УДК 004.891

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Джулій В.М.** (ХмНУ)
к.т.н., с.н.с. **Мірошніченко О.В.** (ВІКНУ)
Бойко Б.О. (ХмНУ)

МЕТОД ПЕРЕДАЧІ ПРИХОВАНОЇ ІНФОРМАЦІЇ БЕЗ СПОТВОРЕННЯ РАСТРОВОГО ЗОБРАЖЕННЯ

У статті запропонований метод передачі прихованої інформації без спотворення растрового зображення. На основі проведеного аналізу наведено поняття прихованого каналу передачі інформації, а також класифікація методів і завдань прихованої передачі інформації.

Проведено огляд існуючих методів впровадження інформації в растрові зображення. Наведено аналіз існуючих програм впровадження інформації в растрові зображення, виявлено їх переваги та недоліки. Розглянуті можливі області застосування стеганографії, зокрема-стеганографія може бути використана для зберігання і розподілення ключів в мережах зв'язку. Виявлені недоліки методів впровадження інформації в растрові зображення і їх програмні реалізації не дозволяють в повній мірі використовувати їх для безпечної передачі інформації. Для усунення виявлених недоліків запропонований метод передачі прихованої інформації без спотворення растрового зображення, який дозволяє із зображення і файла даних, отримати файл-ключ пікселів, за допомогою якого можна буде витягнути файл даних із початкового растрового зображення, без спотворення растрового зображення. При необхідності існує можливість побітово зашифрувати файл-ключ в початкове растрове зображення, в даному випадку при створенні файл-ключа, останній байт пікселя не індексується, тому що він буде змінений.

Для організації прихованого каналу зв'язку, розподілу і передачі ключової інформації запропонований метод, що на відміну від розглянутих, має високу пропускну здатність. Файл-ключ пікселів стискається і зберігається в форматі результуючого растрового зображення. Через низьку ентропію файл-ключа пікселів, він буде мати набагато менший розмір, ніж початкове растрове зображення. При необхідності існує можливість шифрування файл-ключа пікселів методом симетричного шифрування або RSA, що значно підвищить стійкість до атак - впроваджена інформація може піддаватися злому, видаленню чи атакам. Стійкість є головною вимогою, що висувається до будь яких стеганографічних методів, а також забезпечить секретність вбудованої інформації.

Ключові слова: стеганографія, стеганографічні методи, файл-ключ, растрове зображення, прихований канал зв'язку, захист інформації, стегоключ.

Вступ. Зростаючі можливості сучасних засобів зв'язку вимагають розробки спеціальних засобів безпечного зберігання та передачі інформації. Мережева безпека стає все більш актуальною через зростаючий обсяг даних, що передаються по локальних і глобальних мережах. Для захисту інформації від несанкціонованого доступу та використання необхідне забезпечення конфіденційності і цілісності даних. В області комунікації безпека є однією із головних проблем сучасного світу. Найрізноманітніші методи захисту інформації та алгоритми приховування даних були розроблені в останні десятиліття. Стеганографічні програмні засоби приховування інформації забезпечують перевагу перед іншими видами програмної інформаційної безпеки, оскільки текст ховається у зображенні, яке не сприймається як носій текстової інформації. Стеганографія може бути визначена як мистецтво і наука про невидиму комунікацію. Це реалізується приховуванням інформації в іншій інформації, таким чином, відбувається приховування існування переданої інформації. Хоча поняття стеганографії та криптографії схожі, але все ж стеганографія відрізняється від криптографії. У криптографії основна увага приділяється шифруванню даних, в стеганографії основна увага приділяється приховуванню самого факту присутності даних. Стеганографія та криптографія – це способи захисту інформації від несанкціонованого доступу, але ці технології окремо не досконалі, і можуть бути скомпрометовані. Як тільки наявність

прихованої інформації виявляється, або якщо виникне якась підозра, то стеганографія частково зазнає поразки. Ефективність стеганографії можна підсилити шляхом об'єднання її з криптографією. Різні програмні додатки використовують різні формати графічних файлів. Серед усіх графічних форматів найпопулярніший в Інтернеті формат JPEG із-за малих розмірів зображення.

