УДК 681.3.016: 004.633.3

МЕТОД НАДЛИШКОВОГО ПРЕДСТАВЛЕННЯ ТА ЗБЕРЕЖЕННЯ ДАНИХ У ГРАФІЧНИХ КОНТЕЙНЕРАХ

Бельська В.Ю., ст. викл., Костенко П.П., асп., Сухарев О.Є., студ., Шевченко В.О., студ.
Кременчуцький національний університет імені Михайла Остроградського
вул. Першотравнева, 20, 39600, м. Кременчук,Україна
E-mail: ppkostenko@gmail.com, sambademon@gmail.com, vetal.44@meta.ua

Розглядається розробка стеганографічної системи надлишкового представлення даних у зображеннях динамічного кодування. Збереження даних у графічних об'єктах, зокрема JPEG. Викладено функціональні особливості розробленого програмного додатку, його переваги та недоліки в порівнянні з існуючими аналогами. Спектральний аналіз підтвердив ідентичність пустого та заповненого контейнерів, низьку ймовірність факту виявлення наявності інформації. Розглянуті перспективи подальшого розвитку програмного додатку.

Ключові слова: стеганографія, криптографія, контейнер, зображення, JPEG2000.

Вступ. Стрімкий ріст розповсюдження інформаційних технологій значно погіршує захист інформації. Криптографічні методи захисту втрачають свою надійність унаслідок надвисоких розрахункових можливостей комп'ютерних технологій. Розрахункові потужності апаратного та нейро-мережеві технології програмного забезпечення здатні розкодувати передові криптосистеми. Можливим вирішенням цієї проблеми є застосування технологій приховування інформації в інформаційних контейнерах, що дозволяє ввести в оману зловмисника та зберегти конфіденційність даних. Інформаційним контейнером може виступати будь-яка інформація, доступна загальній аудиторії: фото-, відеозображення, електронні підручники, аудіо-файли. Стеганографічний захист дозволяє приховати факт наявності конфіденційної інформації при її передачі каналами зв'язку. При такому захисті можна зменшити ймовірність виявлення в перехопленому повідомленні іншого повідомлення, що призведе до неможливості виникнення будь-яких сумнівів з приводу наявності прихованої інформації.

Аналіз попередніх досліджень. Актуальні питання стеганографічого збереження інформації та ефективні алгоритми приховування були розглянуті в роботах [1-3]. Питання термінології та формування основних стеганографічних протоколів розглянуті в роботах B. Pfitzmann, B. Schneier, S. Craver [4-6]. Описані алгоритми отримали реалізацію в програмному забезпеченні, комплексах математичних розрахунків і моделювання MathCAD, MatLAB.

На даний момент існує спектр програмного забезпечення, що використовує засоби стеганографії для впровадження конфіденційних даних у графічні, аудіо- й відеофайли. Існує багато програмних додатків, які використовуються для цілей стеганографії й призначені для внесення інформації до медіафайлів.

Найбільш популярні з них: Gif-It-Up 1.0 for Windows 95, EZStego (Java), DiSi-Steganograph DOS-додаток, Hide and Seek, MP3Stego, Steganos, Steganography Tools 4, steghide. Порівняння характеристик розглянутого вище програмного забезпечення представлено в табл. 1.

Таблиця 1 – Порівняння характеристик програмного забезпечення для захисту електронних файлів

Назва	Опис програми
Gif-It-Up 1.0 for Windows 95	Приховує дані в GIF файлах, виконуючи підстановку прихованих кольорів зображення
EZStego Java-додаток	Модифікує найменш значимі біти (LSB) яскравості точок GIF та PICT, змінюючи їх кольорову палітру
DiSi-Steganograph DOS-додаток	Приховує дані в файлах PCX
Hide and Seek	Приховує дані в GIF файлах, приховані дані кодує алгоритмом шифрування Blowfish. Виконує випадковий вибір точок для зберігання доданих даних
MP3Stego	Додає дані до звукових файлів формату MP3
Steganos	Програма з асистентом (Wizard) кодує і приховує файли в форматах DIB, BMP, VOC, WAV, HTML
Steganography Tools 4	Попередньо кодує дані за допомогою алгоритмів шифрування IDEA, MPJ2, DES TripleDES і NSEA, а потім приховує їх у графічних файлах, звукових (WAV) файлах або вільних секторах флопі-дисків
Steghide	Steghide - стеганографічна програма, призначена для приховування даних до зображень та аудіофайлів. Колір відповідно до зразкового зображення не змінюються, що підтверджуються стійкістю статистичних тестів частотного аналізу зображень

Стеганографічні технології використовуються не лише для приховування конфіденційної інформації. Зловмисниками, наприклад, розроблено вірус "W32 / Perrun", який "приховує" своє тіло об'ємом 18 К у файлі *.jpg [7].

