УДК 550.34 **doi: 10.26906/SUNZ.2020.1.079**

Т. А. Кошель

Головний центр спеціального контролю Державного космічного агентства України,
смт Городок, Радомишльський район, Житомирська область

ВИБІР МЕТОДА ЛІНГВІСТИЧНОЇ СТЕГАНОГРАФІЇ ДЛЯ ВИКОНАННЯ ЗАВДАНЬ З РЕЄСТРАЦІЇ СЕЙСМІЧНИХ ПОДІЙ

Анотація. Важливим завданням сьогодення в області захисту інформації є впровадження криптологічних методів. Однак на цьому шляху багато невирішених проблем, пов'язаних з руйнівним впливом на криптозасоби таких складових інформаційної зброї, як комп'ютерні віруси, логічні бомби, автономні реплікативні програми. Метою статті є вивчення особливостей синтаксичних методів лінгвістичної стеганографії. У ході досліджень вирішувались задачі ефективного застосування сил та засобів головного центру спеціального контролю під час передачі для обробки даних реєстрації сейсмічних явищ у ближній та дальній зонах. Об'єктом дослідження в роботі є пунктуаційний метод приховування інформації у текстових контейнерах. Запропоновано використовувати модель приховування повідомлень у текстових контейнерах з відкритим доступом. Це можливо на основі блокування несанкціонованого доступу до інформації шляхом шифрування змісту повідомлень. Предметом дослідження є принципи вбудовування та вилучення повідомлень за реалізованим алгоритмом. Методи дослідження: формалізація теоретичної інформації, порівняльний аналіз, розробка методів реалізацій. Розглянуто також атаки на стеганографічні системи та виділено особливості всіх атак. Перевагу було надано синтаксичному методу на основі пунктуації для здійснення приховування інформації під час передачі даних від периферійних центрів до головного центру приймання і обробки інформації. Кінцевими результатами проведеної роботи передбачена реалізація програми вбудовування та вилучення повідомлення в/з контейнера. Було проведено порівняльний аналіз щодо використання типів текстових контейнерів та здійснено аналіз часових рамок процедур вбудовування та вилучення повідомлення.Вказано також і на можливі недоліки пунктуаційного методу. Такі, як складність програмної реалізації, після якої заповнений контейнер повинен відповідати усім вимогам нормальної стеганосистеми, і . труднощі дотримання вимог до пропускної спроможності.

Ключові слова: лінгвістична стеганографія, синтаксичні методи, текстові контейнери, варіативність розділових знаків, пунктуація, кодування.

Вступ

У сучасному світі настільки сильно все залежить від інформації та Інтернету, що нікого не здивуєш викладанням авторських перекладів відомих художніх творів чи власних думок та різноманітних описів, як на просторі Інтернету для закачування іншими, так і для опублікування у блогах та різних соціальних мережах. Тому для застосування у Головному Центрі Спеціального Контролю (ГЦСК) пропонується модель приховування повідомлень саме у текстових контейнерах, з відкритим доступом. Захист інформації від несанкціонованого доступу - одна з найдавніших проблем. Як відомо, ціль криптографії полягає в блокуванні несанкціонованого доступу до інформації шляхом шифрування змісту повідомлень. Ціль стеганографії - приховати сам факт існування секретного повідомлення. При цьому обидва способи можуть бути об'єднані і використані для підвищення ефективності захисту інформації (наприклад, для передачі криптографічних ключів). Комп'ютерні технології додали новий імпульс розвитку й удосконалюванню стеганографії, з'явився новий напрямок в області захисту інформації – лінгвістична стеганографія на основі текстових контейнерів. Дослідження нині відомих синтаксичних методів лінгвістичної стеганографії обумовлюється своєю різноманітністю використання та є запорукою успіху на шляху до розуміння структури приховування та стегоаналізу, для створення власних реалізацій алгоритмів, в залежності від поставлених цілей. Приховування інформації у текстових контейнерах за допомогою пунктуаційного методу несе з собою ряд розробок і пропозицій щодо покращення алгоритму та можливої взаємодії з іншими методами лінгвістичної стеганографії. Актуальність алгоритмів обумовлюється існуючою постійною необхідністю у передачі секретних повідомлень, а досліджені синтаксичні методи лінгвістичної стеганографії мають високу стійкість до виявлення, що дуже цінується у сучасній цифровій стеганографії. Необхідно провести аналіз атак на стеганографічні системи та оцінити особливості всіх атак, що розуміється як відсутність модифікації вбудованих повідомлень для забезпечення непомітності своєї дії. Дослідження, що проводяться в ході виконання поставлених завдань [1] на АСП «ХАРКІВ» допомагають виявити переваги та недоліки методів приховування, складність реалізації та оцінити роботу даного методу [2]. Реалізація алгоритмів приховування та вилучення несе за собою необхідність у детальному вивченні пунктуаційних норм та надмірностей української мови, що також допомагає при аналізі відмінностей між пустим та заповненим контейнерами.