Відносно обчислювальної техніки виділився окремий напрям стеганографії - комп'ютерна стеганографія**.** В якості контейнерів тут використовуються файли різних форматів, мережеві пакети і т.д. Наприклад, інформацію можна впровадити в графічне зображення. Найпоширеніший спосіб LSB (Least Significant Bit), при якому замінюються наймолодші біти контейнера на біти приховуваних даних. Існують декілька видів даного підходу з використанням растрового зображення як контейнера.

BlindHide - найпростіший алгоритм: дані записуються, починаючи з верхнього лівого кута зображення до правого нижнього – піксель за пікселем. Приховані дані програма записує у наймолодших бітах кольорів пікселя. Приховані дані розподіляються у контейнері нерівномірно. Якщо приховані дані не заповнять повністю контейнер, то лише верхня частина зображення буде спотвореною.

Hideseek - алгоритм у псевдовипадковий спосіб розподіляє приховане повідомлення у контейнері. Для генерації випадкової послідовності використовується пароль. Дещо «розумніший» алгоритм, але все ж не враховує особливостей зображення-контейнера.

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

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

Інші методи приховування інформації в графічних файлах орієнтовані на формати файлів з втратою, наприклад, JPEG. На відміну від LSB вони більш стійкі до геометричних перетворень. Це відбувається за рахунок варіювання в широкому діапазоні якості зображення, що призводить до неможливості визначення джерела зображення.

Модель каналу з прихованою передачею інформації. Стеганографія, як наука, визначається наступним чином - це науковий напрям, що вивчає способи прихованої передачі або зберігання інформації, при цьому прихований канал зв'язку організовується на основі відкритого каналу зв'язку з урахуванням особливостей сприйняття інформації. Існують три напрямки стеганографії для організації прихованого каналу передачі інформації: класичний - приховування інформації в потоках даних так, щоб неможливо було виділити або виявити якусь приховану складову частину; комп'ютерний - приховування інформації, в різних комп'ютерних об'єктах, що представляють собою різні файли, програми, пакети мережевих протоколів і т.д.; цифровий - приховування інформації в цифрових даних, що мають аналогову природу (зображення, аудіо- і відеодані).

Стеганографічна система (стегосистеми) - це сукупність засобів і методів, за допомогою яких створюється прихований канал передачі інформації. Контейнер - будь який файл, призначений для впровадження приховуваного повідомлення. Приховуване повідомлення - повідомлення, впроваджуване в контейнер. Повідомленням може бути секретний текст, зображення, фотографія, мітка, водяний знак. Стеганографічний канал (стегоканал) - канал передачі заповненого контейнера (Стего). Стегоключ (ключ) - секретні дані, використовувані в процесі впровадження приховуваного повідомлення в контейнер. При побудові стегосистеми повинні враховуватися наступні положення: супротивник має повне представлення про стеганографічні системи і деталі їх реалізації. Єдиною інформацією, яка залишається невідомою потенційному супротивникові, є ключ, за допомогою якого тільки його власник може встановити факт присутності і зміст прихованого повідомлення, якщо супротивник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому витягти подібні повідомлення до того часу, поки ключ зберігається

в таємниці. Потенційний супротивник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

На рис. 1 представленаузагальнена модель стегосистеми і проілюстровані наведені визначення.

