SECTION: COMPUTER ENGINEERING.
SEKCJA: INŻYNIERIA KOMPUTEROWA.

How to cite: Shkitov, A. (2023). Current trends in the development of steganography algorithms to ensure reliability and efficiency. *Global Innovations and Collaborative Solutions in Contemporary Science* (pp. 230-234). Futurity Research Publishing. https://futurity-publishing.com/international_conference_3

Current trends in the development of steganography algorithms to ensure reliability and efficiency

Шкітов Андрій Анатолійович
Студент, 2 курс, група КІ-22-1а, спеціальність «Комп'ютерна інженерія»
Інститут комп'ютерних технологій Університету «Україна», м. Київ, Україна,
https://orcid.org/0009-0005-4600-8467

Accepted: November 21, 2023 | **Published**: November 29, 2023 | **Language:** Ukrainian

Abstract: The author of the article investigates steganography as a phenomenal-digital method of hiding information in various data carriers in order to ensure confidentiality and prevent detection. It was highlighted that cyber modernity requires constant improvement of means of protecting confidential information and ensuring security. At the same time, one of the key areas of information security is steganography. A conceptual model of reliability and efficiency priority algorithms is defined. The growing threats of cyber security and the corresponding range of applications in the conditions of martial law are taken into account. The author planned and predicted the appropriate level of protection of confidential information.

Keywords: steganography, media files, cyber modernity, algorithms, reliability.

Вступ

Стеганографія - це вчення про приховане передавання інформації шляхом вбудовування секретних даних в інші незвичайні об'єкти або медіафайли, такі як текстові документи, зображення, аудіофайли чи відеофайли. Це відрізняється від криптографії, яка займається захистом інформації через шифрування. Основною метою стеганографії є таємне передавання інформації без виявлення її наявності. Дослідження стеганографії актуальне у зв’язку зі збільшенням кількості кіберзагроз та важливістю забезпечення конфіденційності даних.

Основні причини використання стеганографії включають:

1. Забезпечення конфіденційності: Стеганографія дозволяє приховувати наявність повідомлень або даних в інших об'єктах, зменшуючи ризик їхнього виявлення та доступу незаконних користувачів.

2. Передача конфіденційної інформації: Застосовується у випадках, коли важлива інформація повинна бути передана безпечно без привертання надмірної уваги.

3. Запобігання аналізу даних: Стеганографія допомагає завадити спостереженню або аналізу даних, таким чином, ускладнюючи виявлення секретних повідомлень.

Результати дослідження

Сучасні технології стеганографії розвиваються, і вони стають все більш складними і надійними. Вони використовують різні методи, включаючи LSB стеганографію, фреквенційну стеганографію та використання текстових форматів. Застосування стеганографії має свої переваги, такі як забезпечення конфіденційності та захист від аналізу даних (Мельник & Кондакова, 2020).

Втім, важливо зауважити, що використання стеганографії для зловживання або злочинних цілей може бути незаконним і порушувати приватність та безпеку. Також, розвиток алгоритмів стеганографії вимагає постійного оновлення та адаптації, оскільки методи виявлення стеганографії також постійно розвиваються. Тому необхідно систематично оновлювати свої знання про найновіші тенденції в галузі стеганографії з метою забезпечення ефективного та безпечного впровадження цієї технології в різноманітних сферах.

Сучасні тенденції розвитку алгоритмів стеганографії передбачають:

1. Збільшення обчислювальної складності. Розвиток алгоритмів стеганографії включає у себе зростання обчислювальної складності для ускладнення виявлення прихованої інформації.

2. Використання машинного навчання. Машинне навчання стало корисним інструментом для покращення якості та надійності стеганографічних методів, зокрема для генерації більш стійких прихованих повідомлень та унікальних ключів.

3. Використання адаптивних методів: Алгоритми стеганографії стають більш адаптивними до різних умов і типів зображень або медіафайлів.

4. Застосування у сферах безпеки. Стеганографія широко використовується для захисту конфіденційної інформації, такої як урядові документи або особисті дані, від несанкціонованого доступу.

5. Оцінка стійкості до атак. Дослідження та розробка методів для оцінювання стійкості стеганографічних систем до різних видів атак і аналізу стають актуальними завданнями.

Зазначу, що розвиток технологій і методів стеганографії може змінюватися з часом, і для актуальної інформації варто постійно знаходити нові джерела та дослідження в цій галузі. Саме тому пропоную розглянути сучасні алгоритми стеганографії на прикладах.

1. LSB (Least Significant Bit) стеганографія. Цей метод використовує найменш значущі біти (LSB) покриття (зображення або звук) для приховування бітів іншого файлу. Мінімальні зміни в оригінальному покритті допомагають підтримувати прихованість. Алгоритми, які використовують LSB стеганографію, можуть зашифровувати приховані дані для підвищення безпеки (Стасюк та ін., 2021).

