зловмисник легко, без особливих зусиль може їх використовувати в своїх інтересах.

Отже, на основі вищевикладеного можна зробити наступні висновки:

1. Інформація - це ресурс. Втрата інформації приносить моральні чи матеріальні збитки.

2. Умови, що сприяють неправомірному оволодінню інформацією, зводяться до її розголошенню, витоку і несанкціонованого доступу до її джерел.

3. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки системою захисту інформації, яка буде протидіяти загрозам через блокування неправомірних способів доступу та охоплювати усю множину існуючих способів за засобів захисту інформації

Перелік посилань

1. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту/ О. В. Черевко. // Ефективна економіка. – 2014. – №5. – Режим доступу: http://nbuv.gov.ua/UJRN/efek_2014_5_103

2. Інформаційна безпека. Навчальний посібник. Ч.1/С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

3. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 1999. – 30 с.

Метод приховування великого об'єму даних в файлах формату JPEG

Дацюк Р.М., Муляр І.В.
Хмельницький національний університет

Актуальність вивчення стеганографії постійно зростає, оскільки з поширенням персональних комп'ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу значної кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена розробці нових та вдосконаленню існуючих методів приховування даних. Кількість останніх постійно зростає з часом, але в сучасній науковій літературі [1] відсутня чітка класифікація таких методів, що ускладнює пошук і не дозволяє повною мірою оцінити рівень існуючих досягнень для їх подальшого ефективного використання.

Аналізуючи процес розвитку комп'ютерної стеганографії, можна сказати, що в найближчі роки інтерес до розробки її методів буде дедалі

більше зростати. Актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З іншого боку, швидкий розвиток інформаційних технологій дає можливість впроваджувати ці нові методи захисту.

Стеганографічні методи поряд із криптографічними займають важливе місце серед методів захисту інформації.

Але якщо в криптографії наявність зашифрованого повідомлення саме по собі привертає увагу зловмисника, то в стеганографії прихований зв'язок залишається невидимим, що робить організацію цього процесу досить актуальною.

Загальною особливістю стеганографічних методів є те, що приховане повідомлення або додаткова інформація вбудовується в якийсь нешкідливий, непомічений об'єкт або контейнер, в результаті чого з'являється повідомлення, яке потім відкрито транспортується до одержувача за каналом зв'язку. або зберігаються як такі

Але, більшість стеганографічних алгоритмів дозволяють приховувати невеликі об'єми інформації. Але на практиці часто виникає потреба в прихованій передачі значних масивів даних. Тому дослідження в напрямку розробки методу, що приховує великі об'єми інформації в відомих графічних форматах, для їх подальшої передачі є актуальним.

JPEG - можна сказати один з нових і досить потужних алгоритмів. Він працює на зонах 8x8, де яскравість і колір змінюються досить плавно. В результаті, коли матриця такої області розкладається на подвійний рядок уздовж косинусів, значущими є лише перші коефіцієнти. Таким чином, стиснення в JPEG відбувається за рахунок плавної зміни кольорів зображення.

Структуру JPEG-файлу зображено на рисунку 1.

Цей формат має таку універсальну структуру:

- Title (2 байти) : $ff, $d8 (SOI) (ідентифікується JPEG/JFIF файл);
- фрагмент APPO. Для JFIF файлів йде відразу за маркером SOI;
- довільна кількість "фрагментів" (подібні IFF (Image File Format) частинам);
- кінець (2 байти) : $ff, $d9 (EOI) [2].

Усі фрагменти мають таку структуру:

- Title (4 байти) :
- $ff ідентифікатор фрагменту
- n клас фрагменту (1 байт)
- sh, sl - розмір фрагменту.
- Вміст фрагменту, максимально 65533 байти.