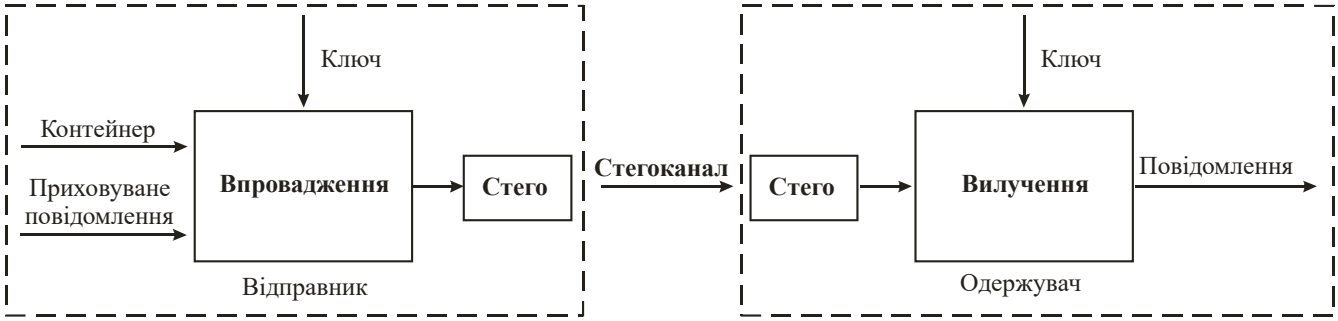

Рис. 1. Узагальнена модель стегосистеми

Відповідно до даної моделі, на стороні відправника приховуване повідомлення впроваджується в контейнер за спеціальним алгоритмом впровадження та ключем. Заповнений контейнер передається по відкритим каналам передачі даних одержувачу. На стороні одержувача із заповненого контейнера витягується вхідне повідомлення за алгоритмом витягування і ключем.

Широке розповсюдження растрових та мультимедійних технологій дало імпульс розвитку нових і вдосконаленню існуючих методів приховування інформації, а також сприяло виникненню більш складних методів організації прихованих каналів зв'язку, в основу яких були покладені особливості подання інформації в комп'ютерних файлах, пристроях, обчислювальних мережах і т.п. На цьому етапі відбувається становлення нового напрямку в області захисту інформації - комп'ютерної стеганографії. Класифікація методів стеганографії представлена на рис. 2.

Рис. 2. Класифікація методів стеганографії

Цифрова стеганографія застосовується для захисту від копіювання і несанкціонованого використання, дозволяє захищати авторські права і інтелектуальну власність в області цифрової аудіо та відео індустрії. Для цього застосовують вбудовування цифрових водяних знаків та ідентифікаційних номерів. Вбудовування невидимих заголовків застосовується для підпису медичних знімків та фотографій, нанесення легенди на карту, швидкого пошуку в базі даних по впровадженим в цифрові об'єкти (наприклад, в фотографії) ключовими словами, синхронізації відеопотоку зі звуком.

До методів організації прихованого каналу зв'язку засобами цифрової стеганографії виставляються наступні вимоги:

- прозорість - відсутність помітних відмінностей між пустим контейнером та заповненим контейнером;

- стійкість до спотворень - впроваджена інформація повинна бути стійкою до різноманітних перетворень, що відбуваються у процесі передачі інформації (вимога прозорості завжди конфліктує з вимогою стійкості до спотворень, тому при впровадженні інформації доводиться знаходити компроміс між прозорістю та стійкістю до спотворень);

- стійкість до атак - впроваджена інформація може піддаватися злому, видаленню чи атакам (вимога стійкості до атак є головною вимогою, що висувається до будь яких стеганографічних методів, проте досягти абсолютної стійкості впровадженої інформації до різних атак практично неможливо);

- можливість впровадження певного обсягу інформації - при істотному збільшенні обсягу впроваджуваної інформації знижується прозорість і стійкість до спотворень (дана вимога вступає в протиріччя з вимогою прозорості та вимогою стійкості до спотворень);

- секретність впровадження (криптостійкість) - у більшості випадків необхідно забезпечити секретність вбудованої інформації, тобто її захист секретним ключем.

Основна частина. Метод передачі прихованої інформації без спотворення растрового зображення дозволяє із зображення і файла даних, який необхідно приховати, отримати файл-ключ, за допомогою якого можна буде витягнути файл даних із початкового зображення, без спотворення початкового растрового зображення. Для того, щоб приховати дані, необхідно на вхід подати растрове зображення у форматі .PNG і файл з даними. А на виході буде отримано файл-ключ у форматі *.PNG (рис. 3а).