У зв'язку зі складністю поєднання корисної інформації з графічним контейнером формату *.jpg, що обумовлено алгоритмом компресування зображення, наразі відомо про існування лише одного представника стеганографічного програмного забезпечення steghide, функціональні характеристики якого дозволяють ін'єкціювати дані до файлу *.jpg. Головним недоліком розглянутого додатку є консольний інтерфейс користувача та складність використання на платформі Microsoft Windows.

У зв'язку із загостренням проблеми конфіденційності та захисту інформації від зловмисників, актуальною задачею є розробка кросс-платформеного програмного забезпечення, здатного ін'єкціювати дані до файлу *.jpg.

Мета роботи. Розробка методики надлишкового представлення даних у зображеннях динамічного кодування.

Матеріал і результати дослідження. На відміну від криптографії, стеганографія призначена для приховування самого факту наявності інформації.

Саме стеганографія (грец. – тайнопис) вивчає методи та засоби приховування інформації. Методи та засоби приховування інформації в електронних файлах відносяться до комп'ютерної стеганографії.

Основними стеганографічними поняттями є повідомлення й контейнер**.** Повідомленням $m \hat{I}\ M$ називають секретну інформацію, наявність якої необхідно приховати, де M – множина всіх повідомлень. Контейнером $b \hat{I}\ B$ називають не секретну інформацію, яку використовують для приховування повідомлень, де B – множина всіх контейнерів. Пустий контейнер (контейнер-оригінал) – це контейнер b, що не містить у собі повідомлення, заповнений контейнер (контейнер-результат) b_m – це контейнер b, що містить повідомлення m.

Стеганографічним перетворенням вважають залежності F и F^{-1} виду:

$$F: M \acute{}\ B \acute{}\ K \circledR B,\quad F^{-1}: B \acute{}\ K \circledR M, \qquad (1)$$

які відповідають трійці (повідомлення, пустий контейнер, ключ із множини К) контейнер-результат, та парі (заповнений контейнер, ключ із множини К) вхідне повідомлення, тобто:

$$F(m, b, k) = b_{m,k},\ F^{-1}(b_{m,k}) = m, \qquad (2)$$

де m∈ M, b,b_m∈ B, k∈ K.

Стеганографічною системою називають $(F,\ F^{-1},\ M, B, K)$ – співвідношення повідомлень, контейнерів та перетворень, що їх поєднують.

Аналіз практично застосованих методів комп'ютерної стеганографії дозволяє виділити наступні основні класи:

1. Методи, що базуються на наявності вільних проміжків в представлення / збереження даних.

2. Методи, що базуються на принципі надлишкового представлення / збереження даних.

3. Методи, що базуються на застосуванні спеціально розроблених форматів представлення / збереження даних.

Варто зауважити, що методи внесення прихованої інформації в об'єкти залежать, перш за все, від призначення й типу об'єкту, а також від формату, в якому представлені дані. Тобто для будь-якого формату представлення комп'ютерних даних можуть бути запропоновані власні стеганографічні методи [8].

Наразі програмне існуюче забезпечення не має функціональних можливостей приховування інформації до зображень типу *.jpg, крім програми Steghide. Проте до недоліків Steghide варто віднести:

– консольний інтерфейс користувача;

– перевантаження ключами налаштування роботи;

– відсутність алгоритму кодування інформації при занесенні до контейнеру;

– не передбачено використання динамічних крипто-ключів та їх захист;

– додаток не підтримує платформу MacOS X.

Тому було прийняте рішення розробити програмний додаток TextHide для надлишкового представлення даних у зображеннях динамічного кодування з простим графічним інтерфейсом та можливістю обробки *.jpg файлів. Програмно реалізовано наступні функції:

– приховування даних у *.jpg *.jpeg *.bmp *.png *.gif *.tiff *.jpe файлах;

– кодування даних за файлом-ключем;

– кодування ключа методами «Цезаря» та «простої перестановки»;

– декодування приховуваної інформації.

Для реалізації підтримки крос-платформеності програмного додатку розробка проводилась в середовищі Qt Creator 2.0.1. Це дозволило реалізувати зручний, інтуїтивно зрозумілий інтерфейс (рис. 1) для полегшення ручної роботи з додатком.

