УДК 004.9

Д.О. Тарасов, А.С. Мельник, М.М. Голобородько
Національний університет “Львівська політехніка”,
кафедра інформаційних систем та мереж

КЛАСИФІКАЦІЯ ТА АНАЛІЗ БЕЗКОШТОВНИХ ПРОГРАМНИХ ЗАСОБІВ СТЕГАНОГРАФІЇ

Сформовано критерії стеганографічних засобів; здійснено загальний огляд стеганографічних алгоритмів; виконано аналіз безкоштовних програмних засобів стеганографії.

Ключові слова: комп’ютерна стеганографія, цілі стеганографії, критерії стеганографічних засобів, стеганографічні алгоритми, програмні засоби стеганографії.

The article deals with the criteria of stenographic means; gives the review of steganographic algorithms; contains analyses of free software steganography.

Keywords: computer steganography, steganography aims, criteria of stenography, steganographic algorithms, steganography software.

Постановка проблеми та аналіз останніх досліджень

Слово “стеганографія” має грецьке походження і буквально означає “тайнопис”. Мета стеганографії – приховати факт існування секретного повідомлення. Такі повідомлення вводять в різноманітні зовнішні “невинні” дані, які не привертають до себе уваги і передають разом з ними без будь-якої підозри збоку.

У давнину для приховування секретних повідомлень використовували покриті воском дощечки, симпатичні чорнила, невидимі за звичайних умов; приховане повідомлення розміщували в певні букви невинних словосполучень, вносили в текст незначні стилістичні, орфографічні або пунктуаційні помилки.

Розвиток засобів цифрової обчислювальної техніки дав поштовх для розвитку комп’ютерної стеганографії, яка ґрунтується на вбудовуванні секретного повідомлення в цифрові дані, що, як правило, мають аналогову природу (аудіозаписи, зображення, відео). Можливе також вбудовування інформації в текстові та скомпресовані файли.

Часто назви понять, що стосуються стеганографії, мають префіксну приставку «стего-» (скорочення від «стеганографічний»). Розглянемо основні поняття комп’ютерної стеганографії: стегосистема, контейнер, стегодані, стегоключ.

Стегосистема – сукупність засобів і методів, які використовують для формування прихованого каналу передавання інформації [1].

Контейнер – цифровий об’єкт (зазвичай це файл), в який вбудовують секретну інформацію. Розрізняють **пустий контейнер** – контейнер без вбудованої інформації і **заповнений контейнер** (стегоконтейнер) – контейнер, який містить вбудовану інформацію.

Стегодані – цифрова інформація (послідовність бітів і байтів, наприклад, у формі файла), яку вбудовують у контейнер.

Стегоключ – секретний ключ, який використовують для вбудовування і видобування стегоданих в/із стегоконтейнера. Залежно від кількості рівнів захисту (наприклад, якщо стегодані попередньо зашифровують) у стегосистемі може бути від одного до декількох стегоключів [1]. Деякі стегосистеми не використовують ключів.

Формулювання цілей статті

У цій роботі ми сформуємо критерії оцінки та класифікації стеганографічних засобів та алгоритмів; виконаємо короткий огляд алгоритмів стеганографії; здійснимо аналіз безкоштовних програмних реалізацій стеганографічних засобів, які існують сьогодні.

Виклад основного матеріалу

Вимоги до стегосистеми залежать від цілей комп'ютерної стеганографії. Вбудовування стегоданих виконують для прихованої комунікації, захисту авторства (цифрові водяні знаки) та для тегування.

Прихована комунікація

Пересилання зашифрованих даних часто привертає зайву увагу зловмисників. Тому іноді для передавання важливих даних застосовують стеганографічні методи. Секретну інформацію вбудовують у контейнер, відкрито передаючи цей контейнер отримувачу (наприклад, пересилаючи поштою або публікуючи в Інтернеті). У такому разі потенційного зловмисника «обманюють», приховуючи фактичне повідомлення. Об'єм секретної інформації може коливатися в значних межах (від декількох байтів до кількох мегабайтів). Основною вимогою є таємність (непомітність) прихованої інформації.