Для того, щоб витягнути файл даних із растрового зображення, необхідно на вхід подати початкове зображення і файл-ключ, отриманий в процесі шифрування, а на виході буде отримано файл даних (рис. 3б).

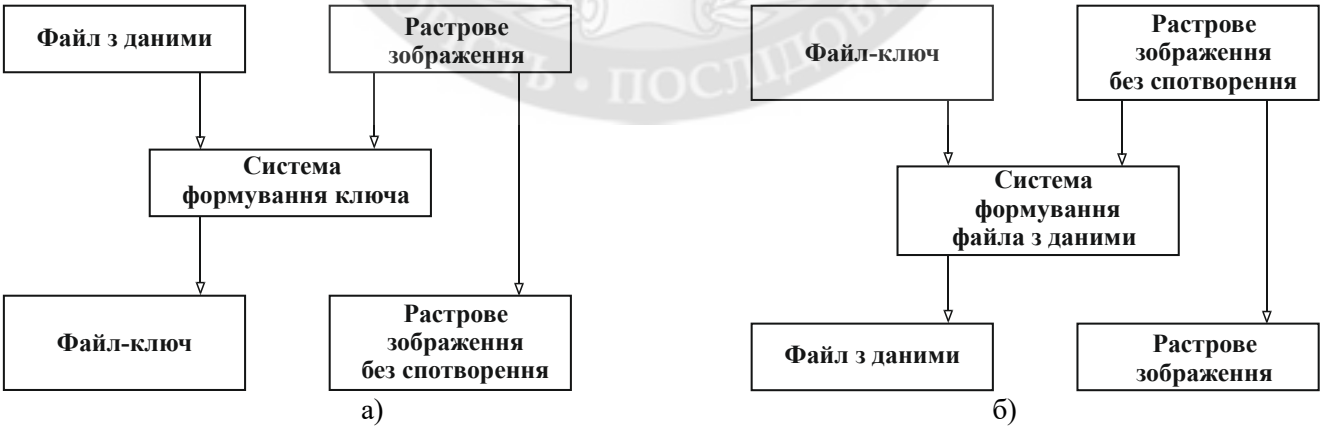

Рис. 3. Загальна схема формування даних: а) формування файла - ключа; б) витягнення файла даних із растрового зображення

Алгоритм роботи системи передачі прихованої інформації без спотворення растрового зображення представлений на рис. 4.

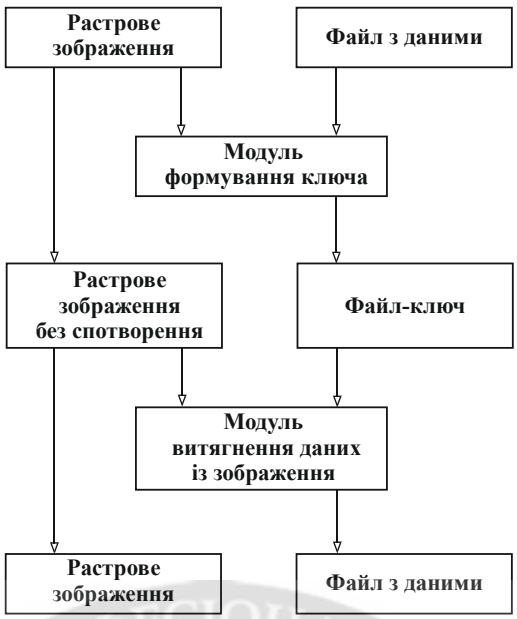

Рис. 4. Алгоритм роботи системи передачі прихованої інформації без спотворення растрового зображення

Принцип роботи алгоритму. В оперативну пам’ять завантажується зображення і файл з даними. Зображення представляє собою масив пікселів розміром чотири байти кожен. Генерується пустий масив пікселів такого ж розміру, що відповідає повністю прозорому (*.PNG формат) або залитому білим кольором (.JPG, .BMP формат) зображенню. Файл з даними завантажується як масив байтів. Програма в циклі проходить по кожному байту файла даних. В ітерації циклу відбувається наступне: запускається цикл, який проходить по масиву пікселів зображення і порівнює поточний байт файла даних з кожним байтом пікселя даної ітерації (лістинг 1.).