Постановка задачі

Одним з основних завдань, пов'язаних з вирішенням питань передачі інформаційних повідомлень з периферійних пунктів спостереження на всій території України до центрального пункту прийому, обробки даних і прийняття рішення щодо застосування сил та засобів ГЦСК, є забезпечення безперервності функціонування каналу передачі даних за

умов достовірності, оперативності і постановці перешкод в розпізнаванні або розкритті змісту прихованих повідомлень [3]. Остання умова виконання завдань є актуальною на цей день для ГЦСК.

Основний матеріал

Стеганографічна або, скорочено, стегосистема – сукупність засобів та методів, які використовуються для формування непомітного каналу передачі інформації. Її метою є не обмежувати доступ до контейнеру, а в значній мірі гарантувати, що вбудовані дані залишаться цілими і немодифікованими та з подальшою можливістю вилучення [4].

При побудові стеганосистеми повинні враховуватися наступні положення [5]:

1) стеганосистема повинна мати допустиму обчислювальну складність реалізації – кількість кроків або арифметико-логічних операцій, необхідних для вирішення проблеми. В даному випадку – процесу приховування/вилучення конфіденційної інформації в/з контейнеру;

2) повинна забезпечуватися необхідна пропускна спроможність, що є особливо актуальним для стеганосистем системи прихованої передачі інформації;

3) повинні забезпечуватися автентичність та цілісність секретної інформації для авторизованого користувача;

4) потенційний стегоаналітик має повне уявлення про стегосистему та деталях її реалізації, єдине, що йому не відоме – це ключ, за допомогою якого можна визначити факт наявності прихованого повідомлення та його зміст;

5) якщо факт наявності прихованого повідомлення стає відомим стегоаналітику, це не повинно дозволити останньому вилучити його до тих пір, поки ключ залишається секретним;

6) порушник не повинен мати будь-яких технічних та інших переваг в розпізнаванні або розкритті змісту прихованих повідомлень.

Характеристики методів

Обираючи алгоритм, за допомогою якого вирішуватиметься поставлена проблема, необхідно опиратися на обов'язкові переваги наступних характеристик:

1) пропускна спроможність – це максимальна кількість інформації, що може міститися в одному контейнері; при цьому, приховувані повідомлення повинні бути безпомилково передані приймальній стороні (отримувачеві) та захищені від атак несанкціонованих користувачів, таких як спроби виявлення наявності каналу прихованого зв'язку, вилучення приховуваних повідомлень та навмисне введення хибних даних або руйнування вбудованої в контейнер інформації [6];

пропускна спроможність відкритого каналу зв'язку визначається як кількість інформації, яка може бути безпомилково передана за один сеанс використання каналу зв'язку;

пропускна спроможність каналу приховуваного зв'язку значно менша за попередню, адже тут за один сеанс використання каналу приховуваного зв'язку передається один елемент контейнеру, в який вбудована приховувана інформація [7];

2) якість приховування – це міра спотворення контейнеру, адже будь-яке приховування повідомлення так чи інакше змінює структуру контейнеру [8];

3) цю характеристику неможливо виразити в числах, тож найкращий спосіб її виміряти – самостійно або за допомогою групи людей наглядно оцінити контейнер до та після приховування; якість приховування залежить від сприйняття людини або групи людей. Висока пропускна спроможність, зазвичай, погіршує якість приховування;

4) робастність – це міра здатності методу зберігати повідомлення навіть після деяких перетворень над контейнером, таких, як лінійна та нелінійна фільтрація, додавання випадкового шуму, стиснення з втратами та відновлення або деякі види обробки [8];

