УДК 004.056.5 doi.org/10.33298/2226-8553/2019.1.28.24

Овчарук І.В., Пристінська А.А.

АНАЛІЗ ЧУТЛИВОСТІ ЗОРОВОГО СПРИЙНЯТТЯ ІНФОРМАЦІЇ ЛЮДИНОЮ НА ОСНОВІ СТЕГАНОГРАФІЧНОГО МЕТОДУ LSB

У статті наведено опис розробленої системи, що використовує стеганографічний метод LSB, який дозволяє захистити текстову інформацію від несанкціонованого доступу шляхом приховування самого факту передачі цієї інформації. Використовуючи стеганографічний метод LSB, емпіричним шляхом проведено аналіз чутливості зорового сприйняття людини щодо модифікації зображення – стеганографічного контейнера при впровадженні в нього повідомлення.

Наведено також огляд напрямків, спрямованих на захист інформації від несанкціонованого доступу, приведені основні методи криптографії та стеганографії.

Ключові слова: *комп'ютерна стеганографія, цифрова стеганографія, цифрові зображення, криптографія, криптографічна хеш-функція, контейнер, програмна система, інтерфейс.*

Постановка проблеми. Одним з актуальних питань є забезпечення безпеки передачі даних по глобальній мережі [1]. Дані, які передаються між користувачами, повинні залишатися конфіденційними. Більше того, інтернет повинен гарантувати захист користувача і його даних від будь-якого роду атак і загроз. Розвиток нових інформаційних технологій і загальна комп'ютеризація призвели до того, що інформаційна безпека не тільки стає обов'язковою, вона ще є однією з характеристик інформаційних систем.

Інформаційна безпека – це процес забезпечення конфіденційності, доступності та цілісності інформаційних ресурсів, який підтримується великим набором засобів і методів для забезпечення захисту даних від різного виду загроз. Розвиток комп'ютерних мереж та засобів мультимедіа привів до появи нових способів забезпечення безпеки даних при передачі їх через інтернет і інші канали зв'язку (телекомунікації). Однією з важливих галузей інформаційної безпеки є стеганографія. Стеганографія – наука про приховану передачу інформації. Розвитку методів стеганографії сприяє обмеження використання криптографії в ряді країн світу і поява проблеми захисту прав власності на інформацію, представлену в цифровому вигляді (цифровий водяний знак).

Розробка програмних систем для захисту інформації є актуальною задачею у зв'язку з розповсюдженням мультимедійних технологій, а також з масовим використанням мереж для передачі інформації.

Аналіз останніх наукових досліджень і публікацій. Питаннями захисту інформації займалися такі дослідники: Коробейников А.Г., Биков С. Ф, Аграновський А.В., Балакін А.В., Грібунін В.Г., Конахович Г.Ф., Пузиренко А.Ю. Кустов В. Н.,. Федчук А. А. У їхніх роботах описано метод LSB, використання алгоритмів стиснення в стеганографії [2, 3, 7]. Питання криптографії висвітлені в роботах Алфьорова А.П., Зубова А.Ю., Кузьміна О.С., Черьомушкіна А.В., Окова І.М., де розглянуто захист з використанням різних видів криптосистем [4–6]. Розвиток інформаційних технологій і масове використання мереж призвело до розробки програмних систем захисту інформації від несанкціонованого доступу. З'явилися спеціалізовані системи, наприклад, перевірка аутентифікації, системи створення електронного цифрового підпису. З розвитком комп'ютерних технологій з'явилися

спеціалізовані програмні продукти відповідного призначення, наприклад, JSteg – одна з перших програм для приховування даних в форматі JPEG, не підтримує шифрування прихованих даних. Програми F5, StegHide спеціалізуються на стеганографічних методах.

Метою даної статті є огляд методів захисту інформації та розробка комп'ютерної системи захисту інформації від несанкціонованого доступу з метою прихованої передачі повідомлень за допомогою стеганографічних контейнерів, а також аналіз зорового порогу чутливості людини використовуючи різний ступінь модифікації зображення.

Викладення основного матеріалу. В галузі захисту виділилося два основні напрямки – криптографія і стеганографія. Мета криптографії полягає в блокуванні несанкціонованого доступу до інформації шляхом шифрування змісту секретних повідомлень. Для шифрування відкритих (вихідних) текстів застосовувалися різні типи шифрів: підстановки, перестановки, гамування, комбіновані шифри. Сучасна криптографія має математичну природу і базується на багатьох математичних дисциплінах, таких як: лінійна алгебра, теорія груп, теорія автоматів, математичний аналіз, теорія дискретних функцій, теорія чисел, комбінаторний аналіз, теорія ймовірностей і математична статистика, теорія кодування, та ін.