Лістинг 1.

```
for (unsigned int j = 0; j <кількість байт файлу; j++) {
for (unsigned int i = 0; i < кількість пікселів зображення; i++) {
        ...
порівняння першого байту пікселя з поточним байтом файла даних
порівняння другого байту пікселя з поточним байтом файла даних
порівняння третього байту пікселя з поточним байтом файла даних
порівняння четвертого байту пікселя з поточним байтом файла даних
        ...
    }}
```

Якщо порівняння дає “правду”, тоді в пустий масив, згенерований на початку роботи системи, по адресу пікселя даної ітерації записується адрес байту в пікселі (рис. 5). В результаті отримаємо масив пікселів, в якому записані адреси на ті місця в зображення, де містяться байти зашифрованого файлу. Якщо прочитати будь який піксель цього масиву, то в ньому буде записаний або “нуль” (немає адреси), або число. Це означає, що коли будем читати даний піксель, то номер пікселя результуючого масиву буде відповідати номеру пікселя початкового растрового зображення, а число, записане в цьому пікселі – номер байта в пікселі. Далі результуючий масив пікселів стискається і зберігається в форматі результуючого растрового зображення. Через низьку ентропію цього масиву, файл буде мати набагато менший розмір, ніж початкове растрове зображення.

Читання даних із початкового растрового зображення. В оперативну пам'ять як масиви пікселів завантажується початкове растрове зображення і файл-ключ. Програма по циклу пробігає по файл-ключу, якщо значення не дорівнює нулю, читається число, записане в пікселі – це і є номер байта, а номер ітерації – це номер пікселя. Отримані номер пікселя і

номер байта в цьому пікселі, представляють собою координати байта в масиві початкового растрового зображення. З набору витягнутих байт формуємо результуючий файл з даними.

Рис. 5. Генерація результуючого масиву пікселей

При використанні даного підходу, отримані результуючі байти будуть перемішані. Це можна виправити наступним чином (рис. 6): при створенні файла-ключа в перших три байти записуємо номер файлового байту, а в останній – номер байту в пікселі згідно вище описаного способу. І при дешифруванні маючи вказаний номер байта можна легко відновити їх порядок.

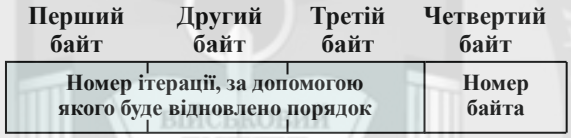

Рис. 6. Структура пікселя файла - ключа

Отриманий файл-ключ можна передати по мережі (при цьому початкове растрове зображення буде знаходитись в мережі без спотворення) і побітово зашифрувати в зображення (рис. 7). При необхідності існує можливість шифрування файл-ключа в початкове растрове зображення. В даному випадку при формуванні файл-ключа, останній байт пікселя не індексується, тому що він буде змінений. Також є можливість шифрування файл-ключа одним із існуючих методів симетричного шифрування або RSA.