5) стійкість до спотворень – унеможливлення зміни повідомлення несанкціонованим користувачем у разі спроби спотворення замість знищення [8]; алгоритми, що дотримуються цієї характеристики ускладнюють задачу зміни вбудованого повідомлення або його заміни;

6) стійкість до виявлення – унеможливлення несанкціонованим користувачем виявлення наявності в тексті прихованого повідомлення шляхом статистичної обробки контейнеру, наприклад, підрахунку ймовірнісних критеріїв букв для заданої мови, кількості пробілів або регістрів літер[6];

7) співвідношення «сигнал/шум» [9]; ця величина є мірою якості приховування та стійкості до спотворень; в основному, великі значення співвідношення є ідеальними для систем комунікації, а малі – для стеганографії, адже контейнер – це шум, а повідомлення – сигнал.

Пропускна спроможність, стійкість до виявлення та робастність відіграють тут взаємопов'язану роль – покращення однієї з характеристик алгоритму, погіршує інші [10], саме тому жодний з алгоритмів не може бути абсолютно стійким до виявлення, повністю робастним та мати максимальну пропускну спроможність. Залежність методів від характеристик показана на рис. 1.

Рис. 1. Взаємопов'язана схема характеристик алгоритмів лінгвістичної стеганографії

Класифікація методів лінгвістичної стеганографії

1. Семаграми – приховують інформацію, використовуючи спеціальні позначки, які ледь помітні людському окові та сприймаються як чинні речі, наприклад, завитки на рукописних літерах або трохи змінені крапки у друкованому варіанті. Текстові семаграми приховують повідомлення, модифікуючи контейнер, змінюючи розмір літер або шрифт [5].

2. Використання «жаргонізмів» - деяких слів або словосполучень, зрозумілих для певної групи людей та не набутих осмисленням для інших. Використання певного «жаргонізму», попередньо знайденого в таблиці з підставленими бітами допомагає приховати невеликі повідомлення не визиваючи тривоги [5].

3. Метод зміни регістрів символів [5]. Даний метод пропонує кодування нульового біта повідомлення нижнім регістром, а одиничного біта – верхнім. Вміст файла-контейнера зчитується посимвольно та змінюється згідно з повідомленням. Кожна буква може містити один біт інформації, тож пропускна спроможність тут досягає ста відсотків. Алгоритм є базовим, тож стійкість до виявлення тут близька до нуля. Робастність також не забезпечується – при найпростішому форматуванні – переводі тексту в один регістр – повідомлення руйнується.

4. Метод додавання кінцевих пробілів. – здійснюється додавання в кінець строки другого пробілу для кодування одиничного біту та залишення одного пробілу для кодування нульового біту [6]. Пропускна спроможність залежить від кількості рядків у контейнері та є досить низькою – порядку 0.05 – 0.1%.

Стійкість до виявлення висока – заповнений контейнер достатньо непомітний для неозброєного ока. Робастність не забезпечується, адже навіть при друкуванні повідомлення руйнується, не кажучи вже про автоматичне форматування та видалення зайвих пробілів.

5. Модифікований метод додавання кінцевих пробілів – в кінці кожного рядка додається від нуля до п’ятнадцяти пробілів, кодуючи пів байт [6]. При правильному форматуванні контейнер залишається непідозрілим, а пропускна спроможність зростає у порівнянні з попереднім методом.

6. Однаковість написання символів. – ряд українських та англійських символів візуально не відрізняється, але вони мають різне позначення у ASCII-таблицях [6]. Пропускна спроможність визначається кількістю схожих символів, а їх майже половина, тобто, порядку п’ятдесяти відсотків. Стійкість до виявлення визначається характером обробки – заміна у текстових редакторах може підсвічуватися як помилка у написанні. Робастність досить висока – прості атаки на форматування не зруйнують повідомлення [11].

7. Допущення помилок в тексті – вставка в текст помилок навмисно для кодування кожного неправильно слова одиничним бітом, можна змінювати слова як на типові помилки, характерні для української мови – «е/и», «ш/щ», «у/ю», «з/с», «н/нн», так і на символ, що знаходиться поряд із замінюваним на клавіатурі, при невеликих об’ємах приховуваного повідомлення це залишається непомітним для людського ока [8]. При відсутності коротких слів у контейнері є можливість приховування одного біта в одне слово.