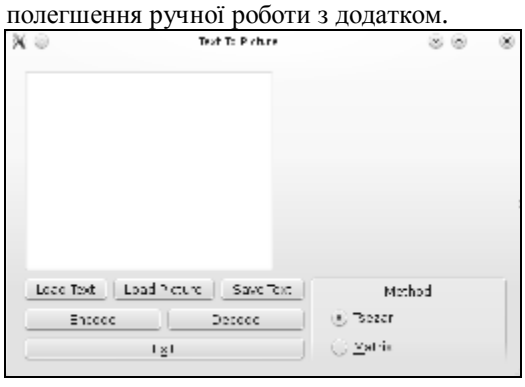


Рисунок 1 – Головне вікно TextHide

Головне вікно складається з двох блоків - «Encode» і «Decode». Відповідно перший – блок, призначений для приховування текстової інформації у відкрите графічне зображення. Другий блок використовується для видобування текстової інформації з графічного файлу.

Передбачено два майстра кодування та декодування, що викликаються кнопками «Encode» і «Decode». Умовою запуску майстра слугує відсутність завантажених до додатку контейнера та даних. На рис. 2 наведено загальну схему роботи програми.

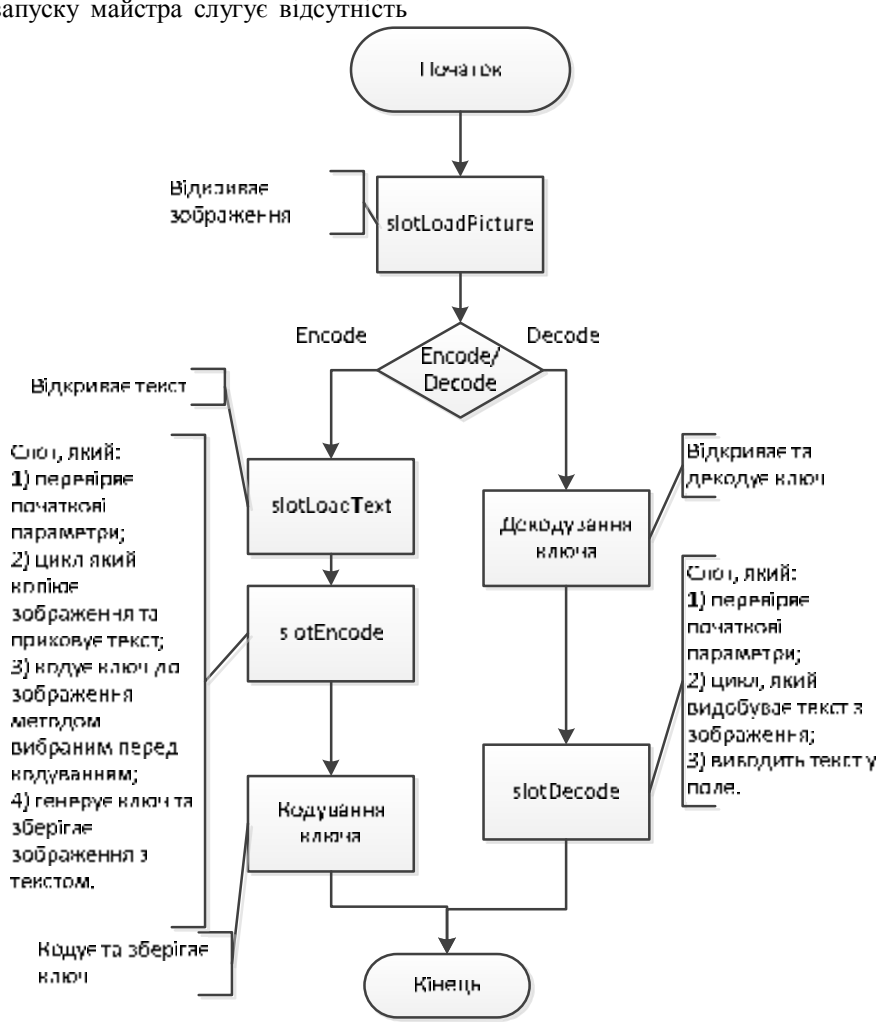


Рисунок 2 – Загальна блок-схема роботи програми

TextHide складається з 2 слотів (методів): слот приховування тексту у зображенні, слот видобування тексту із зображення, а також двох функцій: кодування та декодування ключа. Слот приховування тексту реалізовано з урахуванням особливостей jpg зображень, він підтримує приховування тексту з кодуванням Utf-8.

```
for( int j=0,i=0;i< file_r.size();i++)
 {  in >> a; if(j<by.length())  if(i!=0) if (i>file_r.size()/2)
if(i%krok==0)
{  ch=by[j];  a=ch;  ++j; }
 else
{ch=(unsigned char)((rand()%255)+1);
 a=ch;  }
out << a; in >> a;
if(i>file_r.size()/2)
   { ch=(unsigned char)((rand()%255)+1); a=ch;}
out << a;}
```

Лістинг 1 - Механізм кодування даних до контейнеру

Особливу увагу варто звернути на механізм кодування даних до контейнеру, який наведено в лістингу 1.