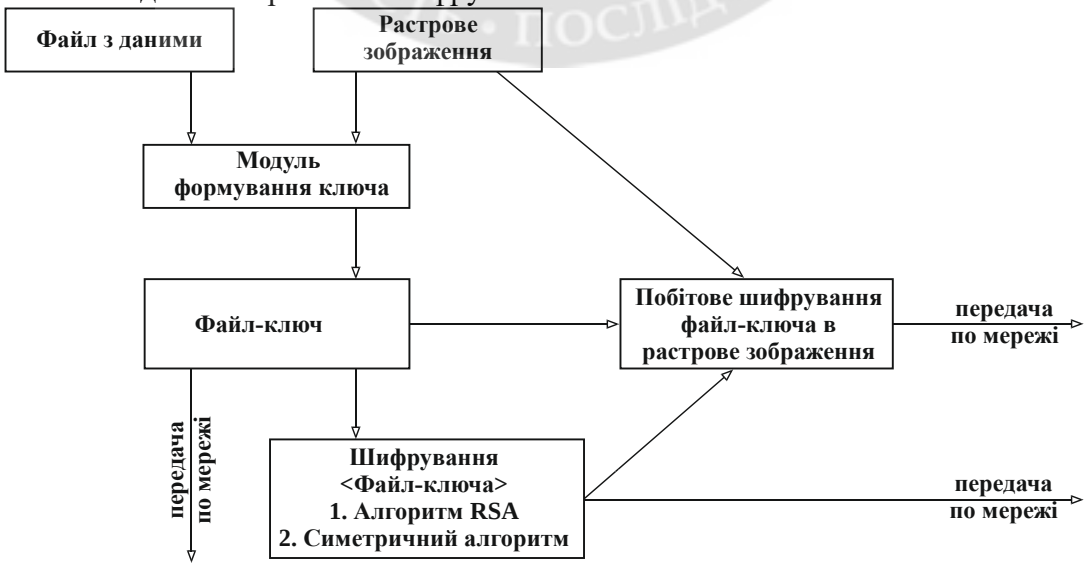

Рис. 7. Загальна схема передачі файл-ключ по мережі

Висновки. На основі проведеного аналізу наведено поняття прихованого каналу передачі інформації, а також класифікацію методів і завдань прихованої передачі інформації.

Проведено огляд існуючих методів впровадження інформації в растрові зображення. Наведено аналіз існуючих програм впровадження інформації в растрові зображення, виявлено їх переваги та недоліки. Розглянуті можливі області застосування стеганографії, зокрема-стеганографія може бути використана для зберігання і розподілення ключів в мережах зв'язку. Виявлені недоліки методів впровадження інформації в растрові зображення і їх програмні реалізації не дозволяють в повній мірі використовувати їх для безпечної передачі інформації. Для усунення виявлених недоліків запропонований метод передачі прихованої інформації без спотворення растрового зображення, який дозволяє із зображення і файла даних, отримати файл-ключ пікселів, за допомогою якого можна витягнути файл даних із початкового растрового зображення. При цьому без спотворення растрового зображення.

Для організації прихованого каналу зв'язку, розподілу і передачі ключової інформації запропонований метод, на відміну від розглянутих, має високу пропускну здатність. Файл-ключ пікселів стискається і зберігається в форматі результуючого растрового зображення. Через низьку ентропію файл-ключа пікселів, він буде мати набагато менший розмір, ніж початкове растрове зображення. При необхідності існує можливість шифрування файл-ключа пікселів методом симетричного шифрування або RSA, що значно підвищить стійкість до атак - впроваджена інформація може піддаватися злому, видаленню чи атакам. Стійкість є головною вимогою, що висувається до будь яких стеганографічних методів, а також забезпечить секретність вбудованої інформації.

ЛІТЕРАТУРА:

1. Васина Т. С. Обзор современных алгоритмов стеганографии / Т. С. Васина // электронное научно-техническое издание «Наука и образование». – 2012.

2. Тропченко А. Ю. Методы сжатия изображений, аудиосигналов и видео : учебное пособие / А. Ю. Тропченко, А. А. Тропченко. – СПб.: СПбГУ ИТМО, 2009. – 108 с.

3. Горбачев В.Н. Методы цифровой стеганографии для защиты изобразительной информации /, Е.М. Кайнарова, А.И. Кулик. – М.: МГУП, 2011. – 224 с.

4. Майк Кон. Scrum: Гибкая разработка ПО. / Майк Кон. – Изд-во: Диалектика-Вильямс, 2016. – С. 576.

5. Лєнков С.В. Концептуальна схема системи інтелектуальної обробки даних / С.В. Лєнков, В.М. Джулій, О.М. Горбатюк, Н.М. Берназ // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2014. – Вип. № 46. – С.181-190

6. Роберт Мартин Гибкая разработка программ на Java и C++. Принципы, паттерны и методики. /Роберт С. Мартин, Джеймс Ньюкирк, Роберт Косс – Изд-во: Диалектика-Вильямс, 2016. – 704 с.

