

ПРИХОВУВАННЯ ТЕКСТУ В ЗОБРАЖЕННЯХ

© Ковальчук А., Стащенко В., 2011

Побудовано стегосистему, яка відповідає таким положенням: інформацією є ключ, за допомогою якого тільки його власник може встановити факт присутності і зміст прихованого повідомлення; якщо ключ зберігається в таємниці, то неможливо дізнатися про зміст прихованого тексту, можливості у розпізнаванні або розкритті змісту прихованого повідомлення відсутні.

Ключові слова: стеганографічна система, діапазон ключа, зображення, криптоаналіз.

An stehosystemu that meets the following provisions: information is the key that allows only the owner can establish the existence and content of the hidden message if the key is kept secret, it is impossible to know the contents of hidden text, or in identifying possible declassification of the hidden message missing .

Keywords: steganographic system, a range of key images, cryptanalysis.

Вступ

Під цифровою стеганографією розуміють приховування однієї інформації в іншій. Причому приховування це має реалізуватися так, щоб, по-перше, не були втрачені властивості і деяка цінність інформації, що приховується, а по-друге, неминуча модифікація інформаційного носія не тільки не знищила смислові функції, але і на певному рівні абстракції навіть не змінювала їх. Тим самим факт передачі одного повідомлення усередині іншого не виявляється традиційними методами.

Можна виділити дві причини популярності досліджень у галузі стеганографії: обмеження на використання криптометодів у деяких країнах світу і поява проблеми захисту прав власності на інформацію, представлену в цифровому вигляді. Першою причиною пояснюється велика кількість досліджень у напрямку класичної стеганографії (тобто приховування факту передачі інформації), другою – ще більше робіт у галузі так званих водяних знаків. Цифровий водяний знак (ЦВЗ) – спеціальна мітка, непомітно впроваджувана в зображення або інший сигнал, щоби так чи інакше захищати інформацію від несанкціонованого копіювання, відстежувати розповсюдження інформації з мереж зв'язку, забезпечувати пошук інформації в мультимедійних базах даних.

Міжнародні симпозиуми з прихованих даних проводяться з 1996 року, з стеганографії перший симпозиум відбувся в липні 2002 року. Стеганографія – наука, яка швидко і динамічно розвивається, використовуючи методи і досягнення криптографії, цифрової обробки сигналів, теорії зв'язку та інформації.

Мета роботи

Побудова стійкого алгоритму приховування тексту в зображенні, а саме :

- забезпечення широкого діапазону ключа;
- захист від основних методів криптоаналізу;
- виключення можливості візуального розпізнавання деталей тексту.

Опис алгоритму шифрування

Вибирають зображення, яке буде контейнером для приховування тексту.

Вибирають текст для приховування, яке відбувається так:

1. Генеруються координати пікселя (x та y), в якому буде прихована перша літера.
2. Зчитується з тексту один символ.
3. Прочитаний символ зв'язують з таблицею символів, які задані в програмі.

4. Якщо символ існує в таблиці символів, то повертається його числовий код.
5. У контейнері генерується піксель, в який буде приховуватись символ.
6. Від каналу RGB цього пікселя віднімається числовий код з п. 2.4. Якщо результат від'ємний, то повернутися на пункт 2.5, інакше створюється піксель з новим значенням каналу RGB.
7. Отриманий піксель додається до нового зображення.
8. Виконуються пункти 2.2 – 2.7 до досягнення останнього символу тексту.
9. Нове зображення зберігається.

Дешифрування

1. Вибирається оригінальне зображення.
2. Вибирається зображення, в якому приховано текст.
3. Порівнюється піксель оригінального зображення і зображення, в якому приховано текст.
4. Різниця пікселів дає числове значення, яке відповідає конкретному символу, в результаті повертається символ.
5. Символ з п.4 додається до стрічки, яка зберігатиме всі символи.
6. Виконуються п. 3 – п.4 до досягнення останнього пікселя оригінального зображення.
7. Стрічка з п.5 зберігається у файлі.

Програмна реалізація алгоритму

Користуючись створеним програмним ужитком, користувач може приховати текстову інформацію у зображенні і зворотно її дешифрувати. Також у програмі є можливість порівняння двох зображень, що дає змогу користувачу побачити, де приховано текст. У програмі немає обмежень на розмір зображення. Програма підтримує такі типи зображень: *.jpg, *.png, *.tif, *.bmp. Текстова інформація для приховування повинна зберігатись у текстовому файлі з розширенням *.txt.

Розмір програми становить 40,0 КБ (40 960 байт). На операційній системі має бути встановлено пакет .NetFramework 2.0. Максимальний об'єм оперативної пам'яті, яку використовувала програма, становить 65 Мб при зображенні розширенням 1600x1200 та тексту з 13720 символів.