Криптографічні методи використовуються для вирішення наступних задач: передачі конфіденційної інформації по каналах зв'язку (наприклад, електронна пошта); встановлення достовірності повідомлень, що передаються; зберігання інформації на носіях в зашифрованому вигляді. За принципами використання ключів [8] криптосистеми розділяються на системи з секретним і відкритим ключем. Стійкість будь-якої криптографічної системи визначається ступенем секретності ключа, що в ній використовується.

В криптографії використовуються спеціальні перетворення інформації за допомогою криптографічної хеш-функції, які мають назву – хешування. Існує декілька різновидів криптографічної хеш-функції залежно від методів, що покладені в основу її побудови. До хеш-функцій, що основані на MD-технологіях, відносяться сімейства хеш-функцій MD, SHA та ін. До хеш-функцій, що основані на блочних шифрах, можна віднести MDC – хеш-функції, а до хеш-функцій, що основані на модулярній арифметиці, відносяться хеш-функції сімейства MASH.

Крім криптографії, існує ще ряд напрямків, пов'язаних із захистом інформації. Методи захисту інформації з використанням голографії є актуальним напрямком, що розвивається. Голографія є розділ науки і техніки, що займається вивченням і створенням способів, пристроїв для запису й обробки хвиль різної природи. Оптична голографія заснована на явищі інтерференції хвиль. Інтерференція хвиль – взаємне посилення чи послаблення двох (або більшої кількості) хвиль при їх накладенні при одночасному поширенні в просторі. Картинка, що виникає при інтерференції хвиль, містить інформацію про об'єкт. Якщо цю картинку фіксувати на світлочутливій поверхні, то утворюється голограма. При опроміненні голограми або її ділянки опорною хвилею можна побачити об'ємне тривимірне зображення об'єкта [8]. Голографія застосовувана до хвиль будь-якої природи і в даний час знаходить все більш практичне застосування для ідентифікації продукції різного призначення.

Якщо криптографія – це наука про методи приховування інформації шляхом, її шифрування, то стеганографія вивчає методи, пов'язані з приховуванням самого факту передачі інформації.

Перевага стеганографії над криптографією полягає в тому, що повідомлення не привертають до себе уваги. Повідомлення, факт шифрування яких не прихований, викликають підозру. Таким чином, криптографія захищає вміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих послань.

В даний час виділяють три основних напрями застосування стеганографії: приховування даних (повідомлень), цифрові водяні знаки і заголовки [9].

В основі маскування даних або стеганографічного аналізу лежить робота з фізичними процесами. Аудіосигнали і зображення – це все фізичні процеси. Ми отримуємо цифрові образи звуку або зображення за допомогою аналого-цифрових перетворювачів.

Стеганографія, з точки зору реалізації – це процес накладення слабкого шуму на реалізацію цифрового процесу.

Прогрес в області інформаційних технологій привів до появи нових напрямків в стеганографії – комп'ютерної та цифрової стеганографії.

Комп'ютерна стеганографія – напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи, наприклад, приховування даних шляхом запису інформації в невикористані файлами області, підміна символів в назвах файлів, а також використання методів стеганографії для приховування текстової інформації.

Цифрова стеганографія – напрям класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти. Як правило, дані об'єкти є мультимедіа-об'єктами (зображення, відео- або аудіо-файли, текстури 3D-об'єктів), внесення змін до яких викликає лише незначні спотворення, що знаходяться нижче порогу чутливості середньостатистичної людини, що не призводить до помітних змін цих об'єктів. Це дозволяє приховувати, наприклад, текстові файли в графічних файлах.

При цьому, криптографічні та стеганографічні методи можуть бути об'єднані і використані для підвищення ефективності захисту інформації

Стеганографічні системи використовуються для вирішення наступних основних задач: захист конфіденційної інформації від несанкціонованого доступу; захист авторського права на деякі види інтелектуальної власності, задачі аутентифікації, відстеження поширення інформації з мереж зв'язку, а також пошуку інформації в мультимедійних базах даних.

В рамках цифрової стеганографії, на відміну від комп'ютерної, не розглядаються питання впровадження даних в заголовки IP-пакетів і файлів різних форматів, в текстові повідомлення.

