УДК 514.18
Бурчак І.Н
Луцький національний технічний університет

# ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВПРОВАДЖЕННЯ ВЕКТОРНИХ РИСУНКІВ ДЛЯ ШИФРУВАННЯ В РАСТРОВІ НОСІЇ ПІД ЧАС ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ З ДИСЦИПЛІНИ "СТЕГАНОГРАФІЯ".

**Бурчак І.Н. Дослідження можливості впровадження векторних рисунків для шифрування в растрові носії під час виконання лабораторної роботи з дисципліни "Стеганографія".** В статті розглянута можливість використання векторних зображень, отриманих в CAD–системах, для шифрування з допомогою стеганографії. Стеганоконтейнерами при цьому являються растрові зображення, наприклад, різноманітні фотографії.
**Ключові слова:** стеганографія, стеганоконтейнер, CAD–системи, растрові та векторні зображення, скриті повідомлення, шифрування.

**Бурчак И.Н. Исследование возможности внедрения векторных рисунков для шифрования в растровые носители во время выполнения лабораторных работ по дисциплине "стеганография".** В статье рассмотрена возможность применения векторных изображений, полученных в CAD–системах, для шифрования с использованием методов стеганографии. При этом в качестве стеганоконтейнеров используются растровые изображения, например различные фотографии.
**Ключевые слова**: стеганография, стеганоконтейнер, CAD–системы, растровые и векторные изображения, скрытые уведомления, шифрование.

**Burchak I.N. Investigation of the possibility of implementation a vector figures in the bitmap images during the laboratory work from the discipline "Steganography".** The article considers the possibility of using vector images obtained in CAD systems for encryption using steganography. Carriers are bitmap images, for example, various photographs.
**Key words:** steganography, steganocontainer, CAD systems, raster and vector images, hidden messages, encryption.

**Постановка проблеми.** В даний час значно зростає роль використання різноманітних способів захисту передачі конфіденційних даних. Приховування одного зображення у іншому – це принцип стеганографії, який останнім часом використовується дуже широко:

- для захисту авторських прав, де впроваджуються ЦВЗ (цифрові водяні знаки);
- для захисту передачі даних у мережах VPN (віртуальних приватних мережах), де відбувається інкапсуляція (вбудовування) пакетів даних;
- для захисту передачі даних, шляхом приховування самого факту передачі даних, коли передається звичайний файл-контейнер (стеганоконтейнер), у якому вбудований файл з конфіденційними даними.

Комп'ютерна стеганографія використовує два файли:

- повідомлення – призначений для приховування;
- контейнер або стеганоконтейнер – для приховування в ньому повідомлення.

Під ключем розуміється секретний елемент, що визначає порядок занесення повідомлення в контейнер. Основними завданнями сучасної комп'ютерної стеганографії є забезпечення автентичності та цілісності файлу. Безпека ґрунтується на збереженні стеганографічним перетворенням основних властивостей переданого файлу при внесенні в нього секретного повідомлення і ключа[3].

**Аналіз останніх досліджень та публікацій.** В основі багатьох підходів до вирішення завдань стеганографії лежить спільна з криптографією методична база, яку заклав ще в середині минулого століття К. Шеннон (C.E. Shannon) [1,4]. Однак і досі теоретичні основи стеганографії залишаються практично недоопрацьованими. На сьогоднішній день існує багато програм, як початкового, так і професійного рівня (Steganos Security Suite, S-Tools, bmpPacker, OpenPuff та ін.), але відсутність лістингу цих програм не дозволяє аналізувати методи стеганографії, які застосовані в цих програмах.

Тому, під час виконання лабораторної роботи з дисципліни "Стеганографія та комп'ютерна графіка", яку вивчають студенти спеціальності "Кібербезпека" постало питання дослідження цілісності та автентичності файлу векторної графіки, після стеганографічних перетворень.