Цифрові водяні знаки (ЦВЗ)

ЦВЗ використовують для захисту інтелектуальної власності контейнера (Intellectual Property). ЦВЗ – це, зазвичай, невеликий об'єм інформації (наприклад, ім'я автора, торгова марка, дата публікації, цифровий ідентифікатор об'єкта (Digital Object Identifier) тощо), яку вбудовують в контейнер з можливістю її подальшого виявлення, зокрема для підтвердження авторства у разі несанкціонованого копіювання. ЦВЗ можна також використовувати для виявлення потенційних піратів [9]: під час продажу в зображення вбудовують інформацію про час продажу та інформацію про покупця. Ключовою відмінністю ЦВЗ від звичайного приховання інформації є наявність активного противника [8]. Наприклад, використовуючи ЦВЗ для захисту авторського права, активний противник намагатиметься видалити чи змінити вбудовані ЦВЗ. Тому основною вимогою є стійкість вбудованих даних до атак. Таємність не є настільки важливою, як у прихованій комунікації.

Feature Tagging (тегування)

Іноді вбудовування даних виконують не стільки задля приховання факту існування інформації, як для зручності – щоб контейнер містив корисну інформацію про його вміст: заголовок, опис тощо. Наприклад, в растрове зображення можна вбудувати імена людей на фотографії чи місце знімання фото. Очевидно, що при копіюванні файла такого зображення копіюватиметься і вся ця інформація. У базу даних зображень можна вбудовувати ключові слова для пошуку. Якщо зображення є фреймом відео, то вбудовані часові маркери можна застосовувати для синхронізації з аудіо. У зображення можна вбудовувати кількість переглядів і використовувати це у "pay-per-view" додатку [9].

Формування критеріїв оцінки стеганографічних засобів

Оцінка стеганографічних засобів комплексна складається з оцінок за різними критеріями (ці критерії можна використовувати також для класифікації стеганографічних засобів). Критерії стеганогафічних засобів розділимо на три групи: критерії оцінки, що стосуються: *а*) контейнерів; *б*) стегоданих; *в*) стеганографічного алгоритму.

Контейнери

Розглянемо критерії, що стосуються контейнерів

Типи контейнерів, які підтримує засіб (зазвичай це файли певного типу, наприклад, зображення bmp, аудіо mp3, відео avi).

Складений контейнер – два та більше окремих файлів, зокрема різних форматів. Можливість стеганографічного засобу використовувати складений контейнер дає змогу приховати великі об'єми стегоданих. Окрім цього, у разі використання складеного контейнера зростає таємність, оскільки частини складеного контейнера можна передавати різними каналами, тому при потраплянні однієї з цих частин до зловмисника він не зможе отримати секретне повідомлення через відсутність інших частин.

Стеганодані

Критерії, що стосуються стегоданих:

типи стеганоданих (файли певного типу, текст);

складені стеганодані (можливість приховання двох та більше окремих файлів, зокрема різних форматів);

компресія стеганоданих (стиснення даних перед приховуванням);

шифрування стеганоданих (перед приховуванням);

використання хеш-суми; наявність хеш-суми стегоданих дає змогу перевірити їхню цілісність після видобування.

Алгоритм

Розглянемо критерії, що стосуються стеганографічного алгоритму (способу вбудовування секретних даних у контейнер).

Робастність – стійкість стеганографічного контейнера до зовнішнього опрацювання [2, 3] (тобто збереження стегоданих після модифікації стегоконтейнера). Цей критерій є критичним для захисту авторства за допомогою ЦВЗ, оскільки зловмисники намагатимуться знищити вбудовані ЦВЗ, виконавши певні перетворення над контейнером [9].

Таємність [2, 3] – стійкість до виявлення стегоданих та їх видобування зі стегоконтейнера. Цей критерій є критичним для прихованої комунікації. Виконаємо декомпозицію критерію таємності:

- *стійкість до виявлення* факту існування стегоданих – залежить від того, чи змінюються певні характеристики контейнера після вбудовування у нього стегоданих:
  - *властивості контейнера* (наприклад, розмір);
  - *аудіовізуальні характеристики* контейнера (після вбудовування стегоданих можлива втрата якості зображення, підвищення кількості шумів тощо);
  - *структура, ключові елементи та статистичні характеристики* контейнера (зміни цих характеристик часто неочевидні, але їх можна виявити, виконавши аналіз стегаконтейнера за допомогою спеціальних засобів);
- *стійкість до отримання* стеганоданих:
  - *шифрування стеганоданих* (під час попереднього шифрування даних, якщо зловмиснику вдасться видобути стегодані, він не зможе розшифрувати їх через відсутність у нього секретного ключа);
  - *складність розподілу стеганоданих* у контейнері.

