах стеганографії, використовують останні досягнення мікроелектроніки (голограми, кінеграми).

До інформаційної стеганографії можна віднести методи лінгвістичної й комп'ютерної стеганографії. Найважливішою категорією стали стеганографічні методи в їхній проекції на інструментарій і середовище, що реалізується на основі комп'ютерної техніки й програмного забезпечення в рамках окремих обчислювальних або керуючих систем, корпоративних або глобальних інформаційно-телекомунікаційних мереж. Такі методи становлять предмет вивчення комп'ютерної стеганографії, що досліджує питання, пов'язані з прихованою передачею й зберіганням інформації, з організацією прихованих каналів у комп'ютерних системах і інформаційно-телекомунікаційних мережах, завадостійкою аутентифікацією, а також з технологіями цифрових водяних знаків і цифрових відбитків.

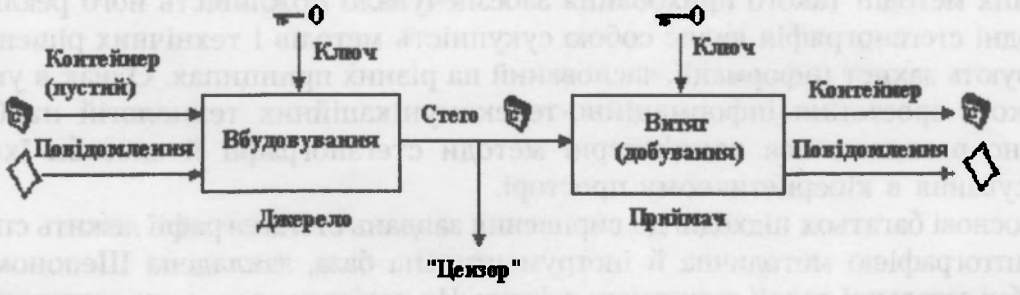
Розвиток комп'ютерної стеганографії відбувається завдяки інтенсивному впровадженню в усі сфери діяльності людини засобів обчислювальної техніки й створенню широких можливостей для оперативного обміну різною інформацією у вигляді текстів, програм, звуку, відео й образів між будь-якими учасниками мережевих сеансів незалежно від їхнього територіального розміщення. Це дозволяє активно використовувати всі переваги, які дають стеганографічні методи.

Загальну схему стеганографічної системи наведено на мал. 1. Вважається, що її функціонування задовольняє наступним положенням:

– для заданого повідомлення, що вбудовується, контейнера й ключа стеганографічне перетворення однозначно формує стегограму;

– за наявності стегоключа зворотне стегоперетворення дозволяє однозначно витягти приховане повідомлення;

– "цензор" (супротивник) не має апріорно точних відомостей про факт існування в контейнері прихованого повідомлення.



Мал.1. Загальна схема стегосистеми

У розглянутій схемі цензорові приділяється роль стеганалітика. Основною метою стеганографічного аналізу є моделювання системи й дослідження її моделі з метою одержання якісних і кількісних оцінок надійності стеганографічного перетворення, а також побудова методик виявлення прихованої інформації, її зміни або руйнування. Стегосистема вважається зламаною, якщо супротивникові, принаймні, вдалося довести факт існування прихованого повідомлення в перехопленому контейнері. Зазвичай виділяють кілька етапів злому стегосистеми:

виявлення факту присутності приховуваної інформації;

добування приховуваної інформації;

викривлення (підміна) приховуваної інформації;

видалення (руйнування) приховуваної інформації;

заборона на здійснення будь-якого пересилання інформації, у тому числі й приховуваної.

Перші два етапи належать до пасивних атак на стеганографічну систему, а останні – до активних (або зловмисних) атак. Основна мета атак на стегосистему аналогічна до атак на криптосистему з тією лише різницею, що різко зростає значимість активних атак, тому що будь-який контейнер може бути змінений з метою видалення або руйнування приховуваного повідомлення. Навіть за найсприятливіших умов для атаки завдання добування прихованого повідомлення з контейнера може виявитися дуже складним. Однозначно стверджувати про факт наявності прихованої інформації можна лише після її виділення й представлення в явному вигляді.

За рівнем забезпечення секретності стегосистеми поділяються на теоретично стійкі системи, практично стійкі й нестійкі.

Теоретично стійка (цілком надійна) стегосистема здійснює приховування інформації тільки в тих фрагментах контейнера, значення елементів яких не перевищує рівня шумів або помилок квантування, і при цьому теоретично доведено, що неможливо створити метод виявлення прихованої інформації. Практично стійка стегосистема здійснює таку модифікацію фрагментів контейнера, зміни яких можуть бути виявлені, але достеменно відомо, що на цей момент у супротивника поки відсутній необхідний для цього інструментарій. Нестійка стегосистема приховує інформацію таким чином, що наявні аналітичні засоби дозволяють її виявити. Стеганаліз допомагає знайти уразливі місця стеганографічного перетворення й провести його поліпшення таким чином, щоб усі зміни, які вносяться до контейнера, знову опинилися б у області теоретичної або практичної нерозрізненості.