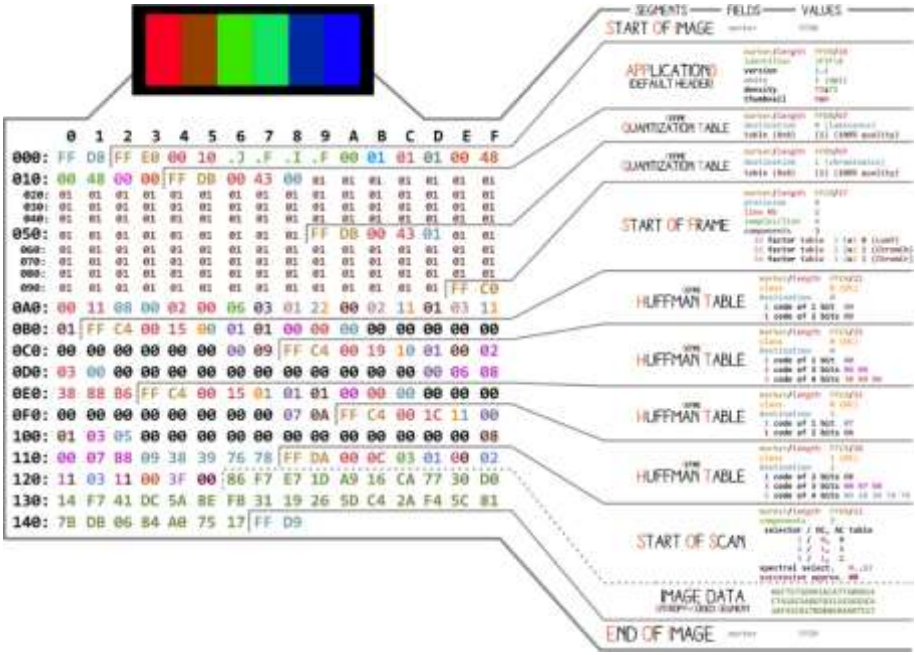

Рисунок 1 – Структура фомату JPEG

Майже кожен двійковий файл містить декілька маркерів (або заголовків). Можете вважати їх свого роду закладками. Вони вкрай важливі для роботи з файлом і використовуються такими програмами як file (на Mac і Linux), щоб ми могли дізнатися подробиці про фото. Маркери вказують, де саме в файлі зберігається певна інформація. Найчастіше маркери розміщуються відповідно до значення довжини (length) конкретного сегмента.

Стиснення даних JPEG (Joint Photographic Experts Group), що дозволяє стискати окремі (нерухомі, нерухомі зображення) зображення, можна розділити на три етапи [3]:

1 етап - трансформація та відбір кольорової інформації;

2 етап - блок дискретних косинусних перетворень (ДКП);

3 етап - квантування та кодування дискретних значень ДКП.

В результаті аналізу файлів JPEG було визначене, що структура JPEG- файлу нерегулярна. І хоча проаналізована вище структура маркерів відповідає в тому або іншому ступені будь-яким JPEG- файлам, але проте будь-якому узятому окремо JPEG- файлу властиві деякі відмінності. Наприклад, в якомусь JPEG- файлі визначена 1 таблиця квантування, і тому 1 блок даних сканування, в іншому файлі визначені декілька таблиць і декілька

блоків. Іноді з'являються JPEG- файли з маркерами перезапуску, що ускладнюють аналіз з поелементним розбором JPEG- структури. Крім того, JPEG- файл іноді зберігає зменшені копії зображень, призначених для попереднього перегляду. В цьому випадку розростається число сегментів даних зображення, що збільшує час при аналізі JPEG- файлу [4].

Отже, базуючись на розглянутій структурі формату JPEG, можна зробити висновки, що є маркери, що визначають сегменти, але що не беруть участі в JPEG- перетворенні. А тому вони не впливають на візуалізацію зображення. І природно вони ігноруються програмою перегляду. Перерахуємо їх:

1. COM;
2. APP15;
3. DAC;
4. DNL;
5. SOF2 - SOF10;
6. Неспецифіковані сегменти.

Розроблений алгоритм, використовуючи специфіку формату для приховування використовує перераховані маркери. Атже фрагменти, які позначаються перерахованими маркерами, дозволяють записувати певні дані. Але необхідн враховувати обмеженість об'єму сегменту, який задається двома байтами - OxFFFF.