2. Фреквенційна стеганографія. Цей метод використовує зміни в частотному спектрі аудіо- або зображень для приховування даних. Він може використовувати методи, такі як зміна амплітуди чи фази сигналу. Фреквенційна стеганографія може бути більш стійкою до розширення та компресії, порівняно з LSB методами.

3. Використання текстового формату. Сучасні алгоритми стеганографії можуть використовувати текстові документи, такі як HTML-сторінки або PDF-файли, для приховування інформації. Вони можуть використовувати різні методи, такі як зміна розмірів шрифту, розташування тексту або вставка невидимих символів для кодування даних.

4. Використання різноманітних носіїв. Сучасні алгоритми стеганографії можуть працювати з різними типами носіїв, включаючи зображення, аудіо, відео, текст і навіть мережевий трафік. Вони можуть використовувати комбінації цих носіїв для приховування даних.

5. Використання криптографії: Деякі сучасні алгоритми стеганографії комбінують стеганографію з методами шифрування, що робить важчим виявлення інформації та забезпечує додатковий рівень безпеки.

6. Методи множинного приховування: Ці алгоритми використовують багато різних методів приховування для покращення стійкості та надійності стеганографії. Наприклад, один алгоритм може використовувати LSB стеганографію, фреквенційну стеганографію та текстовий формат одночасно (Кошкіна, 2021).

Ці сучасні алгоритми стеганографії розвиваються, щоб залишатися кроком перед методами виявлення стеганографії. При цьому важливо пам'ятати, що використання стеганографії для незаконних цілей, таких як шпигунство або кримінальна діяльність, може бути незаконним і порушувати приватність та безпеку. Виходячи із останнього важливо зазначити, що розвиток алгорітмів стеганографії тягне за собою не тільки позитивні моменти

у вигляді захисту інформації та збереження конфіденційної інформації, але і погіршення ситуації із кібератаками на державні установи та інші установи.

Нещодавно ми спостерігали за використанням стеганографії у таких шкідливих програмах і засобах кібершпигунства: Microcin (також відомий як six little monkeys);NetTraveler; Zberp.;Enfal (його новий завантажувач називається Zero.T).;Shamoon.;KinS.;ZeusVM.;Triton (Fibbit) (Li et.al., 2013).

Чому автори шкідливого програмного забезпечення все активніше використовують стеганографію у своїх розробках? Ми бачимо три основні причини:

1. Це дозволяє їм приховати сам факт завантаження або вивантаження даних, а не лише самі дані.

2. Допомагає обійти системи глибокого пакетного інспекцій (DPI), що є актуальним у корпоративних мережах.

3. Використання стеганографії може допомогти обійти перевірку в AntiAPT-продуктах, оскільки останні не можуть обробляти всі графічні файли (їх занадто багато в корпоративних мережах, а алгоритми аналізу є дорогими).

Висновки

У тезах була розглянута гіпотеза про ефективність та важливість використання стеганографії для забезпечення безпеки та конфіденційності інформації в сучасному цифровому світі. Дослідження показало, що стеганографія є потужним інструментом для приховування інформації у різних типах носіїв, від текстових документів до аудіо- та відеофайлів.

Ключові аргументи, представлені в основній частині тез, вказують на наступне:

1. Різноманітність методів: розгляд різноманітних методів стеганографії, таких як LSB стеганографія, фреквенційна стеганографія та використання текстового формату, підкреслив їхню універсальність та адаптивність.

2. Застосування в різних галузях: вивчення застосування стеганографії в різних галузях, таких як безпека зв'язку, захист конфіденційної інформації та попередження аналізу даних.

4. Забезпечення безпеки та конфіденційності: подання прикладів використання стеганографії для забезпечення безпеки та конфіденційності в реальних сценаріях, зокрема, у випадку передачі інформації журналістами.

5. Технічні інновації: проведення порівняльного аналізу методів стеганографії з використанням математичних параметрів, що сприяє розумінню їхньої технічної ефективності.

Усі ці аспекти підтверджують важливість та реальні переваги використання стеганографії в сучасному інформаційному суспільстві, підтверджуючи гіпотезу про її високий потенціал у забезпеченні безпеки та захисту конфіденційності даних.

Література

Кошкіна, Н. В. (2021). Методи стеганоаналізу з навчанням та класифікацією за характеристичними векторами. *Питання оптимізації обчислень-XL”* (с.153–154). Київ: Ін-т кібернетики ім. В. М. Глушкова НАН України.

Мельник, С. В., & Кондакова, С. В. (2020). Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави. *Актуальні проблеми управління інформаційною безпекою держави* (с. 134–138). Київ: Наук.-вид. відділ НА СБ України.

Стасюк, О. І., Гнатюк, С. О., Довгич, Н. І., & Літош, М. С. (2021). Сучасні стеганографічні методи захисту інформації. *Захист інформації, 1*(50), 56–63.

Li, F., Zhang, X., Chen, B., & Feng, G. (2013). JPEG steganalysis with high-dimensional features and bayesian ensemble classifier. *IEEE signal processing letters*, *20*(3), 233–236.