У методі кодування виділяються три головних елементи:

– функція перевірки початкових даних,яка перевіряє наявність зображення та тексту;

– функція вирахування кроку;

– цикл приховування тексту.

Всі функціональні особливості TextHide спрямовані на коректне приховування тексту у jpeg файли, з тим, щоб не пошкодити зображення та надійно приховати текстову інформацію. Для підсилення стеганографічної стійкості генерується випадковий символ, що дозволяє надійно приховати корисну інформацію, та кодується ключ кодування даних.

За допомогою розробленого додатка було проведено ряд експериментів. Закодовано текст «*Наш навчальний заклад став першим на Полтавщині класичним університетом. Раніше він мав статус профільного ВНЗ, тобто у його назві було визначення "політехнічний". Згідно з розпорядженням Каб-*

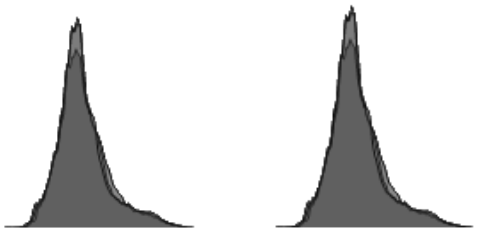
міну він набуває статусу класичного університету. Проект нового Закону України "Про освіту" визначає, що класичний університет створюється за умови, якщо у ньому за денною формою навчається не менше ніж шість тисяч студентів не менше ніж за вісьмома галузями освіти і здійснюється підготовка наукових кадрів не менше ніж за вісьмома галузями освіти і здійснюється підготовка наукових кадрів не менше ніж з восьми наукових спеціальностей. «*Наш університет має статус класичного*». *Політехнік №5 (68), серпень 2009 р.*» до зображення рис. 3.

Рисунок 3 – Оригінал зображення JPEG
(Розмір 350x219) 54,1 Kb

Результатом кодування є заповнений контейнер (рис. 4) і файл-ключ із записом: «骾_aM^^b^». Внаслідок кодування розширення зображення та його якість залишились без змін, що підтверджується спектральним аналізом (рис. 5).

Рисунок 4 – Зображення після обробки
програмою

Пустий контейнер мав розмір 54,1 КБ, заповнений контейнер – 108 КБ, при розмірі тексту 1,12КБ. У ході проведення другого досліду було закодовано 50% тексту першого досліду, тобто 0,56 КБ. У результаті заповнений контейнер мав розмір 108 КБ. Це доводить, що розмір вихідного контейнера не залежить від розміру тексту. Така особливість дозволяє приховувати різні інформаційні блоки в однакових контейнерах при високій ймовірності надійності захисту даних.



До Після

Рисунок 5 – Спектри пустого
та заповненого контейнерів

До недоліків програми можна віднести:

– надлишкове кодування даних;

– обмежену кількість даних, що можна приховати до графічного файлу, яка залежить від початкового розміру інформаційного контейнеру.

Перспективним у подальшому розвитку вбачається реалізація додаткових алгоритмів кодування ключа, кодування ключа ітераційними шифрами, внутрішнє кодування даних до занесення в контейнер, використання в якості контейнера відео- та аудіофайлів.

Висновки. Розроблено програмний додаток для надлишкового представлення даних в зображеннях динамічного кодування. На відміну від існуючих стеганографічних програмних продуктів розроблена система дозволяє додавати дані до будь-яких графічних файлів, зокрема JPEG формату. Застосування отриманого програмного продукту дозволяє приховувати дані до графічних контейнерів з високою надійністю. Порівняльний аналіз спектральних характеристик не дозволяє виявити зміни в зображенні. Розміщення різної за змістом та кількістю інформації не призводить до зміни розширення та розміру контейнеру. Суттєвими перевагами створеної утиліти є приховування даних в *.jpg *.jpeg *.bmp *.png *.gif *.tiff *.jpe файлах, кодування даних за файлом-ключем, кодування ключа, кросплатформеність (підтримка: Mac OS X, Microsoft Windows, Linux/X11, Windows CE, Symbian, MeeGo). До недоліків програми можна віднести надлишкове кодування даних, що за наявності пустого контейнеру дозволить виявити факт присутності даних у файлі та обмежену кількість даних, що можна приховати до графічного файлу, яка залежить від початкового розміру інформаційного контейнеру. Подальший розвиток вбачається в підсиленні крипто-стійкості алгоритмів кодування ключа, реалізації внутрішнього кодування даних до занесення в контейнер, використання потокових типів даних в якості контейнера.