Значна частина досліджень в області цифрової стеганографії присвячена вбудовуванню конфіденційних повідомлень і цифрових водяних знаків в статичну графіку, наприклад, в файли форматів, що не використовують стиснення (BMP, або Windows Bitmap). В даний час розроблено велику кількість алгоритмів вбудовування інформації та цифрових водяних знаків в графічні файли, що використовують стиснення з втратами (в тому числі і JPEG).

Приховування впроваджуваних даних, які в більшості випадків мають великий обсяг, пред'являє серйозні вимоги до контейнера: розмір контейнера в кілька разів повинен перевищувати розмір вбудованих даних.

Відкритий текст, де прихована інформація, що зашифрована стеганографічним алгоритмом, називається контейнером. За протяжністю контейнери можна поділити на два типи: безперервні (потокові) і обмеженої (фіксованої) довжини. Контейнер може бути згенерований самою стегосистемою. Наприклад, як контейнер для вбудовування повідомлення може генеруватися фрактал Мандельброта. Такий підхід називають конструюючою стеганографією.

До методів приховування інформації відносять, наприклад, методи заміни найменшого значущого біта (Least Significant Bits – LSB). Суть методу полягає в приховуванні інформації шляхом зміни останніх бітів зображення, які кодують колір, на біти повідомлення, що приховується. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини. Модифікація молодших бітів у більшості випадків не викликає значної трансформації зображення і не виявляється візуально [9].

Іншим методом вбудовування повідомлень є використання особливостей форматів даних, що використовують стиснення з втратою даних (наприклад, JPEG). Цей метод (на відміну від LSB) більш стійкий до геометричних перетворень і виявлення каналу передачі, так як є можливість в широкому діапазоні варіювати якість стисненого зображення, що робить неможливим визначення походження спотворення.

До методів приховування даних відноситься метод Куттера-Джордана-Боссена (метод «хреста»), який застосовується для вбудовування інформації в зображення [10].

При використанні даного методу 1 біт повідомлення впроваджується в 1 піксель контейнера. Секретний ключ задає координати пікселів, в які буде здійснюватися вбудовування. Вибір зміни яскравості конкретного кольору обумовлений особливістю зорової

системи людини. Зображення розглядається в моделі RGB. При встановленні яскравості червоного і зеленого кольорів залишаються без змін, яскравість синього – змінюється за формулою:

$$B^*_{x,e} = \begin{cases} B_{x,y} + \lambda Y_{x,y}, \text{при } m_i = 1 \\ B_{x,y} - \lambda Y_{x,y}, \text{при } m_i = 0 \end{cases}$$

де, $B_{x,y}$ – яскравість синього кольору пікселя с координатами (x, y); $B^*_{x,e}$ – змінена яскравість синього кольору пікселя; $Y_{x,y}$ – яскравість пікселя; m_i – і-ий біт повідомлення, що вбудовується; λ – коефіцієнт, що задає енергію вбудованого біта даних (задається, виходячи з функціонального призначення і особливості стеганосистеми).

Для отримання інформації використовується прогнозоване значення яскравості пікселя синього кольору.

Одним з найбільш перспективних напрямків комп'ютерної стеганографії є технологія використання цифрових водяних знаків (ЦВЗ, digital watermarking) – у даному випадку, створення невидимих оку знаків захисту авторських прав на графічні та аудіофайли. Такі ЦВЗ поміщаються в файл і розпізнаються спеціальними програмами, які витягують з файлу інформацію про створення файлу, авторські права, як вступити в контакт з автором і т.д.

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії або інші оцифровані твори мистецтва. Основними вимогами, які пред'являються до таких вбудованих даних, є надійність і стійкість до спотворень. Цифрові водяні знаки мають невеликий обсяг, проте, з урахуванням зазначених вище вимог, для їх вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень або заголовків. У сучасних системах формування цифрових водяних знаків використовується, наприклад, принцип вбудовування мітки, що є вузькосмуговим сигналом, в широкому діапазоні частот, який маркує зображення.

У роботі створено стеганографічну систему приховування текстової інформації в графічному зображенні, яке є контейнером (рис. 1). Система розроблена в VisualStudio 2010 C# Windows Form.