Опис методів і класів

CreateImage – клас призначений для опрацювання зображення, в якому присутні такі методи:

Public void Coding(Bitmap duplicatepicture, int NumberFromTextBox) – метод, призначений для приховування тексту в зображенні. Параметр duplicatepicture – передається новий Bitmap, в якому буде створено нове зображення, та параметр NumberFromTextBox для приймання номеру таблиці кодування.

public void EncodingText(Bitmap originalpicture, ref ProgressBar progress, int NumberOfTable) – метод, призначений для дешифрування тексту. Параметр originalpicture – передається Bitmap оригінального зображення, progress – для відображення процесу дешифрування у компоненті ProgressBar та NumberOfTable для приймання номеру таблиці кодування.

public Bitmap ChekingBothPicture(Image img, Bitmap bmp, ref ProgressBar progress) – метод, призначений для порівняння двох картинок для отримання пікселів, в яких приховані символи. Image img – змінна для оригінальної картинки, Bitmap bmp – для копії картинки, ref ProgressBar progress – передача стану ProgressBar для відображення стану роботи програми.

int CodeSymbol(Color c, Color c2) – метод призначений для порівняння двох пікселів для отримання числа закодованого символу. Color c і Color c2 – піксель оригінального зображення та його копії.

Клас *TransIterator* – клас, призначений для приймання числа символу для переведення його в букву і навпаки, прийняття букви і повернення його числового коду. Передбачає такі методи:

public int IntoUkrainian(char word, int numbtable) – метод, призначений для переведення символу в числовий код. char word – змінна для зберігання символу та int numbtable – код вибраної таблиці для кодування.

public char FromUkrainian(int number, int numbetable) – метод, призначений для переведення числового коду в символ. *int number* – змінна для зберігання числового значення, та *int numbetable* – код вибраної таблиці для кодування.

Клас *ChekingDate* – клас, призначений для збереження одного методу для перевірки достовірності картинки. У ньому присутній один метод:

public bool Validation() – метод, призначений для перевірки дат: чи збігається дата створення зображення з теперішньою датою дешифрування; якщо дати збігаються, повертає значення TRUE, і FALSE коли дати відрізняються.