Для цього методу характеристики «якість приховування» та «співвідношення сигнал/шум» є обернено пропорційними.

8. Використання синонімів – маючи великий словник синонімів та зроблену з нього правильно підібрану таблицю для різних випадків, можна замінняти слова згідно з цією таблицею на потрібні для приховування повідомлення [8].

Змінювати можна хоч кожне слово, що забезпечую високу пропускну спроможність, виявлення неможливе без якого-небудь неточного використання синонімів, що може підштовхнути на думку про наявність прихованого повідомлення в тексті, але це лише у текстах, сформованих особисто, наприклад, будь-які заміни у загальновідомих літературних творах одразу ж розпізнаються. Робастність висока, адже будь-які зміни контейнера не призведуть до зміни тексту.

9. Застосування емодзі – піктограм, що зображують емоції [9]. У кожної емодзі є своє кодове уявлення, також на одну й ту саму емоцію доводиться порядку трьох – чотирьох емодзі. Шляхом виявлення синтаксично - емоціональної складової речення можна в кінці проставляти деякі з них, в залежності від приховуваного повідомлення, відсутність же емодзі відзначати нульовим бітом. Пропускна спроможність досить висока. Щодо виявлення – це малоймовірно. Робастність залежить від типу відображення та кодування операційної системи: деякі емодзі можливо замінити просто на квадрати, що призведе до знищення повідомлення.

10. Пунктуаційна варіативність – приховування даних у контейнері шляхом використання правил української мови при перерахуваннях, узагальнюваних словах та при зміні структури тексту, наприклад, - розбиття речення на два простих замість одного складного, щоб прибрати кому, та, навпаки, вставити цю кому, об’єднавши прості речення [9].

Також дієвим способом є заміна ком на сполучники при перерахуваннях та навпаки. Пропускна спроможність досить невелика, адже у порівнянні з кількістю символів, кількість розділових знаків є незначною, але це компенсується високою стійкістю до виявлення та робастністю.

Оцінка алгоритмів лінгвістичної стеганографії

Виконаємо аналіз існуючих методів та занесемо результати у таблицю (табл. 1), використовуючи такі критерії:

1. *Якість приховування*:

«2» – різниця між заповненим контейнером та контейнером без прихованого повідомлення не відчувається;

«1» – різниця помітна, якщо її шукати. «0» – наявність прихованого повідомлення можна побачити неозброєним оком.

2. *Робастність*:

«2» – після дій над контейнером повідомлення збереглося у повному обсязі;

«1»- після змін контейнера повідомлення можливо вилучити та прочитати, але з невеликими спотвореннями. «0» – повідомлення зруйноване.

3. *Пропускна спроможність*:

«2» – порядку 61-100%.

«1» – порядку 41-60%. «0» – порядку 11-40%

Таблиця 1 – **Оцінка алгоритмів лінгвістичної стеганографії**

Назва алгоритму	Оцінка 1	Оцінка 2	Оцінка 3	Загальна оцінка
Семаграми	1	0	2	3
Використання «жаргонізмів»	1	2	1	4
Метод зміни регістрів символів	0	0	2	2
Метод додавання кінцевих пробілів	2	0	0	2
Модифікований метод додавання кінцевих пробілів	2	0	1	3
Однаковість написання символів	1	2	1	4
Припущення помилок в тексті	1	1	1	3
Використання синонімів	2	2	2	6
Застосування емодзі	2	1	2	5
Пунктуаційна варіативність	2	2	1	5

Класифікація атак на лінгвістичні методи стеганографії

1. Найбільш розповсюджена та проста атака – суб'єктивна, а саме, спроба виявити наявність прихованого повідомлення «на око». Може застосовуватися лише для абсолютно незахищених стеганосистем. Тим не менш, вона найбільш розповсюджена на начальному етапі [9].

Першочерговий аналіз може містити у собі наступні пункти [12]:

1.1) первинне сортування стеганосистеми за зовнішніми ознаками;

1.2) виділення стеганосистеми з відомим алгоритмом вбудовування;

1.3) визначення використаних алгоритмів;

1.4) перевірка достатності обсягу матеріалів для стегоаналізу;

1.5) перевірка можливості проведення аналізу в окремих випадках;

1.6) фналітична розробка стегоматеріалів та методів зламу стеганосистеми;

1.7) виділення стегосистеми з відомими алгоритмами приховування але невідомими ключами.