**Виклад основного матеріалу й обгрунтування отриманих результатів.** Для виконання лабораторної роботи з "Стеганографії та комп'ютерної графіки" студенти спеціальності –

Кібербезпека користуються програмою OpenPuff. Вона має ряд переваг, які обґрунтовують її використання у навчальному процесі:

- не потребує попередньої інсталяції;
- розмір папки з програмою складає 8,75 МБ (9 179 136 байт);
- є безкоштовною, тобто вільною від ліцензування (з відкритим вихідним кодом).

На рис.1 представлено інтерфейс головного вікна (зліва) та вікна програми OpenPuff для стеганографічного вбудовування (справа) графічних файлів-повідомлень у ланцюжок стеганоконтейнерів.

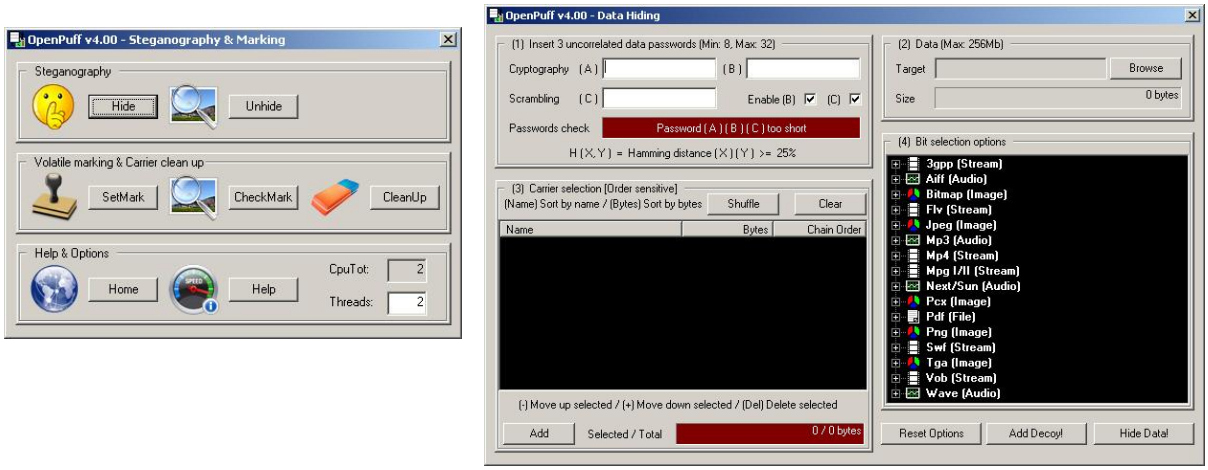


Рисунок 1. Головне вікно (зліва) програми OpenPuff та вікно для стеганографічного вбудовування графічних файлів (справа).

В мережі Інтернет описано, що вона добре працює з такими файлами у якості повідомленнь та стеганоконтейнерів – зображеннями, аудіо, відео, та файлами flash і adobe. Однак всі вони мають великий розмір. І при збільшенні розміру файлу-повідомлення, різко пропорційно збільшуватись мусить і файл, чи ланцюжок файлів-стеганоконтейнерів. Але у кафедральному домені кожна група студентів, яка має обліковий запис обмежена груповою квотою на розмір папки /**Home/Server, де студенти зберігають всі свої лабораторні роботи. І з ціллю зменшення обсягу групових папок ми провели дослідження можливості використання, в якості файлів повідомлень – векторних 3D твердотільних моделей, створених в CAD – системах комп'ютерної графіки.

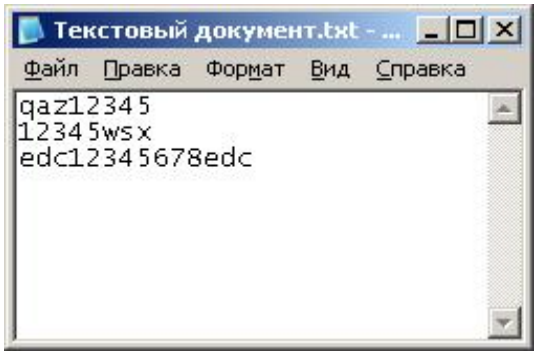


Рисунок 2. Паролі шифрування.