ЛІТЕРАТУРА

1. Gustav J. Simmons, The Prisoner`s Problem And The Subliminal Chanel, Advances in Cryptology: Proceedings of Workshop on Communications Security (Crypto`83, David Chaum, ed.), Plenum press 1984. – С.51-67.

2. Gustav J. Simmons, The History of Subliminal Channels, // IEEE Jiurnal on Selected Areas of Communications. – 1998. – Vol.16, № 4. – C. 452-461.

3. J. Fridrick, R.Du, M. Long, Steganoalysis of LSB Encoding in Color Images, Proceedings of ICME 2000, New York, USA.

4. B. Pfitzmann, Information Hiding Terminology. In: Information Hiding, Springer Lecture Notes in Computer Science.

5. B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code 2nd ed. New York // John Wiley and Sons, 1996.

6. S. Craver. On Public-Key Steganography in the Presence of an Active Warden // Technical report RC 20931, IBM, 1997, 13c.

7. Анализ методов защиты информации. – Режим доступа: http://www.masters.donntu.edu.ua /2007/fvti/mikhayluk/diss/index.htm.

8. Стеганография и стегоанализ. Обзор существующих программ. – Режим доступа: http://users.livejournal.com/ zauberer /11819.html.

9. Шлее Макс «Qt4.5.Профессиональное программирование на C++ / Макс Шлее. – БХВ-Петербург, 2010. – 896 с.

10. Лишнер Рей C++ Справочник / Лишнер Рей. – СПБ.: Питер, 2005. – 907 с.

11. Гатчин Ю. А. Основы криптографических алгоритмов. Учебное пособие / Ю. А. Гатчин, А. Г. Коробейников. - СПб.: СПбГИТМО(ТУ), 2002.

12. Josef Pieprzyk Fundamentals of Computer Security. — Springer, 2003. — P. 6.

13. JPEG. – Режим доступа: http://ru.wikipedia.org/wiki/JPG

14. Аграновский А. В. Практическая криптография: алгоритмы и их программирование / А. В.Аграновский, Р. А. Хади. – М.: СОЛОН-Пресс, 2009. – 256 с.

Стаття надійшла 29.11.2010 р.
Рекомендовано до друку к.т.н., доц. Чорним О.П.

МЕТОД ИЗБЫТОЧНОГО ПРЕДСТАВЛЕНИЯ И СОХРАНЕНИЯ ДАННЫХ В ГРАФИЧЕСКИХ КОНТЕЙНЕРАХ

Бельская В.Ю., ст. преп., Костенко П.П., асп., Сухарев О.Є., студ., Шевченко В.О., студ.
Кременчугский национальный университет имени Михаила Остроградского
ул. Первомайская, 20, 39600, г. Кременчуг, Украина
E-mail: ppkostenko@gmail.com,sambademon@gmail.com,vetal.44@meta.ua

Рассматривается разработка стеганографической системы убыточного представления данных в изображениях динамического кодирования. Сохранение данных в графических объектах, в частности JPEG. Изложены функциональные особенности разработанного программного приложения, его преимущества и недостатки по сравнению с существующими аналогами. Спектральный анализ подтвердил идентичность пустого и заполненного контейнеров, низкую вероятность факта выявления наличия информации. Рассмотрены перспективы дальнейшего развития программного приложения.

Ключевые слова: стеганография, криптография, контейнер, изображение, JPEG2000.

METHOD OF THE REDUNDANT REPRESENTATION AND SAVED DATA TO THE GRAPHIC CONTAINER

Belska V., Sen. Lect., Kostenko P., post-grad., Sukharev A., stud., Shevchenko V., stud.
Kremenchuk Mykhailo Ostrohradskyi National University
vul. Pershotravneva, 20, 39600, Kremenchuk, Ukraine
E-mail: ppkostenko@gmail.com, sambademon@gmail.com,vetal.44@meta.ua

The article deals with the steganography system in the dynamic coding images with losing data. Storing data in graphic objects, in particular JPEG. Described functional of the developing software application, its advantages and disadvantages in comparison with existing analogues. Spectral analysis confirmed the identity of the empty and filled containers, a low probability of detection of the fact of availability of information. The prospects for further development of application software.

Key words: steganography, cryptography, container, image, JPEG2000.