Розглянемо основні етапи розробки даного методу:

Згідно до вимог, до впровадження приховані данні мають бути зашифровані і стиснуті. Потім необхідно врахувати параметри впровадження і об'єм стегоконтейнера.

Так як у форматі JPEG реалізовано стиснення з втратами, то потрібно реалізувати ряд попереджувальних заходів при впроваджені прихованих данних, щоб їх вберегти від спотворення [5].

Спочатку відбувається перетворення JPEG- файлу у BMP-файл (потік даних). В результаті відбувається збільшення розміру потоку даних через зміни кодування інформації про колір різних ділянок початкового зображення. Але з огляду на те, що в BMP- форматі піксель закодований 3 байтами, що відповідають за вклад основних кольорів (R - червоного, G - зеленого і B - синього) в підсумковий колір пікселя, розмір потоку збільшується досить помітно і тому дає можливість впровадження великого об'єму інформації.

Структура алгоритму запису прихованих даних зображено на рис. 2

З метою мінімальної зміни просторової області, реалізована стеганосистема за умовчанням використовує тільки молодший біт такого байта. Це дозволяє отримати мінімальну вірогідність виявлення детектування навіть на зображеннях з великою площею заливки синього кольору.

Рисунок 2 - Алгоритм запису прихованих даних

Отже, розроблений алгоритм орієнтований для вирішення завдання прихованої передачі даних. Він, як і будь-який інший стеганографічний алгоритм може виконувати процедури впровадження/витягання інформації. Такою інформацією бувають ідентифікаційні номери, ЦВЗ і так далі. Істотною і дуже корисною властивістю є автоматизація функціональності по впровадженню/вбудовуванню і дружність програмної реалізації стеганоалгоритма по вхідних/вихідних параметрам.

Перелік посилань

1. Юдін О. К. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О. К. Юдін, Р. В. Зюбіна, О. В. Фролов // Радиоэлектроника и информатика. — Х. : НХНУРЕ, 2015. — № 3. — С. 24-31.

2. Steganography and Digital Watermarking: a global view [Електроний ресурс] - Режим доступу до ресурсу: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/proiect.pdf.

3. LSB стеганография [Електроний ресурс]. - 2019. - Режим доступу до ресурсу: https://habr.eom/ru/post/112976

4. Рейда О.В. Аналіз та дослідження форматних стеганоалгоритмів на основі графічних контейнерів / Рейда О.В., Джулій В.М. // Тези доповідей Всеукраїнської науково-практичної конференції "Інтелектуальний потенціал – 2018". – 2018 – С. 86-90.

5. Cristi Cuturicu, JPEG - Алгоритм стиснення, Code Net [Електронний ресурс] / Формати файлів, - Режим доступу: http://www.codenet.ru/progr/forrnt/jpeg_00.php

Метод створення віртуальних полігонів на основі технологій хмарних обчислень системи управління базами даних

Джулій В.М., Лукін В.С., Чешун В.М.
Хмельницький національний університет

При виконанні дослідження було поставлено наступні задачі:

– дослідження і вибір існуючих систем, придатних для реалізації цілей і задач цієї роботи;

– проектування апаратно-програмного комплексу, включаючи дослідження і побудову всіх його підсистем;

– створення працюючого прототипу апаратно-програмного комплексу;

– визначення ефективності прототипу.

В рамках поставлених завдань розроблені наступні підсистеми апаратно-програмного комплексу та забезпечено їх взаємодію для виконання цілей цієї роботи:

– обчислювальна підсистема (система віртуалізації);

– мережева підсистема;

– система зберігання даних;

– система автоматизації надання послуг та забезпечення універсального доступу.

Для вирішення поставлених завдань розроблена архітектура інфраструктури віртуальних полігонів.