Як бачимо, у лівому верхньому куті вікна вбудовування програми OpenPuff пропонується ввести від одного до трьох паролей. Це дає можливість вводу додаткових шарів захисту повідомлення. Перед розміщенням повідомлення в контейнері буде проведено шифрування та перемішування даних. І хоча процесс витягнення файлу-повідомлення з контейнера має становити складний процесс обчислення – все ж основною характеристикою після цього має бути автентичність файлу-повідомлення з першоджерелом. Передача ключа робиться окремо і

заздалегідь, але у нашому (навчальному) випадку ми записуємо паролі окремим текстовим файлом, як на рис 2.

У правій частині вікна вбудовування (рис.1 справа) можемо також задати ступінь впровадження (заміни оригінальних пікселей на вбудовані з файла-повідомлення). Задається вона від мінімуму (12% - замінюється тільки один не значущий біт з восьми) і максимум (50% ), по замовчуванню стоїть значення 20%. Вибирається тип файлів стеганоконтейнера і вказується щільність впровадження даних, яка потім відображається у результаті обробки файлів – рапорті виконання завдання рис5.

На рис.3 приведено алгоритм взаємодії користувача та програмного забезпечення. Спочатку вводимо паролі, потім попередньо підготовлений файл повідомлення, і програма відразу вказує розмір файлу, який необхідно буде заховати у стеганоконтейнер. Попередньо також готуємо ряд фотографій, ланцюжок яких і zбуде служити стеганоконтейнером. Їх повинно бути достатньо, щоб вмістити при заданій щільності файл-повідомлення.