Створення й експлуатація надійного стегозасобу передбачає наявність певного інструментарію для його контролю й оцінки. Кількісна оцінка стійкості стеганографічної системи до зовнішніх впливів являє собою складне завдання, що на практиці зазвичай реалізується методами системного аналізу, математичного моделювання або експериментального дослідження. Оцінка якості основної характеристики стегосистеми рівня прихованості забезпечується шляхом здійснення аналітичних досліджень (стеганалізу) і натурних випробувань. Для оцінки якості приховання повідомлення часто удаються до відомих методів з інших областей, у першу чергу – криптографічного аналізу.

Один із основних напрямів у комп'ютерній стеганографії полягає у використанні властивостей надмірності інформаційного середовища. Варто врахувати, що при прихованні інформації відбувається спотворення деяких

статистичних властивостей середовища, які необхідно враховувати для зменшення демаскуючих ознак. Тому в деяких випадках досить ефективним є метод оцінки рівня прихованості, забезпечуваного стегозасобом, на основі аналізу його статистичних характеристик.

Для методів комп'ютерної стеганографії можна запровадити певну класифікацію (мал. 2).

За способом добору контейнера розрізняють методи сурогатної стеганографії, селективній стеганографії й стеганографії, що конструює.

У методі сурогатної (безальтернативної) стеганографії відсутня можливість вибору контейнера – для приховання повідомлення обирається перший-ліпший контейнер, найчастіше не зовсім придатний для повідомлення, що вбудовується. У цьому випадку фрагменти контейнера заміняються на фрагменти приховуваного повідомлення таким чином, щоб зміна не була помітною. Основним недоліком цього методу є те, що він дозволяє приховувати лише незначну кількість даних.

У методах селективної стеганографії передбачається, що приховане повідомлення повинне відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велику кількість альтернативних контейнерів, щоб потім обрати найбільш придатний з них для конкретного повідомлення.

Мал. 2. Класифікація методів приховування інформації

У конструюючих методах стеганографії контейнер генерується самою стегосистемою. Тут може бути кілька варіантів реалізації (наприклад, шум контейнера може моделюватися приховуваним повідомленням).

За способом доступу до приховуваної інформації розрізняють методи для потокових (безперервних) контейнерів і методи для контейнерів довільного доступу (обмеженої довжини).

Методи, що використовують потокові контейнери, працюють із потоками безперервних даних (наприклад, IP-телефонія). У цьому випадку приховувану інформацію необхідно включати до інформаційного потоку в режимі реального часу. Про потоковий контейнер не можна попередньо сказати, коли він почнеться, коли закінчиться й наскільки довгим він буде.

Методи приховування, що використовують контейнери з довільним доступом, призначені для роботи з контейнерами фіксованої довжини (наприклад, файлами). У цьому випадку заздалегідь відомі розміри контейнера і його вміст. Фрагменти контейнера для розміщення приховуваної інформації можуть обиратися за допомогою придатної псевдовипадкової функції.

За типом організації контейнери, подібно до завадозахищених кодів, можуть бути систематичними й несистематичними. У систематично організованих контейнерах можна вказати на фрагменти, у яких приховане повідомлення. При несистематичній організації контейнера такого розділення зробити не можна. У цьому випадку для виділення прихованої інформації необхідно обробити вміст всієї стегограми.

За використовуваним підходом стегометоди можна розбити на два класи: цифрові методи й когнітивні методи.

Нині головним чином поширені цифрові методи стеганографії, суть яких полягає в непомітному й надійному приховуванні одних бітових послідовностей в інших, що мають аналогову природу (звук, зображення або інші оцифровані безперервні сигнали). У таких методах зазвичай використовується надмірність контейнера (головним чином маніпулюють із цифровим представленням його елементів: пікселами, різними коефіцієнтами перетворень). Основний недолік цих методів – недостатня стійкість до активних атак на стегоб'єкт із метою руйнування прихованого каналу.

Когнітивні методи, на відміну від цифрових, дозволяють будувати стегоперетворення, у яких би враховувалися семантичні властивості контейнера. Передумовою цього є успішний розвиток досліджень зі створення штучного інтелекту й сучасний стан комп'ютерної техніки.

За призначенням розрізняють власне методи стеганографії для прихованої передачі або прихованого зберігання даних, а також методи приховування даних у цифрових об'єктах з метою захисту самих цифрових об'єктів.