Ємність – максимальна кількість інформації, яка може бути вбудована в контейнер певного розміру. Зазвичай ємність контейнера визначають з урахуванням обмежень таємності та робастності. В [8] розглянуто два альтернативні визначення поняття стеганографічної ємності.

Зазначимо, що, залежно від шкали, оцінки бувають: *а*) *бінарними* (оцінюють значеннями «є» і «немає», залежно від того, чи притаманний об'єкт критерію стеганографічному засобу, чи ні); *б*) *градуйованими* (оцінка може набувати певного числового значення у визначеному діапазоні).

Критерії, що стосуються контейнерів і стегоданих, оцінюють бінарними оцінками, алгоритму – переважно градуйованими. Формування єдиної градуйованої шкали оцінювання цих критеріїв виходить за межі цієї роботи.

Типи контейнерів та стеганографічні алгоритми

Розглянемо стеганографічні алгоритми, класифіковані за контейнерами, для яких використовують ці алгоритми.

Графічні растрові зображення без палітри

LSB (Least Significant Bit – найменший значущий біт) – суть методу полягає в заміні останніх значущих бітів у контейнері на біти приховуваної інформації. Наприклад, розглянемо 24-розрядне растрове зображення як контейнер. Кожному пікселу відповідає три байти (значення трьох компонент кольору – червоного, зеленого і синього). Приховані дані можна записувати в останній біт кожного байта (тобто один піксел зображення міститиме три біти секретних даних). Різниця між пустим і заповненим контейнером візуально буде непомітною.

Стеганографічне зображення, отримане в результаті роботи LSB-алгоритму, дуже чутливе до будь-яких модифікацій (тобто низький рівень робастності). Найменше опрацювання цього зображення призведе до втрати вбудованої інформації.

Виявлення прихованої LSB-алгоритмом інформації можливе через виявлення аномальних характеристик розподілу значень наймолодших бітів цифрового сигналу [8], але деякі модифікації LSB-алгоритму не змінюють цих характеристик, відповідно розподіляючи секретні дані.

Розглянемо підвиди LSB-алгоритмів для растрових зображень без палітри [4].

BlindHide (приховування всліпу). Найпростіший алгоритм: дані записують, починаючи з верхнього лівого кута зображення до правого нижнього – піксел за пікселем. Приховані дані програма записує у наймолодших бітах кольорів піксела. Приховані дані розподіляються у контейнері нерівномірно. Якщо приховані дані не заповнять повністю контейнер, то лише верхня частина зображення буде засміченою.

HideSeek (заховати–знайти). Цей алгоритм у псевдовипадковий спосіб розподіляє приховане повідомлення у контейнері. Для генерації випадкової послідовності використовує пароль. Дещо «розумніший» алгоритм, але все ж не враховує особливостей зображення-контейнера.

FilterFirst (попередня фільтрація). Виконує фільтрацію зображення-контейнера – пошук пікселів, у які записуватиметься прихована інформація (для яких зміна наймолодших розрядів буде найменш помітною для ока людини).

BattleSteg (стеганографія морської битви). Найскладніший і найдосконаліший алгоритм. Спочатку виконує фільтрацію зображення-контейнера, після чого прихована інформація записується у «найкращі місця» контейнера у псевдовипадковий спосіб (подібно, як у HideSeek).

Графічні растрові зображення з палітрою

LSB. Використання цього алгоритму для зображень з палітрою (наприклад, GIF) пов'язане з деякими труднощами. Кожен піксел записаний індексом, який вказує на певний колір палітри (таблиці, в які записані всі кольори зображення). Навіть зміна значення наймолодшого біта цього індексу може призвести до радикальної зміни кольору піксела. Для мінімізації цього побічного ефекту палітру попередньо сортують так, щоб колірна різниця між сусідніми (за індексами) кольорами була мінімальною [8].

Аудіофайли

LSB. Принцип роботи цього методу для аудіофайлів аналогічний, як для растрових зображень. У разі аудіофайлів для запису інформації використовуються молодші біти кожного звукового семплу.

Polarity Inversion (інверсія полярності). У більшості мов потік повітря, що утворюється під час звукоутворення, є однонапрямленим. Це викликає постійну полярність коливань мовлення. Людська слухова система не в змозі розрізнити мовні сигнали з додатною й від'ємною полярністю. Цей факт використовується у цьому методі.