Для приховування текстової інформації застосовано метод LSB. Суть методу полягає в спотворенні зображення таким чином, щоб ці спотворення не були помітні для людського ока. Як контейнер використовується графічне зображення в форматі BMP. Для представлення кольору використовується колірна модель RGB, тобто колір, який бачить людина, виходить в результаті змішування трьох кольорів Red, Green, Blue (червоного, зеленого, синього). Файл формату BMP, зазвичай, не вживає стиснення, що дає можливість заховати в ньому досить велику кількість інформації. У форматі BMP зображення зберігається як матриця значень відтінків кольору для кожної точки зображення, що зберігається. Якщо кожна з компонент (каналів кольору) простору RGB зберігається в одному байті, вона може набувати значень від 0 до 255 включно, що відповідає 24-х бітній глибині кольору. Особливість зору людини полягає в тому, що вона слабо розрізняє незначні коливання кольору. Кожен колір (піксель) кодується одним байтом (8 біт). У BMP таких кольорів три (червоний, синій, зелений) – разом 3 байти (24 біти). Щоб записати інформацію і при цьому не спотворити зображення, дані записуються в молодші біти кольорів зображення. Тобто, молодші біти в складових кольору пікселя замінюються бітами повідомлення.

Схема заміни молодших бітів:

1 байт повідомлення:

10 101 010

RGB пікселя:

R: 11110**00**

G: 00001**000**
B: 11001**000**
Новий піксель, після заміни молодших бітів:
R: 11110**10**
G: 00001**101**
B: 11001**010**

Величина переданого повідомлення залежить від величини контейнера. У даному випадку контейнер фіксованої довжини. Впроваджене повідомлення не призвело до помітної модифікації контейнера. Тоді отримуємо, що даний метод дозволяє передавати повідомлення розміром 1/8 контейнера, якщо міняти 1 біт або 1/4 контейнера, якщо змінювати 2 останні біти.

Проведемо аналіз чутливості зорового сприйняття людини щодо модифікації зображення. Для 24-бітного кольору зміна в кожному з трьох каналів одного найменш значущого біта (тобто крайнього правого) призводить до зміни менш ніж на 1% інтенсивності даної точки, що дозволяє змінювати їх непомітно для ока.

Зашифруємо повідомлення, що наведено у вікні програми (рис.1)

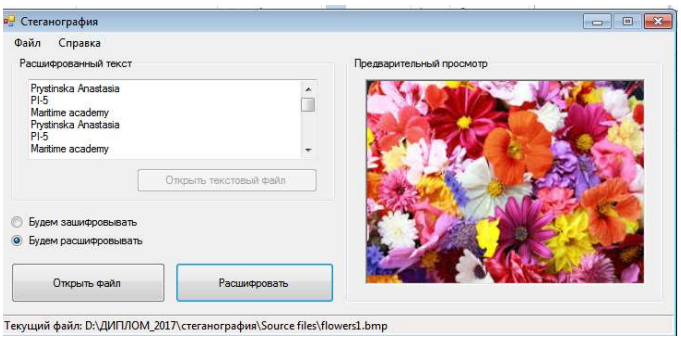

Рисунок 1 – Інтерфейс програми

Далі наводяться тільки зображення. На рис.2 наведено контейнер

Рисунок 2 – Контейнер

Експериментальним шляхом було зашифровано інформацію у біти в трьох каналах пікселя (RGB) у різній послідовності. Пораховано у відсотках залежність зміни зображення від зміни різної послідовності бітів.

Замінимо 2 біти в каналі Red (r), Green (g), Blue (b). Нижче наведено порядок заміни бітів методом LSB у відповідних масивах: r[6] = m[0], r[7] = m[1], g[5] = m[2], g[6]=m[3], g[7]=m[4], b[5] = m[5], b[6] = m[6], b[7] = m[7]. Тобто, в каналах замінюються молодші біти. Розрахуємо

відсоток зміни кольору пікселів зображення: V= (2/255 + 3/255 + 3/255+ 3/255)*100% = 8/255*100% =3%

Контейнер, що містить повідомлення, наведено на рис.3

Рисунок 3 – Стеганографічний контейнер

Як видно на зображенні, при зміні кольору пікселів на 3%, різниця для ока невідчутна.

Розглянемо ще один приклад. Збільшимо кількість біт, що замінюються, але знову будемо замінювати тільки молодші біти. В кожному замінюються останні 3 біти: r[5]=m[0], r[6]= m[1], r[7] = m[2], g[5] = m[3], g[6] = m[4], g[7] = m[5], b[5] = m[6], b[6]=m[7], b[7] = m[8].

Колір пікселів зображення зміниться на: V= (3/255 + 3/255 + 3/255)*100% = 9/255*100 =3,5%.

Контейнер, що містить повідомлення, наведено на рис.4.

Рисунок 4 – Стеганографічний контейнер

У даному випадку маємо незначні спотворення у відтінку, але різниця для ока невідчутна за рахунок того, що змінюються 3 молодші біти.