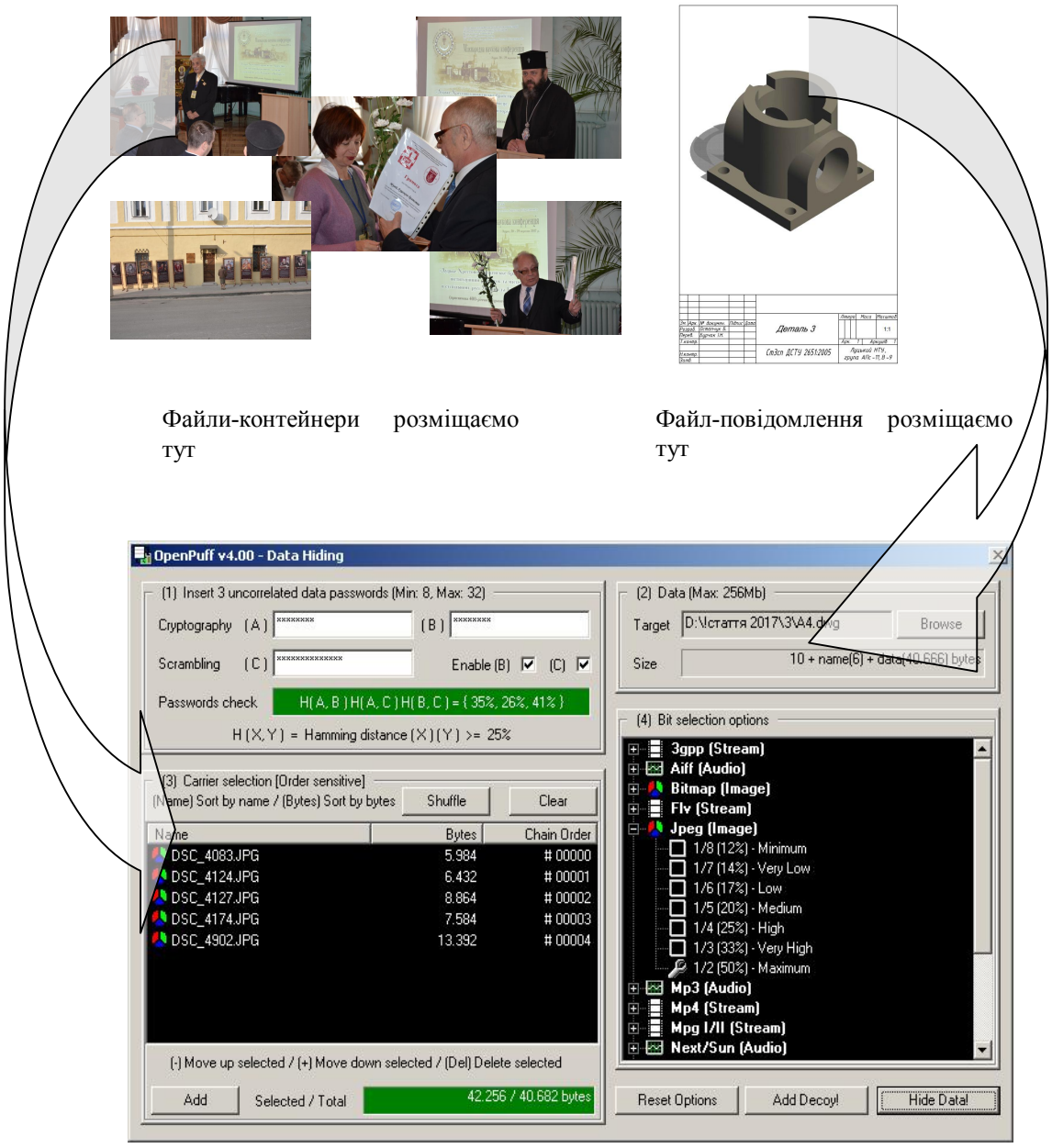


Рисунок 3. Вікно OpenPuff для вбудовування файлів.

Якщо файлів буде надлишкова кількість, то програма вкаже в рапорті, скільки файлів використано (рис4) у вікні завершення процесу.

Неабияке значення має порадок ланцюжка стеганоконтейнерів. При видобуванні файла-повідомлення він має бути незмінним, як і паролі. Вся ця інформація зберігається у протоколі завершення завдання як і ступінь заміни. Початок протоколу приведений на рис.5, закінчення – на рис.6.


Рисунок 4. Вікно завершення завдання.

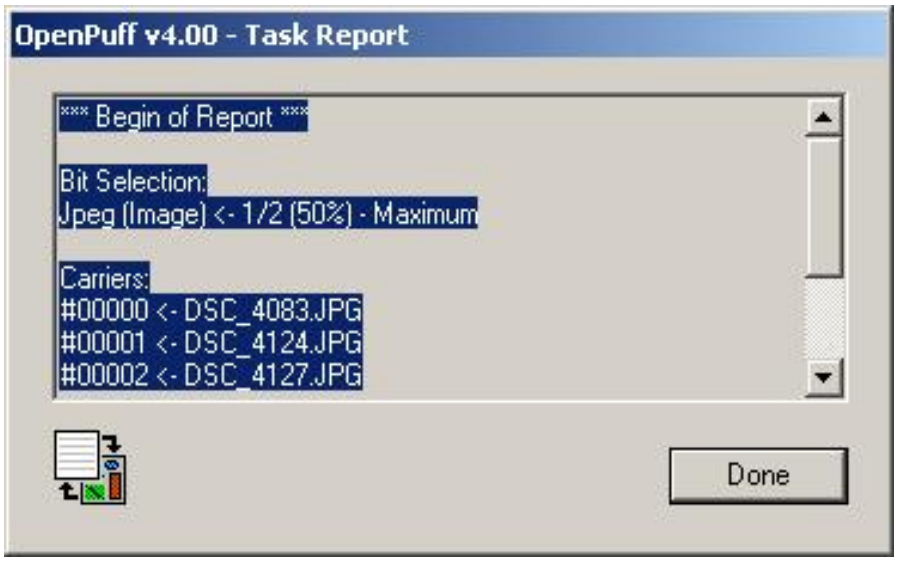


Рисунок 5. Протокол завершення завдання – початок.