Аудіосигнал ділиться на сегменти (зазвичай для мовленнєвого сигналу це склади) і кожному сегменту призначається один біт інформації. Значення біта задається зміною полярності сегмента [11].

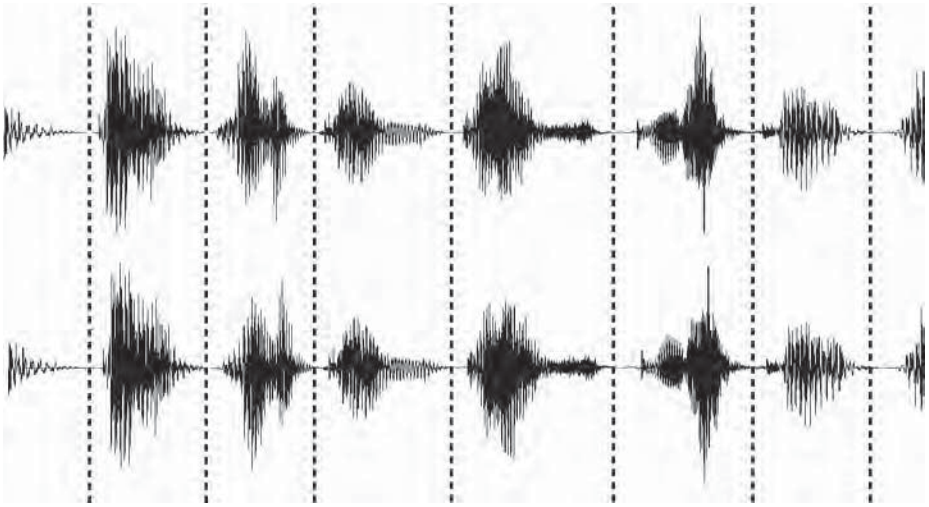

Рис. 1. Аудіосигнал до (зверху) та після (знизу) використання алгоритму інверсії полярності. Пунктиром розділено сегменти аудіосигналу

Echo Hiding (ехо-приховування). Цей метод виконує приховування даних додаванням відлуння у звуковий сигнал. До параметрів відлуння належать: початкова амплітуда, часу спаду і зсуву (час затримки між вихідним сигналом і його відлунням) (рис. 2). При зменшенні зсуву два сигнали змішуються і відлуння перестає бути відчутним для людини, зазвичай, якщо відстань між ними близько 1 мс [10].

Аудіосигнал розділяють на сегменти, кожному з яких призначається біт. Далі для кожного сегмента виконується зміна параметрів відлуння. Використовують два часи затримки: один – для кодування нуля, другий – для кодування одиниці.

Phase Coding (фазове кодування) – вбудовування інформації в фазу сигналу. У цьому методі фаза початкового сегмента аудіосигналу модифікується залежно від вхідних даних. Фази наступних сегментів узгоджуються з нею для збереження різниці фаз. Це необхідно, тому що людське вухо дуже чутливе до різниці фаз.

Фазове кодування є одним з найефективніших способів кодування за критерієм відношення сигнал–шум. Головним недоліком можна вважати низьку пропускну здатність [10].

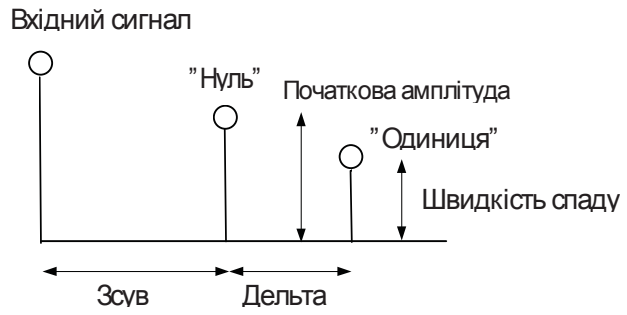

Рис. 2. Параметри ехо-сигналу

Perceptual Masking. Маскуванням називається ефект, за якого слабке, але відчутне звукове коливання стає менш відчутним за наявності іншого, гучнішого (сигнал маскування). Ефект маскування залежить від спектральних і часових характеристик маскованого сигналу і сигналу маскування [10].

Spread Spectrum (SS, розширення спектра). За методом розширення спектра намагаються якомога більше «рознести» приховану інформацію по частотному спектру сигналу звуку. Це аналогічно до систем, що використовують реалізацію LSB, яка у випадковий спосіб поширює біти вхідних даних в усьому спектрі. Проте, на відміну від кодування LSB, метод SS розміщує секретне повідомлення над частотним спектром звукового файла, використовуючи код, який не залежить від звукового сигналу. В результаті кінцевий сигнал займає більшу смугу пропускання, ніж насправді необхідно для передавання [13].

