УДК 004.4

Д. В. Телефус
В. В. Лукічов
Л.М. Куперштейн

СИСТЕМА ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ЧАСТОТНІЙ ОБЛАСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

Вінницький національний технічний університет

Анотація

Спроектовано стеганографічну систему захисту інформації у цифрових зображеннях на основі методу прихування у частотній області зображення. У якості стегоконтейнера система використовує зображення формату JPEG.

Ключові слова: кібербезпека, стеганографія, прихована передача інформації, дискретне косинусне перетворення, зображення JPEG.

Abstract.

A steganographic system of information security in digital images based on hiding method in frequency range of an image has been designed. System uses JPEG images as a container.

Keywords: cybersecurity, steganography, hidden information transmission, discrete cosine transform, JPEG images.

Вступ

Характерною особливістю сучасної науки є те, що вона перетворюється на складний і безперервно зростаючий соціальний організм, у динамічну, рухливу виробничу силу суспільства [1].

Аналіз останніх досліджень [2-3] показує, що у наукових публікаціях особливу увагу присвячено принципам та засобам забезпечення інформаційної безпеки, серед яких важливе місце посідає організація прихованого обміну інформації на основі застосування методів комп'ютерної стеганографії.

На сьогоднішній день найбільшу популярність в комп'ютерній стеганографії здобули стеганографічні методи, які використовують у ролі контейнера зображення [2].

Наразі, існує чимало методів стеганографії для графічних файлів. Стеганографічні методи приховування даних у просторовій області зображення є нестійкими до переважної більшості відомих видів спотворювань, а також використовують не найбільш поширені формати цифрових зображень. Більш стійкими до різноманітних спотворювань, у тому числі й компресії, є методи, які використовують для приховування даних частотну область контейнера [3].

Метою роботи є підвищення захищеності інформації за рахунок розробки стеганографічної системи на основі методу приховування у частотній області зображення.

Технічне проектування системи

Архітектура системи приховування інформації в цифрових зображеннях складається з наступних блоків:

- блок приховування інформації;
- блок вилучення інформації;
- блок генерування стеганоключа;

Загальна схема архітектури стеганографічної системи зображена на рисунку 1.

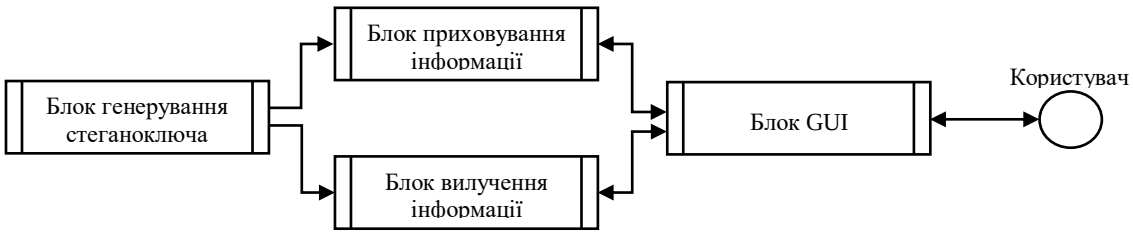

Рисунок 1 – Загальна схема архітектури стеганографічної системи

Кожен блок, що входить до складу архітектури виконує власні специфічні функції.

1) Блок приховування інформації призначений для реалізації вбудовування прихованого повідомлення в незаповнений контейнер. На вхід блоку надходять контейнер, стеганоключ та приховане повідомлення. Суть роботи блоку полягає у приховуванні бітів повідомлення за допомогою попередньо визначених стеганоключем позицій коефіцієнтів дискретного косинусного перетворення (ДКП). ДКП є базовим для стандарту JPEG [3].

2) Блок вилучення інформації призначений для реалізації вилучення прихованого повідомлення із заповненого контейнера. На вхід блоку надходять заповнений контейнер та стеганоключ. Даний блок відновлює приховане повідомлення на основі порівняння визначених коефіцієнтів ДКП із величиною P.

3) Блок генерування стеганоключа призначений для створення стеганоключа на базі введеного користувачем паролю. Блок перетворює символьний пароль в позиції коефіцієнтів ДКП, які будуть використовуватися для приховування та вилучення інформації.

4) Блок GUI призначений для відображення графічних компонентів програми.

Загальний алгоритм роботи стеганографічної системи зображений на рисунку 2.