2. Атака на основі відомого заповненого контейнера [6]. У цьому випадку несанкціонований користувач має одне або декілька стего, при цьому приховування повідомлення здійснювалося одним й тим самим способом. Задача полягає у виявленні факту наявності прихованого повідомлення та його вилучення або знаходженні ключа. Знаючи ключ, можливо провести аналіз наступних повідомлень.

3. Атака на основі відомого вбудованого повідомлення [6]. Цей тип атаки є характерним для систем захисту інтелектуальної власності, коли в якості водяного знаку використовується відомий логотип фірми. Задачею аналізу є отримання ключа. Якщо відповідний прихованому повідомленню заповнений контейнер – невідомій, то задача досить важко вирішується.

4. Атака на основі обраного секретного повідомлення [6]. У цьому випадку правопорушник має змогу пропонувати свої повідомлення та аналізувати отримані стего.

5. Адаптивна атака на основі вибраного секретного повідомлення [6]. Ця атака є частковим випадком попередньої, у цьому випадку правопорушник має змогу нав’язувати повідомлення, виходячи з аналізу попередніх стего.

6. Атака на основі вибраного заповненого контейнера [6]. Стегоаналітик має детектор стего у вигляді «чорної скриньки» та декілька стего. Задача полягає у знаходженні ключа.

7. Атака на основі відомого пустого контейнера[6]. Шляхом порівняння пустого контейнера з стего, стегоаналітик завжди може встановити факт наявності прихованого повідомлення.

8. Атака на основі вибраного пустого контейнера[6]. Зазвичай використовуються такі контейнери, приховати наявність повідомлення в яких досить важко.

9. Атака на основі відомої математичної моделі контейнера або його частини [6]. При цьому необхідно виділити різницю підозрілого повідомлення від відомої моделі. Задача приховування полягає у тому, щоб не пошкодити статистичну структуру контейнера.

Всі ці атаки мають одну особливість: вони не змінюють повідомлення та не спрямовані на протидію декодерові. В цьому їх позитивна сторона: вони навряд чи можуть насторожити відправника та отримувача.

Стеганосистема вважається зламаною, якщо порушнику вдалося, принаймні, довести факт існування прихованого повідомлення в перехопленому контейнері [13]. Передбачається, що порушник здатний здійснювати будь-які атаки і має необмежені обчислювальні можливості. Якщо йому не вдається підтвердити гіпотезу про те, що в контейнері приховане повідомлення, то стеганосистема вважається стійкою.

Ефективність розробленої стеганосистеми будемо досліджувати за наступними показниками:

1. За показником ємкості – це співвідношення розміру файлу-повідомлення до розміру файлу-контейнеру.
2. За часом приховування.
3. За часом вилучення.
4. За суб'єктивною оцінкою різниці між порожнім та заповненим контейнерами.
5. За показником ефективності – добутком першого та третього показників.

Контейнери класифікуватимемо за стилями сучасної української літератури:

1. *Художній стиль*. У ньому поєднано емоційність, образність та експресивність. В ньому зосереджується все багатство української мови з використанням неосяжної кількості розділових знаків та їх неоднозначним використанням.
2. *Науковий стиль*. Особливістю є використання термінів, точності та логічності. Менш багатий на пунктуацію за попередній стиль.
3. *Офіційно діловий стиль*. Це мова ділових паперів та законів, і хоч розділових знаків тут достатньо, та їх зміна буде доволі підозрілою.
4. *Публіцистичний стиль*. Зазвичай використовується в засобах масової інформації із застосуванням великого обсягу потрібних нам розділових знаків.
5. *Епістолярний стиль*. Особливістю є використання великої кількості вставних слів та форм ввічливості, що збільшує кількість пунктуаційних знаків.

Перейдемо до оцінки ефективності застосування представлених пустих контейнерів за показником ємкості. Графік залежності можна побачити на рисунку (рис. 2).