7. Грибунин В.Г. Цифровая стеганография. /В.Г. Грибунин, И.Н. Оков, И.В. Туринцев // М.: СОЛОН-Пресс; 2002. - 261 с.

8. Конахович Г.Ф. Компьютерная стеганография / Г.Ф Конахович, А.Ю. Пузыренко // Теория и практика. Киев: МК-Пресс, 2006. -288с.

9. Мамаев М. Технологии защиты информации:в Интернете/ Мамаев М., Петренко С. //: Специальный;справочник..СИб::Иитер 2002. -848 с.

10. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия – Телеком, 2010. – 232 с.

11. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К.: Юниор, 2003. – 501 с.

12. Кузнецов О. О. Стеганография : навч. посібник / О.О. Кузнецов, С.П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 232 с.

13. Конахович Г. Ф. Компьютерная стеганография : теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

14. Грибунин В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2012. – 272 с.

REFERENCES:

1. Vasina T. S. Review of modern algorithms of a steganografiya/T.S.Vasina//electronic scientific and technical edition "Nauka I Obrazovaniye". – 2012.

2. Tropchenko A. Yu. Methods of compression of images, audiosignals and video: manual / A.Yu. Tropchenko, A.A. Tropchenko. – SPb.: St.Petersburg State University of ITMO, 2009. – 108p.

3. Methods of a digital steganografiya for protection of graphic information / V.N. Gorbachev, E.M. Kaynarova, A.I. Kulik, I.K. Metelev. – M.: MGUP, 2011. – 224p.

4. Mike Kohn. Scrum: Flexible software development. / Mike Kohn. – Publishing house: Dialectician Williams, 2016. –576p.

5. Lenkov S.V. The scheme to system _ntelektualno ї obrobk the danikh / S.V. Lenkov, V.M. Dzhul_y, O.M. Gorbatyuk, N.M. Bernaz//Zb_rnik the naukovikh праць V_yskovy to a _nstitut Ki§vsky nats_onalny to an un_versitet імені Taras Shevchenk is conceptual. – To.: VIKNU, 2014. – VIP. No. 46. – p.181-190

6. Robert Martin Flexible development of programs on Java and C ++. Principles, patterns and techniques. / Robert S. Martin, James Nyyukirk, Robert Koss – Publishing house: Dialectician Williams, 2016. – 704p.

7. Gribunin V.G. Digital steganografiya. / V.G. Gribunin, I.N., I.V. Fetters, Residents of Turin//M.: SOLON Press; 2002. - 261 p.

8. Konakhovich G.F. Computer steganografiya/ G. Ф Konakhovich, A.Yu Puzyrenko//Theory and practice. Kiev: MK-Press, 2006. - the 288p.

9. Mamayev M. Technologies of protection информации:в Internet / Mamayev M., Petrenko S.//: Special; reference book. SIB:: Iiter 2002.-848 p.

10. Ryabko B.Ya. Fundamentals of modern cryptography and steganografiya / B.Ya. Ryabko, A.H. Fionov. – M.: The hot line – the Telecom, 2010. – 232p.

11. Horoshko V. A. Methods and means of information protection/VA. Horoshko, A.A. Chekatkov. – To.: Junior, 2003. – 501 p.

12. O.O. Steganografiya's smiths: навч. pos_bnik / O.O. Kuznetsov, S.P. Євсеєв, O.G. Korol. – X.: Look. HNEU, 2011. – 232p.

13. Konakhovich G. F. Computer steganografiya: theory and practice / G.F. Konakhovich, A.Yu. Puzyrenko. – To.: MK-Press, 2006. – 288p.

14. Gribunin V. G. Digital steganografiya / V.G. Gribunin, I.N. Okov, I.V. Turintsev. – M.: SOLON Press, 2012. – 272 p.

Рецензент: д.т.н., проф. Барабаш О.В., завідувач кафедри вищої математики Державного університету телекомунікацій

д.т.н., проф. Ленков С.В., к.т.н. Джулий В.Н.,
к.т.н. с.н.с. Мирошниченко О.В., Бойко Б.А.