До останніх методів належать методи цифрових водяних знаків і цифрових відбитків. Цифрові водяні знаки, поміщені у файл, містять спеціальну інформацію (час створення файлу, ім'я власника авторських прав і т.п.) і можуть бути розпізнані тільки спеціальними засобами. Цифрові відбитки забезпечують вбудовування в кожну копію файлу унікального номера, що захищається, що дозволяє власникові інтелектуальної власності ідентифікувати користувачів, які порушують ліцензійні угоди й передають інформацію третій стороні, а також у деяких випадках відстежити шлях проходження незаконної копії.

За типом інформаційного середовища виділяють стеганографічні методи для аудіосередовища, для зображень і відео, для текстового середовища, програмного середовища.

Широкого розвитку методи комп'ютерної стеганографії набули стосовно аудіосередовища, тому що в цьому випадку можливе пересилання великих обсягів прихованих даних у звукових повідомленнях, трансльованих мережею (телевізійною, телефонною, радіо), а також переданих через мережу Інтернет або у

файлах електронною поштою. Особливості слуху людини дозволяють успішно застосовувати такі методи кодування даних при їхньому приховуванні, як метод найменших значущих бітів; метод кодування луна-сигналом; метод широкополосного кодування й метод фазового кодування.

При розробці стегометодів для роботи із зображеннями або відеосередовищем використовують такі особливості системи зору людини, як низька чутливість до контрасту й відносна нечутливість до малих просторових змін яскравості й кольору. Для графічного середовища найчастіше використовуються зазначені вище методи найменшого значущого біта й широкополосного кодування, метод модифікації яскравості й кольоровості зображення, а також маскування й модифікація різних алгоритмічних перетворень зображення або їхніх стисків.

Розвиток комп'ютерної стеганографії стимулюється розвитком глобальних інформаційно-телекомунікаційних мереж, які надають можливість вільного підключення до них всіх бажаючих. Наявність таких особливостей у структурі й організації глобальної мережі як створення серверів, сайтів, реалізація нсевдоактивних режимів обміну й інше особливо сприяє масовому застосуванню стеганографії. Специфіка інформаційно-телекомунікаційних мереж дозволяє використовувати будь-який тип інформаційного середовища, що використовується в цих мережах. Такими типами можуть бути графічні зображення, звукові файли, тексти, програмне забезпечення різного призначення, мультимедійні файли, різні енциклопедії, системи, що навчають або інші системи, орієнтовані на рішення тих або інших прикладних завдань. У межах одного діалогового сеансу можна використовувати той самий тип інформаційного середовища, обґрунтовуючи відновлення відповідних файлів розходженням версій їх реалізації, тим більше, що версії можуть відображати спеціалізацію файлу до тієї або іншої предметної області, його часову модифікацію й т.і.

Існуюча теоретична база стеганографії дозволяє будувати моделі й отримувати обґрунтовані оцінки різних методів стегозахисту, формувати нові напрями досліджень у комп'ютерній стеганографії. У рамках інформаційної моделі стеганографії доцільно виділити наступні типи моделей стеганографічного перетворення:

І. Модель, що описує взаємодію стеганографічно захищеного повідомлення із зовнішнім середовищем. Елементами такої моделі є:

– учасники прихованого обміну повідомленнями (абоненти);

– "супротивник", що здійснює спроби несанкціонованого доступу до інформації, що захищається, у вигляді тої або іншої загрози;

– система керування атрибутами стеганографічного перетворення.

ІІ. Модель, що описує стеганографічне перетворення повідомлення. Як елементи моделі фігурують:

інформаційне середовище, у якому приховане повідомлення;

саме приховуване повідомлення;

алгоритми або методи приховування повідомлення в інформаційному середовищі.

ІІІ. Модель, що описує вплив загроз на певне інформаційне середовище, у якому міститься приховане повідомлення.

Модель, яка описує взаємодію стеганографічно захищеного повідомлення з абонентами й супротивником, що створює ті або інші загрози, найчастіше орієнтована на одержання відносної оцінки параметрів стегосистеми. Такі моделі

дозволяють лише приблизно оцінювати систему, оскільки в цьому випадку можливі різноманітні види загроз, від яких залежить захищеність інформації й, відповідно, можливості абонентів в організації прихованого листування. Прикладом залежності захищеності прихованого повідомлення від типу загроз, що впливають на нього, може слугувати наступне. Якщо загроза полягає тільки у виявленні факту наявності приховуваної інформації (що актуально у випадку прямого протиборства із супротивником), то тоді вона може скомпрометувати всю систему захисту. Якщо загроза полягає лише в пасивному перехопленні повідомлення, то в цьому випадку вона може не впливати прямим чином на можливості абонентів. Якщо загроза полягає в перехопленні повідомлення й його модифікації або руйнуванні, то в цьому випадку зменшуються можливості одержувача у використанні прийнятого повідомлення. Це й пояснює той факт, що моделі систем стегозахисту, які відповідають такій широкій постановці завдання, не можуть бути достатньо ефективними з погляду одержання параметрів, що характеризують стеганографічний метод.