Приклад та результати

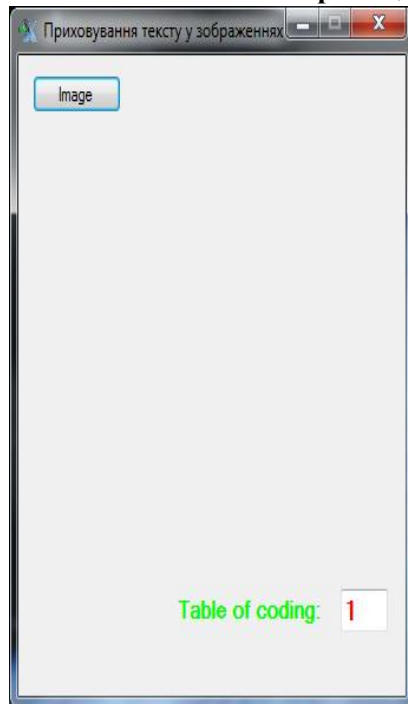


Рис. 1. Головне меню



Рис. 2. Вибір зображення

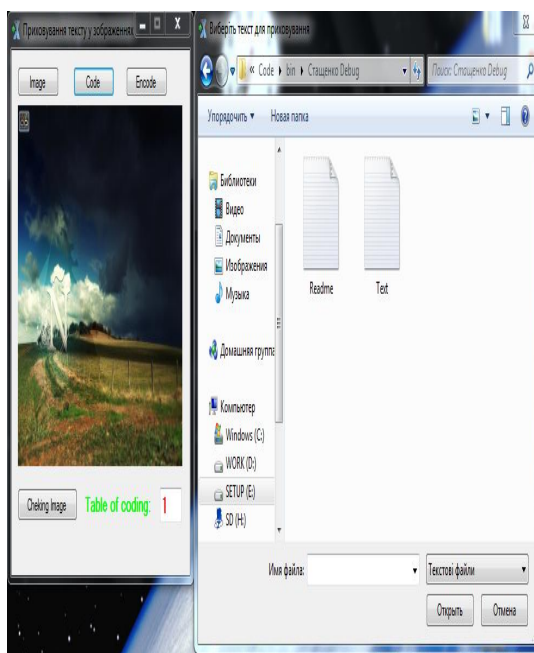


Рис. 3. Вибір тексту для приховування

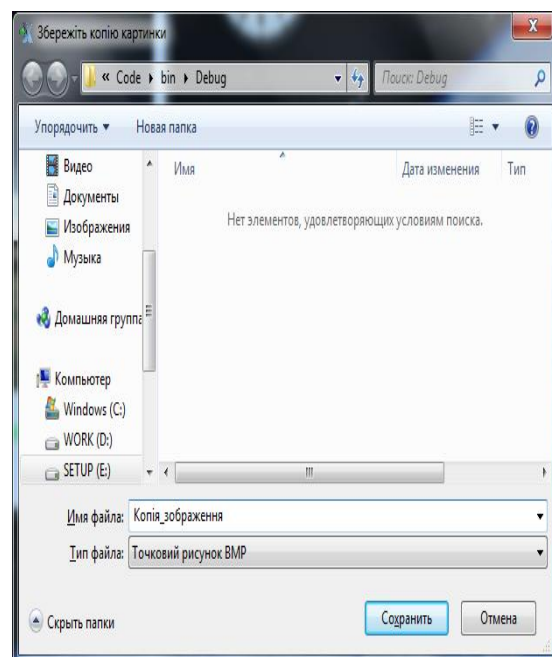


Рис. 4. Збереження зображення з прихованим текстом

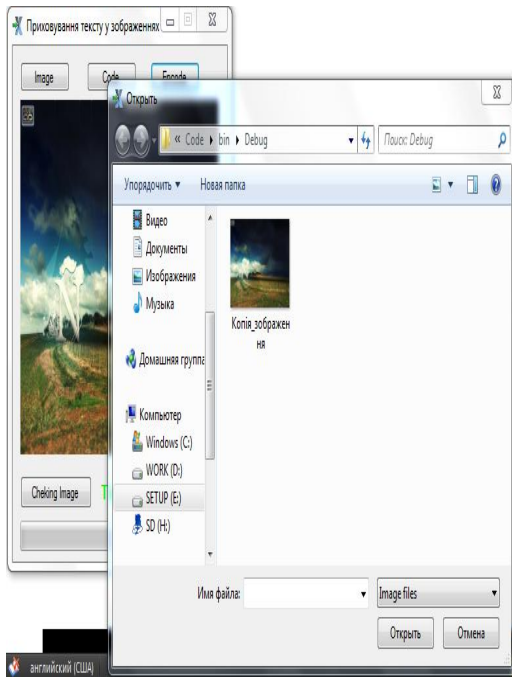


Рис. 5. Вибір зображення, в якому приховано текст

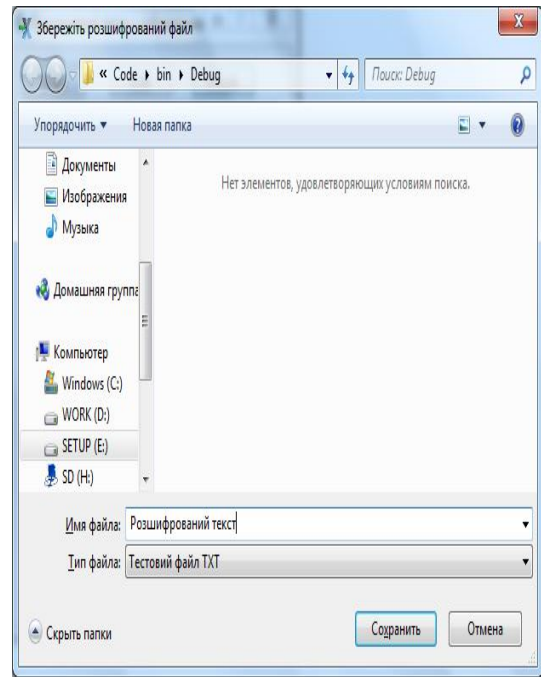


Рис. 6. Збереження дешифрованого тексту

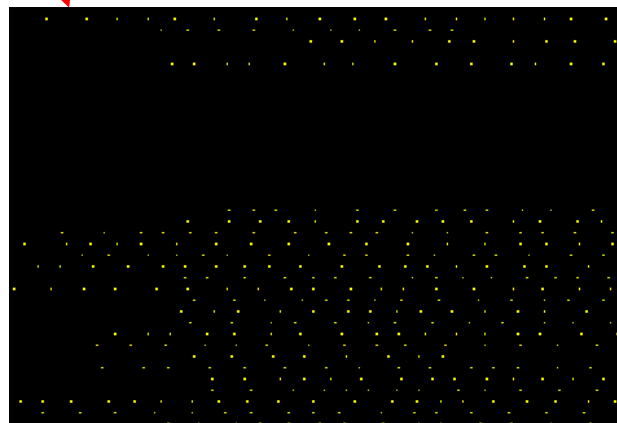
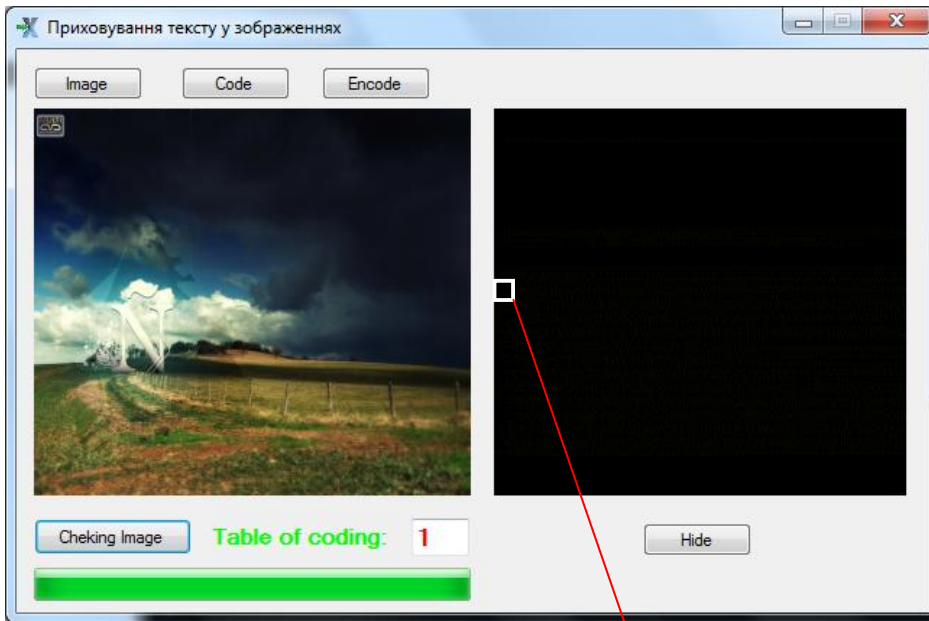


Рис. 7. Результат порівняння зображень

Висновок

З порівняння рис. 3 і рис. 7 видно, що початкове зображення (рис. 3) і зображення з прихованою інформацією (рис. 7) візуально не відрізняються. Тобто алгоритм може бути використаний для передавання графічних зображень. Запропоновані модифікації можуть бути використані стосовно будь-якого типу зображень але найбільших переваги отримують у випадку використання кольорових зображень, і зображень з чіткими контурами.

Для збільшення швидкодії можна здійснювати шифрування вектора з n елементів (по блоках пікселів, оскільки поелементний доступ до файлу займає більше машинного часу).

1. Бредли Л. Джонс, Питер Єйткен. *Освой самостоятельно C за 21 день.* – 6-е изд.; Пер. с англ. – М.: Вильямс, 2005. – С.555–561. 2. Нортон П., Йао П. *Программирование на Borland C++: В 2-х т.* – Т. 1. – К.: Диалетика, 1993. – С.47–48. 3. П Нортон П., Йао П *Программирование на Borland C++: в 2-х т.* – Т. 2. – К.: Диалетика, 1993. – С.12–14. 4. Вейскас Д. *Эффективная работа с Microsoft Access 7.0.* – П., 1997. – С. 19–48.

В. Юзевич, Н. Крап*

Фізико-механічний інститут ім. Г. В. Карпенка НАН України, Львів