Tone Insertion (вставка тонів). Метод вставки тонів ґрунтується на поганій чутності та нечіткості низьких тонів у присутності компонент значно вищого спектра.

Розглянемо приклад, в якому відбувається вставка двох низькочастотних тонів. Аудіосигнал ділиться на сегменти. Для кожного сегмента обчислюється його потужність f_e. У кожен сегмент додають два тони різної частоти f_0, f_1, проте з різною потужністю. Якщо необхідно записати нуль, тоді потужність f_0 встановлюється 0.25 f_e, а потужність f_1 – 0.001 f_0. Якщо 1 тоді потужність f_1 встановлюється 0.25 f_e, а потужність f_0 – 0.001 f_1. [12]

Відеофайли

Дискретно-косинусне перетворення (ДКП). Цей метод виконує зміну коефіцієнтів дискретно-косинусного перетворення. Дискретно-косинусне перетворення використовується для алгоритму стиснення JPEG для перетворення блоків пікселів зображення 8 х 8 на 64 ДКП коефіцієнти [14].

Один зі стегоалгоритмів використовує таку особливість. Стиснені дані зберігаються як цілі числа, проте усі обчислення виконуються з числами з плаваючою комою, після чого їх округляють. Помилки округлення визначають ступінь втрати при стисненні. Цей алгоритм використовує рівні округлення для приховування інформації [15].

Неформатований текст [5]

Маніпулювання пробілами між словами. Різна кількість пробілів між словами може приховувати інформацію. Наприклад, нулю відповідає один пробіл, одиниці – два.

Додавання хвостових пробілів. У кінець кожного речення чи абзацу додають певну кількість пробілів. Наприклад, нуль пробілів у кінці речення відповідає бітовій послідовності 000, сім пробілів – 111.

Зміна порядку маркерів кінця рядка. Індиферентність більшості текстових редакторів до порядку слідування символів переведення рядка (CR) та повернення каретки (LF) уможливлює використання цієї пари для позначення одного біта інформації: CR/LF може відповідати нулю, CR/LF – одиниці.

Заміна символами з іншої абетки. Цей метод передбачає заміну кириличного символу на символ латиниці з таким самим виглядом (значення біта – нуль) або відмову від такої заміни (значення біта – одиниця).

Морфологічно-синтаксичний метод [6, 7]. Послідовність речень розглядають як послідовність бітів. Функція, яка визначає, чи речення відповідає нулю, чи одиниці, може бути найрізноманітнішою. Наприклад, чи речення активне, чи пасивне; чи речення містить два іменники; чи останній біт хешу речення є нулем, чи одиницею тощо. Складний для реалізації метод, через специфіку вбудовування прихованої інформації: на основі прихованої інформація формують контейнер (можливо, перефор-мульовуючи речення контейнера, зберігаючи при цьому їхню семантику). Особливою відмінністю методу є те, що прихована інформація зберігається у разі переведення контейнера з одного формату в інший, навіть при друці на папір. Наприклад, вбудована в зображення інформація існуватиме доти, доки зображення існуватиме в цифровій формі.

Форматований текст

Форматування символів тексту розглядають як бітову послідовність. Форматування, яке відповідає нулю, візуально дуже близьке до форматування, що відповідає одиниці (різниця непомітна для неозброєного ока). Наприклад, нулю відповідає розмір символу в 14 кеглів, одиниці – 14,5 кегля, або нулю – колір RGB(0, 0, 0), одиниці – RGB(0, 0, 1).

Стиснені (скомпресовані) файли

Файли з секретними даними стискають і додають в кінець скомпресованого файла так, що ці файли є “невидимими” для звичайних програм-архіваторів. Цей метод використовує нестандартний алгоритм створення скомпресованих файлів і його (з відповідними модифікаціями) також можна застосовувати для файлів-контейнерів інших типів.

Аналіз стеганографічних засобів

У таблиці наведено результати практичного аналізу програмних засобів стеганографії.