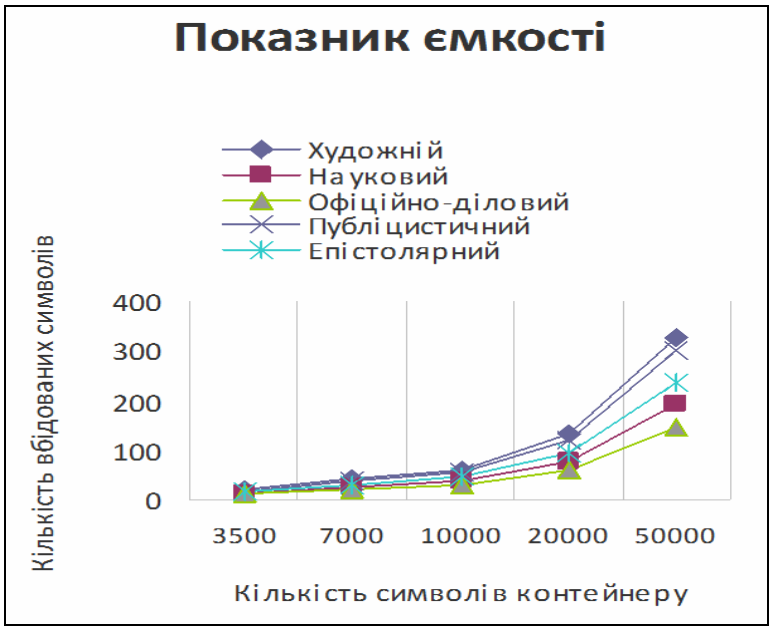

Рис. 2. Залежність показнику ємкості від збільшення повідомлення

Роздивившись уважно цей рисунок, можна зробити висновок, що для невеликих повідомлень до двадцяти символів однаково ефективно можна застосовувати будь-який з обраних за стилем пустий контейнер. З ростом вбудованого повідомлення можемо виявити залежність, а саме, що найбільш сприйнятливим для приховування є контейнер художнього стилю, на другому місці – контейнер публіцистичного стилю, на третьому – епістолярний, на четвертому – науковий, і останнє, п'яте місце посідає контейнер офіційно-ділового стилю.

Час приховування інформації – це час в мілісекундах, через який пустий контейнер стане заповненим. Основними компонентами є складність реалізації, тобто час на обробку правил вбудовування, пошук розділових знаків при зчитуванні контейнеру та заміна необхідних пунктуаційних знаків (рис. 3).

Розглянувши уважно ці графіки, можна зробити висновок, що тип контейнеру майже не впливає на час приховування, адже процедура вбудовування однакова для всіх типів контейнерів, різницю становить лише зчитування контейнеру, а саме, його необхідна кількість символів для приховування. Різниця на невеликих обсягах приховуваного повідомлення взагалі не відчувається і становить порядку секунди, з ростом об'єму повідомлення ця величина може сягати порядку до півхвилини.

Процедура зчитування відбувається шляхом посимвольного зчитування контейнеру та декодування розділових знаків із подальшим перетворенням бітової послідовності у текст. На рисунку (рис. 4) показано графік залежності часу від розміру приховуваного повідомлення для усіх типів контейнеру одночасно.

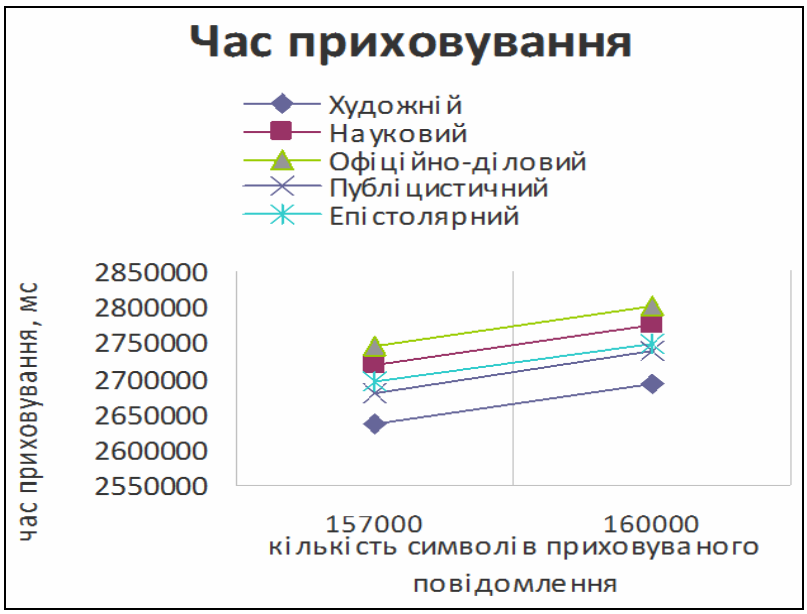

Рис. 3. Аналіз часових рамок процедури вбудовування

Проаналізувавши час, необхідний для вилучення повідомлення при використанні різних типів контейнерів, можна зробити висновок, що тип контейнеру не впливає на процедуру вилучення, адже процедура зчитування та декодування є однаковою для всіх типів.