Тепер замінимо 5 бітів в каналі Red, а в інших двох каналах – по 3 молодших біти. Колір пікселів зображення зміниться на: V= (5/255 + 3/255 + 3/255)*100% = 11/255 =4%

Контейнер, що містить повідомлення, наведено на рис.5.

Рисунок 5 – Стеганографічний контейнер

Зміна червоного кольору стає відчутною для зору людини. Однак, потрібно врахувати, що збільшення розміру переданого повідомлення призводить до більш сильних спотворень у зображенні. Якщо, наприклад, в каналі Red замінити 7 бітів, а в інших змінювати по 3 біти, то колір пікселів зображення зміниться таким чином: V =(7/255 + 3/255 + 3/255)*100% = (13/255)*100% =5%

Контейнер, що містить повідомлення, наведено на рис.6.

Рисунок 6 – Стеганографічний контейнер

При зміні кольору пікселів на 5% спотворення на зображенні добре помітні. Аналогічно можна виявити поріг чутливості, замінюючи різну кількість бітів по інших кольорових каналах.

Висновок та пропозиції. Розроблена авторами система дозволяє приховувати текстову інформацію в графічному зображенні – стеганографічному контейнері, що дозволяє забезпечити сам факт передачі інформації, а також за допомогою реалізації метода LSB можна проаналізувати чутливість зорового сприйняття людини, отримуючи різний ступінь модифікації зображення. Система завантажує текстове повідомлення та контейнер з відповідних файлів і впроваджує повідомлення в контейнер; дозволяє зашифрувати і дешифрувати інформацію, тобто отримати її з контейнера, у якому повідомлення знаходиться.

ЛІТЕРАТУРА

1. Губенко Н. Е., Сипаков Д. С. Анализ особенностей методов цифровой стеганографии для защиты информации, передаваемой по открытым каналам / Н. Е. Губенко, Д. С. Сипаков // Информатика и кибернетика. – Донецк: ДонНТУ, 2015. – № 2. С. 28-37.

2. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин, С. Сапожников. – М.: Вузовская книга, 2009. – 220 с.

3. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография / В.Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.

4. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиус АРВ, 2001. – 480 с.

5. Оков И. Н. Криптографические системы защиты информации / И. Н. Оков. – СПб.: ВУС, 2001. – 236 с.

6. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин – СПб.: БХВ, 2000. – 384 с.

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

8. Криптографические методы защиты информации [Электронный ресурс]. – Режим доступа:
http://edulib.pgta.ru/els/_/disk/27.03.02%20-.pdf

9. Основные положения стеганографии [Электронный ресурс]. – Режим доступа: http://citforum.ck.ua/internet/securities/stegano.shtml

10. Стеганографический метод Куттера-Джордана-Боссена [Электронный ресурс]. – Режим доступа: http://cryptowiki.net/index.php?title=File

Овчарук И.В., Пристинская А.А.

АНАЛИЗ ЧУВСТВИТЕЛЬНОСТИ ЗРИТЕЛЬНОГО ВОСПРИЯТИЯ ИНФОРМАЦИИ ЧЕЛОВЕКОМ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА LSB

В статье приведено описание разработанной системы, использующей стеганографический метод LSB, который позволяет защитить текстовую информацию от несанкционированного доступа путем сокрытия самого факта передачи этой информации. Используя стеганографический метод LSB, эмпирическим путем проведен анализ чувствительности зрительного восприятия человека по модификации изображения – стеганографического контейнера при внедрении в него сообщения. Приведен также обзор направлений по защите информации от несанкционированного доступа, основные методы криптографии и стеганографии.

Ключевые слова: *компьютерная стеганография, цифровая стеганография, цифровые изображения, криптография, криптографическая хэш-функция, контейнер, программная система, интерфейс.*

Ovcharuk I., Prystinska A.

SENSITIVITY ANALYSIS OF VISUAL PERCEPTION OF INFORMATION BY PERSON, BASED ON LSB STEGANOGRAPHIC METHOD

The article describes the developed system that uses a steganographic method of LSB, which allows to protect text information against unauthorized access by hiding the fact that information was transfered. Using steganography method LSB, empirically was conducted a sensitivity analysis of human visual perception of image modification - the insertion of steganographic container in his message. Also, there are shown overviews of ways to protect information from unauthorized access and given the basic methods of cryptography and steganography.

Keywords: *computer steganography, digital steganography, digital images, cryptography, cryptographic hash function, container, software system, interface.*