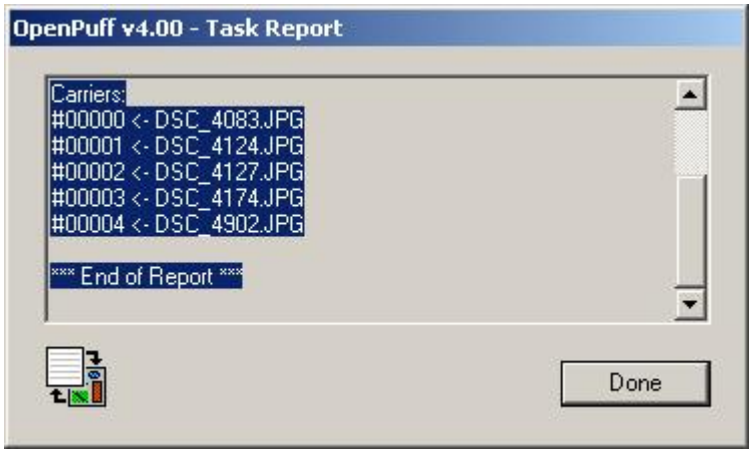


Рисунок 6. Протокол завершення завдання – закінчення.

Видобування файла- повідомлення із ланцюжка стеганоконтейнерів відбувається у такій же самій послідовності, як і в процесі вбудовування файлів. Попередньо створюється папка, куди має бути проведено витягування файлу-повідомлення. Протокол завершення завдання показаний на рис.7. Тепер можемо порівняти розмір та властивості видобутого файлу з стеганоконтейнера і файлу перщоджерела. Також перевіряємо його в AutoCAD, де він був початково створений

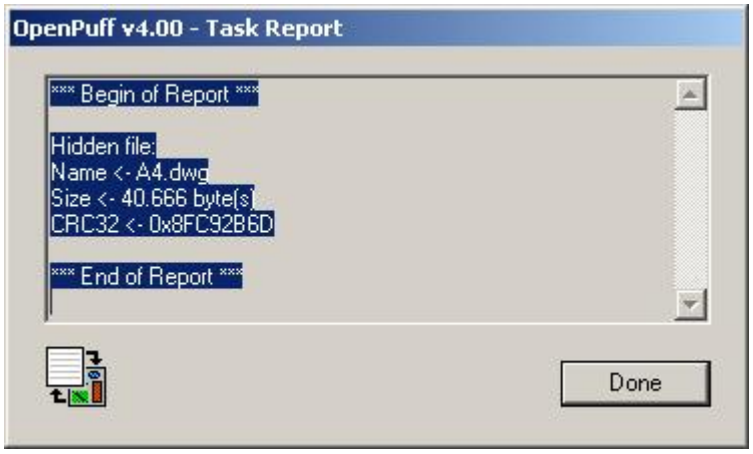


Рисунок 7. Протокол видобування файлу.

**Висновки та перспективи подальшого дослідження.** Беручи до уваги вищесказане, можна зробити висновок про те, що на сьогоднішній день залишається актуальною науково-технічна проблема удосконалення алгоритмів і методів проведення стеганографічного приховування конфіденційних даних або захисту авторських прав на певну інформацію. Стеганографія у комбінації з криптографією отримала новий поштовх для розвитку нових галузей мережевої, файлової і IP-телефонії.

1. C.E. Shannon, *A Mathematical Theory of Communication.* Bell System Technical Journal, 27 (1948), pp.379-423, 623-656.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: "МК-Пресс", 2006. — 288 с.
3. Навроцький Д.О. Методи комп'ютерної стеганографії. /Вісник Національного технічного університету України "КПІ" Серія – Радіотехніка. /Радіоапаратобудування.-2007.-№35, С105-108.
4. Шеннон К. Работы по теории информации и кибернетики. / Пер. с англ. — М.:Иностр. литература, 1963. — 829 с.