Суб'єктивне оцінювання стеганосистем є найпоширенішим видом атак і полягає у самостійному, без використання технічного або програмного забезпечення, аналізуванні та прийняття рішення щодо наявності прихованого повідомлення у контейнері.

Для аналізу різниці пустого від заповненого контейнерів було запропоновано саме цю модель виявлення прихованого повідомлення.

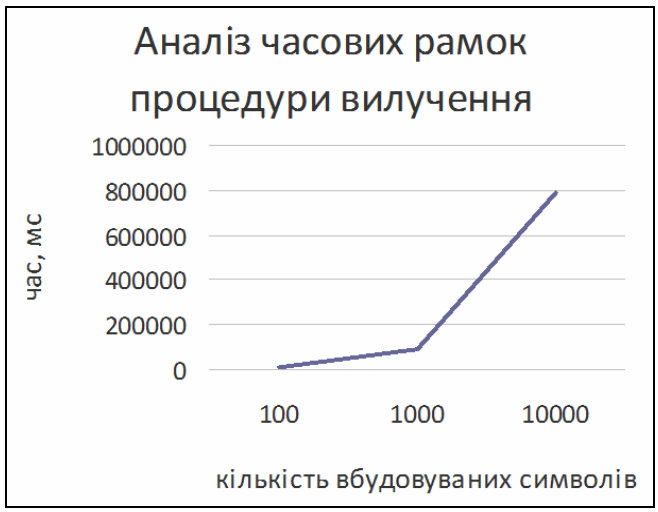

Рис. 4. Графік залежності часових рамок від кількості приховуваних символів для процедури вилучення повідомлення

Проведення порівняння здійснювалося як самостійно, так із залученням групи людей, було виявлено деякі закономірності:

1. Тип контейнеру впливає на виявлення прихованої інформації.
2. Виявлення факту наявності повідомлення «на око» прямо порційно залежить від ступеню знання пунктуаційних норм української мови дослідником.
3. Стійкість до виявлення залежить від кількості пробілів та розділових знаків у самому приховуваному повідомленні.

Пропозицією щодо підвищення стійкості до виявлення може слугувати більш детальний підхід до вибору типу текстового контейнеру або ж, самостійне його створення

Висновки

Характерною тенденцією в даний час в області захисту інформації є впровадження криптологічних методів. Однак на цьому шляху багато ще невирішених проблем, пов'язаних з руйнівним впливом на криптозасоби таких складових інформаційної зброї, як комп'ютерні віруси, логічні бомби,

автономні реплікативні програми. Об'єднання методів лінгвістичної стеганографії і криптографії є запропонованим виходом з положення, що створилося. У цьому випадку можна усунути слабкі сторони відомих методів захисту інформації і розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки. Проаналізувавши всі, нині відомі, методи лінгвістичної стеганографії та оцінивши засоби їхнього використання, було обрано синтаксичний метод на основі пунктуації для здійснення приховування інформації під час передачі даних від периферійних центрів до головного центру приймання і обробки інформації. Дослідження всіх методів у подальших дослідженнях допоможе характеризувати та структурувати межі застосування запропонованих методів у ГЦСК, виявити недоліки та переваги окремих алгоритмів та вибрати цікавий та неординарний напрямок для подальшого його реалізації та застосування за призначенням. Аналіз пунктуаційної варіативності української мови на другому етапі досліджень зможе дати поштовх для вибору методу кодування та вибору окремих розділових знаків для використання у процедурах приховування та вилучення повідомлення Практична цінність виконаної роботи полягає у використанні рекомендацій під час розробки алгоритмів вбудовування та вилучення інформації з можливістю їхнього подальшого вдосконалення. Проведений аналіз допоміг виявити можливі недоліки пунктуаційного методу. По-перше, це складність програмної реалізації, після якої заповнений контейнер повинен відповідати усім вимогам нормальної стеганосистеми. По-друге, це боротьба із пропускною спроможністю.