Показником якості стеганографічного засобу (і методу, відповідно), який впливає на таємність, є природа шуму, який з’являється в стегоконтейнері після приховання даних у ньому. Всі шуми можна розділити на три групи: лінійний шум (шум наявний тільки у тій частині контейнера, де записані приховані дані; приховані дані записують у відповідні біти контейнера, починаючи з його початку); рівномірний шум (приховані дані рівномірно розподілені по контейнеру); контентно-залежний шум (приховані дані розподілено у контейнері так, що утворений шум мінімально впливає на зміну сприйманого людиною вмісту контейнера, тобто на його аудіо-візуальні характеристики).

		Steganos File Manager	MSU StegoVideo	StegoMagic	wbStego4	OpenStego	SteganoWav	SteganoZip	NetToolsSTEG	Hiding Glyph	SteganoG	Max File Encryption	Digital Invisible Ink Toolkit	Puff	GifShuffle	CryptArkan
Commercial/Free		C	F	F	F	F	F	F	F	F	F	C	F	F	F	F
ОС	Windows	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Linux				x	x							x			
Interface: Win/Console		W	W	W	W	W	W	W	W	C	W	W	W	W	C	W
Тип файла-контейнера	bmp	x		x	x	x				x	x		x	x		x
	jpeg	x												x		
	gif														x	
	wav	x		x			x							x		x
	mp3													x		
	avi		x													
	txt			x	x											
	html				x											
	rtf								x							
	pdf				x											
	zip							x								
	Будь-який файл											x				
	Складений													x		x
	Декілька окремо					x										
Стегодані	Тільки txt		x													
	Текст			x			x		x						x	
	Будь-який файл	x		x	x	x		x		x	x	x	x	x		x
	Папка	x								x						
	Складені	x						x				x		x		x
	ЦВЗ				x									x		
Стиснення						x		x						x		
Шифрування				x	x	x		x	x		x	x		x	x	x
Захист паролем		x	x	x	x	x		x	x		x	x		x	x	x
Зберігає атрибути*		x				x		x		x	x	x		x		x

* Для відновлення даних не потрібно знати, які саме дані було приховано.

На рис. 3 на прикладі нестисненого растрового графічного зображення-контейнера показано три різновиди шуму (для наочності показано маски, за якими записані стегодані).

Деякі програми під час приховання даних взагалі не змінюють у файлах-контейнерах аудіо-візуальних характеристик. Так, наприклад, програма Max File Encryption дописує у певний спосіб приховані дані в кінець файла-контейнера. Схожий метод використовує програма SteganoZip для приховування даних у архівних zip-файлах. Недолік такого методу в тому, що він змінює властивості контейнера, тому приховані у такий спосіб дані легко виявити, проаналізувавши розмір, структуру та вміст контейнерів.

Інший метод, який не змінює сприйманого контенту контейнера, використовує програма GifShuffle для приховання даних у контейнерах gif-формату. Суть цього методу полягає у перетасуванні палітри gif-файла для зашифрування прихованих даних. Недолік – приховати таким способом можна лише невелике текстове повідомлення. Це зумовлено розмірністю палітри gif-файлів. Цей метод має низьку стійкість до виявлення стегоданих, оскільки змінює структуру палітри gif-файла.

а *б*

в *г*

Рис. 3. Природа шуму у стегоконтейнері:
а – оригінальне зображення-контейнер; б – лінійний шум;
в – рівномірний шум; г – контентно-залежний шум

Найкращою з погляду практичності є програма Puff. Вона підтримує найбільше серед інших програм форматів даних (зокрема скомпресовані формати растрових зображень та аудіо). Програма може використовувати складений контейнер, що дає змогу приховувати великі обсяги даних. Можна приховувати як будь-які файли, так і папки, причому декілька водночас. Приховані дані програма архівує та шифрує. Програма має високу швидкодію навіть за великих обсягів даних.

Програма Digital Invisible Ink Toolkit завдяки можливості симуляції приховування даних демонструє та дає змогу наочно оцінити роботу різних стеганографічних методів. Цю програму можна використовувати при вивченні та дослідженні стеганографічних методів.

Програма Hiding Glyph приховує дані у контейнері 24-розрядного bmp-формату особливим методом: ключем для отримання прихованих даних є оригінал файла-контейнера. Програма забезпечує високу ємність контейнера: співвідношення об’єму прихованих даних до об’єму контейнера може сягати 1:3 (тоді як більшість методів дають не більше ніж 1:8), при цьому зберігаються візуальні характеристики зображення – шум непомітний для неозброєного ока.