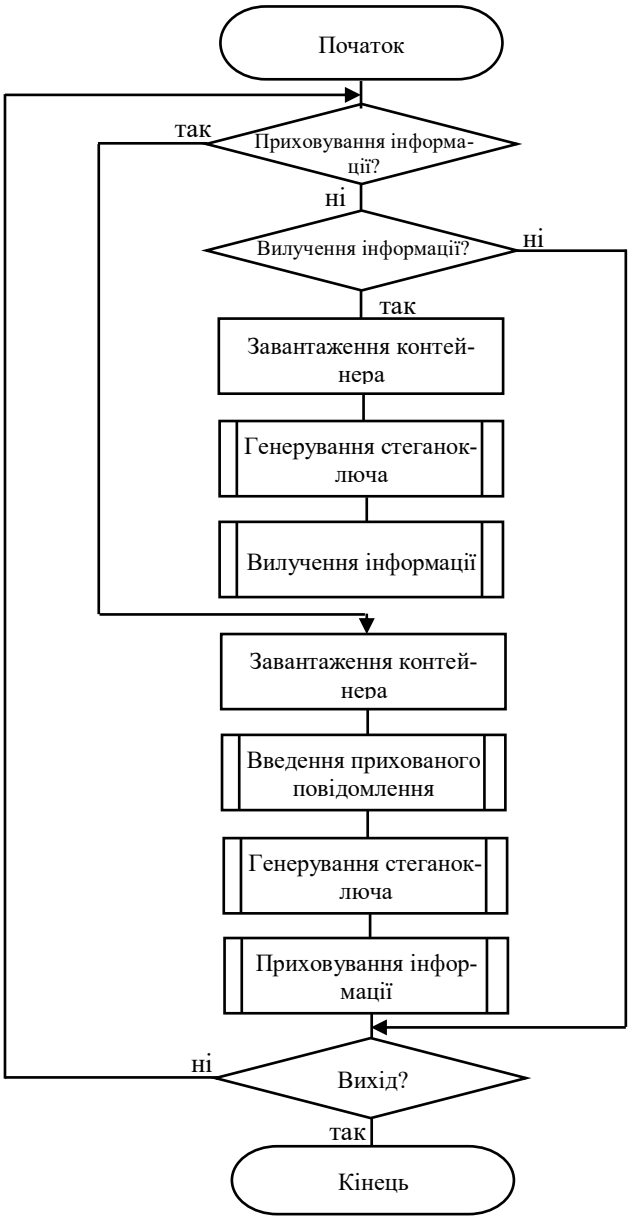

Рисунок 2 – Загальний алгоритм роботи стеганографічної системи

На основі розробленого алгоритму розроблено програмний засіб. Після запуску програми користувач бачить перед собою головне вікно програми. Користувачу доступні такі дії: «приховування повідомлення», «вилучення повідомлення» або «вихід».

1) «Приховування повідомлення»:
   a. Користувач натискає на кнопку «Відкрити» та в діалоговому вікні обирає файл-контейнер -> Програма перевіряє формат файлу, якщо користувач обрав файл із розширенням jpeg – завантажує контейнер, інакше користувач повинен обрати інший файл;
   b. Користувач вводить пароль -> Програма перевіряє довжину паролю, якщо введений пароль має довжину не менше 8-ми символів – користувач продовжує роботу з програмою, інакше користувач повинен ввести інший пароль;
   c. Користувач обирає тип введення секретного повідомлення -> Якщо користувач обирає введення через текстове поле, програма перевіряє довжину повідомлення, якщо обсяг повідомлення не перевищує максимально допустимий – користувач продовжує роботу, інакше користувач повинен ввести повідомлення меншої довжини. Якщо користувач обирає введення через текстове файл, програма завантажує повідомлення із текстового файлу, якщо обсяг повідомлення допустимий – користувач продовжує роботу, інакше користувач повинен обрати інший текстовий файл;
   d. Користувач натискає на кнопку «Приховати» -> Програма виконує приховання секретного повідомлення у контейнер. Якщо операція пройшла успішно користувач зберігає прихований контейнер, інакше виводиться повідомлення про помилку.
2) «Вилучення повідомлення»:
   a. Користувач натискає на кнопку «Відкрити» та в діалоговому вікні обирає заповнений контейнер -> Програма перевіряє формат файлу, якщо користувач обрав файл із розширенням jpeg – завантажує контейнер, інакше користувач повинен обрати інший файл;
   b. Користувач вводить пароль -> Програма перевіряє довжину паролю, якщо введений пароль має довжину не менше 8-ми символів – користувач продовжує роботу з програмою, інакше користувач повинен ввести інший пароль;
   c. Користувач натискає на кнопку «Вилучити» -> Програма виконує вилучення секретного повідомлення з контейнера. Якщо операція пройшла успішно користувач зберігає прихований контейнер, інакше виводиться повідомлення про помилку. Якщо користувач вводить вірний пароль, у текстовому полі буде відображено приховане повідомлення, інакше буде відображено випадковий набір символів.
3) «Вихід»:
   a. Користувач натискає на кнопку «Вихід» -> Програма завершує роботу.

Висновки

Розроблено архітектуру стеганографічної системи захисту інформації у цифрових зображеннях на основі методу приховування у частотній області зображення. Розроблено програмний засіб для приховування інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Кузнецов О. О. Стеганографія : навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. // – Х. : Вид. ХНЕУ, 2011. – 232с.
3. Васюра А.С., Лукічов В.В. Метод вбудовування даних у зображення за можливості jpeg-стиснення // Тези доповідей III Міжнародної конференції з оптоелектроних інформаційних технологій «Photonics-ODS 2008». – Вінниця, 2008. – С.33-34.

Телефус Дмитро Володимирович — студент групи 1БС-19м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dmytro.telefus@gmail.com

Лукічов Віталій Володимирович — кандидат технічних наук, старший викладач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua

Купершmейн Леонід Михайлович – кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: kupershtein@vntu.edu.ua

Telefus Dmytro V. — Student of 1BS-19m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: dmytro.telefus@gmail.com

Lukichov Vitaliy V. — Candidate of Technical Sciences, Senior Lecturer of the Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: lukichov.vitalyi@vntu.edu.ua,

Kupershtein Leonid M. – PhD, Associated Professor of the Information Protection Chair, Vinnytsia National Technical University, Vinnytsia.