СПИСОК ЛІТЕРАТУРИ

1. Виноградов Ю. А. Комплексное применение сейсмического и инфразвукового методов регистрации волновых полей для выделения сигналов от наземных взрывов в процессе мониторинга природной среды в Евро-Арктическом регионе: Автореф. дис. канд. техн. наук. Москва, 2004, 26 с.
2. Дубровин В. И., Смирнов А. А. Совместное использование инфразвуковых и сейсмических данных для повышения точности локализации. Вестник НЯЦРК. 2011. Вып. 3. С. 140-144.
3. Андрущенко Ю. А., Гордієнко Ю. О. Аналіз ефективності застосування критеріїв ідентифікації вибухів та землетрусів для локальних та регіональних подій в умовах платформної частини України. Геофіз. журн. 2009. Т. 31. № 3. С. 121-129.
4. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко – К.: МК – Пресс, 2006 – 288 с.
5. Основи комп'ютерної стеганографії / Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. – В.: ВДТУ, 2003. – 143 с.
6. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев – М: САЛОН-ПЕСС, 2009 – 272с. (Серия «Аспекты защиты»).
7. Garces, M. A. Traveltimes for infrasonic waves propagating in a stratified atmosphere / M. A. Garces, R. A. Hansen, K. G. Lindquist // Geoph. J. Int., 1998. - P. 135, 255-263.
8. Beutelspacher A. Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Berlin: Springer-Verlag, 2009.
9. Потапова Р. К. Речь: коммуникация, информация, кибернетика. М.: Изд-во УРСС, 2010. 600 с
10. Лящук О. І., Андрущенко Ю. А., Гордієнко Ю. О., Карягін Є. В. Корнієнко І. В. Можливість використання даних інфразвукового моніторингу під час ідентифікації природи сейсмічних подій. Геофіз. журн. - 2015. - 37, № 6. - С. 105-114.
11. Gibbons S. J., Ringdal F., Kværna T., 2007. Joint seismic-infrasonic processing of recordings from a repeating source of atmospheric explosions. J. Acoust. Soc. Am. 122 (5), 158-164. doi: 10.1121/1.2784533
12. Wayner P. Strong Theoretical Steganography. – Berlin: Cryptologia, 2005. 410 p.
13. Асминг В. Э., Евтюгина З. А., Виноградов Ю. А., Федоров А. В. Анализ инфразвуковых сигналов, генерируемых техногенными источниками. Вестник МГТУ. 2009. Т. 12. № 2. С. 300-307.

Received (Надійшла) 22.11.2019
Accepted for publication (Прийнята до друку) 15.01.2020

The choice of linguistic steganography method for seismic events registration tasks

T. Koshel

Abstract. Today an important challenge for information security is the introduction of cryptological methods. However, there are many unresolved issues related to devastating impact on the cryptocurrencies of such components of information weapons as computer viruses, logic bombs, and standalone replication programs. The purpose of the article is to study the features of syntactic methods of linguistic steganography. In the course of the research the problems of effective use of forces and means of the MainVcenter Of Special Control during transfer for processing of data of seismic phenomena registration in near and far zones were solved. The object of the study is the punctuation method of hiding information in text containers. It is suggested to use a message hiding model in open-source text containers. It is possible by blocking unauthorized access to information by encrypting the message content. The subject of the study is the principles of embedding and removing messages by the implemented algorithm. Research methods are the formalization of theoretical information, comparative analysis and development of implementation methods. Attacks on steganographic systems are also considered and features of all attacks are highlighted. Preference was given to a punctuation-based syntactic method for concealing information while transmitting data from peripheral centers to the main receiving and processing center. The final results of the work provided for the implementation of the program embedding and removing messages to and from the container. A comparative analysis was conducted on the use of text container types and an analysis of the timeframe for embedding and retrieving procedures, and the possible disadvantages of the punctuation method. Such as the complexity of the software implementation, after which the filled container must meet all the requirements of a normal quilting system, and. difficulties in meeting bandwidth requirements.

Keywords: linguistic steganography, syntaxic methods, text containers, variativity of single signs, punctuation, coding.