Другий метод моделювання дозволяє описати процес стеганографічного перетворення, його вплив на інформаційне середовище й, відповідно, досліджувати можливості виявлення прихованого повідомлення без урахування впливу загроз на інформаційне середовище або саме повідомлення. На основі таких моделей можна одержувати абсолютні параметри й абсолютні характеристики тих або інших стегоперетворень. У цьому випадку порівняльний аналіз різних стеганографічних методів може здійснюватися на основі абсолютних параметрів.

Третій метод моделювання являє собою опис взаємодії різних моделей загроз із моделями стеганографічних перетворень. У рамках цього підходу можна досліджувати певну обрану модель стегоперетворення з узагальненою моделлю набору загроз, які генеруються супротивником, і отримати фактичні значення параметрів стеганографічної моделі, що становить практичний інтерес. У цьому випадку не можна виключати участі абонентів із зовнішнього середовища моделей, оскільки в кінцевому підсумку параметри абонента і його модель, що описує використання прихованого повідомлення, визначають цінність тієї або іншої моделі стегозахисту.

Моделі першого типу назвемо зовнішніми моделями стегосистеми, моделі другого типу – абсолютними моделями, а третього типу – інтегральними моделями.

Цілком очевидно, що інтегральна модель описує взаємодію трьох моделей і, як наслідок, складається з наступних компонентів:

– абсолютної моделі стеганографії (АМ);

– моделі супротивника, що враховує систему можливих погроз на стегосистеми (МП);

– моделі абонентів стегоповідомлення (МАС).

Модель супротивника являє собою в найпростішому випадку сукупність загроз, які може формувати й застосовувати супротивник стосовно абсолютної моделі. Очевидно, що для досягнення супротивником мети з дискредитації АМ може виявитися необхідним використання певного комплексу загроз, що у свою чергу може являти собою окрему модель, яка входить до складу зазначеної вище моделі типу МП. Компрометація абсолютної моделі, що на змістовому рівні являє собою мету функціонування МП, може бути досить багатосторонньою й полягати в наступних впливах:

– перехоплення стегограми й виявлення факту наявності прихованого повідомлення;
– здобування зі стегограми прихованого повідомлення;
– знищення прихованого повідомлення;
– модифікація прихованого повідомлення й т.д.

Природно, що та або інша мета МП істотно залежить від МАС. Можлива ситуація, коли реалізація деякої мети МП може призвести до неприпустимості використання повідомлення в рамках МАС у силу наступних причин:
– повному знецінюванню повідомлення з погляду параметрів моделі МАС;
– впливу повідомлення, що може привести до погіршення параметрів МАС;
– ліквідації МАС, як компоненти інтегральної моделі, внаслідок повної компрометації АМ з боку МП.

Перші дві причини не вимагають додаткових коментарів. Щодо третьої, МАС розглядається з погляду участі адресата в інтегральній моделі. Це означає, що МАС складається з опису тільки тих параметрів, які досить виразно пов'язані, насамперед, з параметрами АМ і можливими повідомленнями, що походять із АМ. Прикладом параметрів АМ можуть служити стеганографічні ключі й інші компоненти, які необхідні для вирішення зворотного завдання стегоперетворення.

Слід підкреслити, що у викладених уявленнях про моделі з різними компонентами інтегральної моделі досить чітко співвідносяться такі поняття, як пряме й зворотне завдання стеганографії, а також завдання стеганографічного аналізу. Пряме завдання стеганографії вирішується винятково в рамках АМ. Зворотне завдання стеганографії вирішується винятково в рамках МАС. Завдання стеганалізу вирішується в рамках МП.

Насамкінець слід зазначити, що головна особливість стеганографічних методів – приховування факту наявності інформації, що захищається, дозволяє успішно вирішувати широке коло завдань із захисту інформації в обчислювальних си-стемах і мережах телекомунікацій. Створення глобальної світової інформаційної інфраструктури (кібернетичного простору), масове впровадження ком'ютеризованих засобів автоматизації дозволяє реалізовувати нестандартні підходи нри розробці методів комп'ютерної стеганографії. Нині головним чином поширені методи цифрової стеганографії, засновані на надмірності середовища приховування, що має аналогову природу й представлена в цифровому вигляді. Ці методи успішно працюють зі звуком і зображенням, але мають обмежене застосування й високу вразливість стегонаграфічного каналу. Сучасні досягнення в галузі штучного інтелекту й комп'ютерних технологій є основою для розширення бази побудови стеганографічних перетворень та подальшого розвитку стеганографії в цілому.

Отримано 24.03.2011