МЕТОД ПЕРЕДАЧИ СКРЫТОЙ ИНФОРМАЦИИ БЕЗ ИСКАЖЕНИЯ РАСТРОВОГО ИЗОБРАЖЕНИЯ

В статье предложенный метод передачи скрытой информации без искажения растрового изображения. На основе проведенного анализа приведено понятие скрытого канала передачи информации, а также классификация методов и заданий скрытой передачи информации. Проведен обзор существующих методов внедрения информации в растровые изображения. Приведен анализ существующих программ внедрения информации в растровые изображения, выявлены их преимущества и недостатки. Рассмотренные возможные области применения стеганографии, в частности -стеганография может быть использована для хранения и распределения ключей в сетях связи. Выявленные недостатки методов внедрения информации в растровые изображения и их программные реализации не позволяют в полной мере использовать их для безопасной передачи информации. Для устранения выявленных недостатков предложенный метод передачи скрытой информации без искажения растрового изображения, который позволяет из изображения и файла данных, получить файл-ключ пикселов, с помощью которого можно будет вытянуть файл данных из начального растрового изображения, без искажения растрового изображения. При необходимости существует возможность побитово зашифровать файл-ключ в начальное растровое изображение, в данном случае при создании файлового ключа, последний байт пикселя не индексируется, потому, что он будет изменен. Для организации скрытого канала связи, распределения и передачи ключевой информации предложенный метод, в отличие от рассмотренных методов, имеет высокую пропускную

способность. Файл-ключ пикселов сжимается и хранится в формате результирующего растрового изображения. Через низкую энтропию файлового ключа пикселов, он будет иметь намного меньший размер, чем начальное растровое изображение. При необходимости существует возможность шифровки файл- ключа пикселов методом симметричного шифрования или RSA, что значительно повысит стойкость к атакам - внедренная информация может поддаваться взлому, удалению или атакам. Стойкость является главным требованием, которое выдвигается к стеганографическим методам, а также обеспечит секретность встроенной информации.

Ключевые слова: стеганография, стеганографические методы, файл-ключ, растровое изображение, скрытый канал связи, защита информации, стегоключ.

prof. Lenkov S.V., Ph.D. Dzhuliy V.M., Ph.D. Miroshnihenko O.V., Boyko B.O.

THE METHOD OF RETAINED INFORMATION TRANSMISSION WITHOUT DRAWING ROTATION

The method of transmitting hidden information without distorting the raster image is proposed in the article. The concept of a hidden channel of information transmission, as well as the classification of methods and tasks of latent information transmission is determined on the basis of the analysis.

An overview of existing methods for information implementing in bitmap images has been carried out. An analysis of existing programs for information implementing in bitmap images is presented and their advantages and disadvantages are revealed. The possible areas of steganography can be used to store and distribute keys in communication networks. The defined drawbacks of information implementation methods in bitmap images and their software implementations do not allow them to be fully used for the safe transmission of information. The method of transmitting hidden information without distorting a raster image, which allows the image and data file to obtain a pixel file key, by which it will be possible to extract the data file from the original raster image without distorting the bitmap imageu is proposed to eliminate the identified shortcomings. If necessary, it is possible to encrypt bitwise the file key in the original raster image, in this case when creating a file key, the last pixel byte is not indexed, because it will be changed.

The proposed method, in contrast to the considered methods, has a high bandwidth for organizing a hidden communication channel, the distribution and transmission of key information. The pixel key file is compressed and stored in the resulting raster image. It will have a much smaller size than the original raster image due to the low entropy of the pixel key file. If necessary, it is possible to encrypt the pixel file key using the symmetric encryption method or RSA, which will greatly increase the resistance to attacks - the information embedded may be subject to hacking, deletion, or attacks. Stability is the main requirement for any steganographic methods, as well as secrecy of the built-in information.

Keywords: steganography, steganographic methods, file key, raster image, hidden communication channel, information security, steganography.