Висновки

У цій роботі сформовано критерії порівняння засобів стеганографії, виконано практичний аналіз 15 програмних засобів стеганографії. Всі ці програми доступні для вільного скачування в мережі Internet.

Більшість програм для стеганографічного захисту у ролі контейнера використовують нескомпресовані 24-розрядні bmp-зображення та 16-розрядні wav-аудіофайли. Це зумовлено поширеністю цих форматів та простотою роботи з ними. Одиниці програм підтримують формати

зображень jpeg та аудіоінформації mp3. Ці програми мають велике практичне значення, оскільки більшість інформації зберігається саме у скомпресованому вигляді.

1. Генне О.В. Основные положения стеганографии [Електронний ресурс] // "Защита информации. Конфидент". – 2000. – № 3. – 10 с. – Режим доступу: http://www.citforum.ru/internet/securities/stegano.shtml 2. Васюра А. С. Метод шаблонного вбудовування даних у вейвлет-коефіцієнти на основі критерію стеганографічної стійкості / А.С. Васюра; В.В. Лукічов // Інформаційні технології та комп'ютерна техніка. – Наукові праці ВНТУ. – 2009. – № 1. – 8 с. 3. Васюра А. С. Підвищення ефективності методу шаблонного вбудовування даних у зображення / А.С. Васюра; В.В. Лукічов // Інформаційні технології та комп'ютерна техніка. – Наукові праці ВНТУ. – 2008. – № 3. – 10 с.4. K. Hempstalk Digital Invisible Ink Toolkit: Documentation and FAQs [Електронний ресурс] // University of Waikato – 2005. – Режим доступу: http://diit.sourceforge.net/doco.html 5. Беляев А. Стеганограмма: скрытие информации // Программист. – 2002. – №1 6. Words Are Not Enough: Sentence Level Natural Language Watermarking / M. Topkara, U. Topkara, M.J. Atallah // Department of Computer Sciences, Purdue University, West Lafayette, IN, 47906, USA. – 2006. – 10 p.7. Syntactic tools for text watermarking / Hasan M. Meral1, Emre Sevinç, Ersin Ünkar ma ін. // Department of Computer Engineering, Boğaziçi University, Cognitive Science Program, Boğaziçi University. – 2007. – 12 с. – ISBN 978-0-8194-6618-1. 8 Image Steganography: Concepts and Practice / M. Kharrazi, H.T. Sencar, N. Memon // Department of Electrical and Computer Engineering, Department of Computer and Information Science, Polytechnic University, Brooklyn, NY 11201, USA. – 2004. – 31 p. 9. A Review of Data Hiding in Digital Images / Eugene T. Lin, Edward J. Delp // Video and Image Processing Laboratory (VIPER), School of Electrical and Computer Engineering, Purdue University, West Lafayette, Indiana. – 1999. – 5 ст. 10. Грибунин В. Г. Цифровая стеганография / В.Г. Грибунин, И. Н. Оков, И. В. Туринцев. – СПб.: Солон-Пресс, 2002. – 272 с. – ISBN: 5-98003-011-5. 11. The effect of polarity inversion of speech on human perception anddata hiding as an application / S. Sakaguchi, T. Arai, Y. Murahara // Proceedings of the Acoustics, Speech, and Signal Processing, 2000. on IEEE international Conference – 2000. – ISBN: 0-7803-6293-4 12. Audio steganography for covert data transmission by imperceptible tone insertion [Електронний ресурс] / Kaliappan Gopalan, Stanley Wenndt // Department of Engineering, Purdue University Calumet – 2004. – Режим доступу: http://www.calumet.purdue.edu/engr/docs/GopalanKali_422_049.pdf 13. Перепелица С.А. Системы и сети связи, ч.1 Теоретические основы передачи данных в информационных системах. Конспект лекций / С.А. Перепелица, Н.В. Богач. – СПб.: Изд-во СПбГПУ. – 2008. – 182 с. 14. Data Hiding in Video [Електронний ресурс] / J.J. Chae, B.S. Manjunath // Department of Electrical and Computer Engineering, University of California – 1999. – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.6652&rep=rep1&type=pdf 15. Стеганография и существующие носители [Електронний ресурс] / Д. Вылегжанин // Курс "Защита информации", кафедра радиотехники, Московский физико-технический институт (МФТИ). – 2004. – Режим доступу: http://www.re.mipt.ru/infsec/2004/essay/2004_Steganigraphy_in_current_medium__ Vilegzhanin.pdf.