* Львівський інститут економіки і туризму,
кафедра природничо-математичних дисциплін

МОДЕЛЮВАННЯ ТУРИСТИЧНИХ ПОТОКІВ З ВИКОРИСТАННЯМ МУРАШИНИХ АЛГОРИТМІВ

Ї Юзевич В., Крап Н., 2011

Запропоновано рекомендації щодо моделювання туристичних потоків з використанням мурашиних алгоритмів.

Ключові слова: туристичні потоки, моделювання, послуги, мурашині алгоритми.

The recommendation for the modelling of tourist streams with the use of ant algorithms is presented.

Keywords: tourist streams, modelling, services, ant algorithms.

Вступ

Туризм – це саме та галузь економіки, яка заслуговує в Україні на більшу увагу, оскільки вона може забезпечити нові робочі місця, збільшення надходжень до скарбниці держави від зовнішньоекономічної діяльності та поповнення бюджету через сплату податків [1].

Невід'ємною складовою світового туристичного процесу є вітчизняна туристична галузь. Попри всі політичні та соціально-економічні негаразди останніх років, індустрія туризму стала тією галуззю народного господарства України, яка з року в рік без залучення державних дотацій стабільно нарощує обсяги діяльності.

Туризм в Україні може і повинен стати сферою реалізації ринкових механізмів, джерелом поповнення державного та місцевих бюджетів, засобом загальнодоступного і повноцінного відпочинку та оздоровлення, а також ознайомлення з історико-культурною спадщиною та сьогоденням нашого народу і держави.

Постановка проблеми

Велика кількість ситуацій аналізу туристичних потоків, пов'язаних із складними системами та системами прийняття рішень, зводиться до задач оптимізації. Оптимізаційні проблеми такого типу можна описувати з допомогою мурашиних алгоритмів, оскільки в туризмі перспективним є