4. Лукаш С.И. Техника и технология анализа объектов для экологической и медицинской диагностики по запаху / С. И. Лукаш, О. К. Колесницкий, И. Д. Войтович // Комп'ютерні засоби, мережі та системи, - 2006, - №5, С.141-148.

5. Лукаш С. И. Особенности работы матричных полупроводниковых сенсоров в системе «ЭЛЕКТРОННЫЙ НОС». Ч.II. / С. И. Лукаш, И. Д. Войтович, З. В. Веткина, О. К. Колесницкий // Комп'ютерні засоби, мережі та системи. – 2008. - № 7. - С.101-109.

6. W. Maass, T. Natschläger, and H. Markram. Real-time computing without stable states: A new framework for neural computation based on perturbations. *Neural Computation*, 14(11):2531-2560, 2002.

7. Kolesnytskyj O. K. Optoelectronic Implementation of Pulsed Neurons and Neural Networks Using Bispin-Devices / O. K. Kolesnytskyj, I. V. Bokotsey, S. S. Yaremchuk // Optical Memory & Neural Networks (Information Optics). – 2010. – Vol.19. – №2. – P.154–165. – ISSN 1060-992X.

Надійшла до редакції
25.2.2013 р.

УДК 681.31.05

О.Н. РОМАНЮК, К.В. ОГОРОДНИК, В.В. МАРТИНЮК
Вінницький національний технічний університет

СИСТЕМА СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ПОВІДОМЛЕНЬ

В статті запропоновано систему стеганографічного захисту повідомлень у вигляді bmp-зображень з двома рівнями захисту: стеганографічним та криптографічним. Проведено оцінку параметрів надійності запропонованої системи.

Ключові слова: стеганографія, криптографія, захист повідомлень, обробка bmp-зображень.

The article proposed steganographic system security messages as bmp-images with two levels of protection: steganographic and cryptographic. The estimation of reliability parameters of the developed system is carried out.

Keywords: steganography, cryptography, defense communications, processing bmp-images.

Вступ

Інформація є одним із найцінніших предметів сучасного життя. Отримання доступу до неї з появою мережі Інтернет стало досить простим. З іншого боку, легкість та швидкість такого доступу значно підвищили загрозу порушення безпеки даних при відсутності заходів їх захисту – загрозу несанкціонованого доступу до інформації.

Задача надійного захисту авторських прав, прав інтелектуальної власності або конфіденційності даних від несанкціонованого доступу є однією із найстаріших і повністю невирішених на сьогодні проблем. В зв'язку із стрімким розвитком комп'ютерних технологій питання захисту інформації, що представлена у цифровій формі, є надзвичайно актуальним. І, як наслідок, актуальним є розробка нових методів захисту інформації з підвищеною надійністю.

Обгрунтування методу стеганографічного захисту повідомлень

На сьогодні найбільш поширеними методами захисту інформації є методи криптографії та стеганографії [1].

Криптографічний захист інформації полягає у зміні останньої з метою зробити її незрозумілою для оточуючих. Але наявність закодованого повідомлення сама по собі привертає увагу і зловмисник, маючи криптографічно захищений файл, одразу розуміє про наявність секретної інформації у ньому і спрямовує всю потужність своєї комп'ютерної системи на дешифрування даних.

Стеганографічний захист інформації має на меті приховати сам факт існування секретної інформації, щоб у зловмисника взагалі не виникало підозр про наявність цієї прихованої інформації. В іншому випадку проблема інформаційної безпеки знову повертається до стійкості криптографічного коду [2]. Таким чином, стеганографія зазвичай не замінює криптографію, а доповнює її.

Загальний процес стеганографії можна виразити простою формулою: в сучасному розумінні стеганографічна система – це сукупність засобів та методів, що використовуються для формування прихованого каналу передачі інформації.

Запропонований нами метод також включає в себе стеганографічну та криптографічну складову. Загальна структурна схема стеганографічної системи захисту повідомлень наведена на рис. 1.

Для запропонованого нами методу:

контейнер – будь-яке зображення формату.bmp (наприклад, листівка з поздоровленнями);

повідомлення – будь-яка текстова інформація, також представлена у вигляді зображення формату.bmp.

Алгоритм захисту повідомлення буде включати наступні етапи: криптографічне перетворення вхідного повідомлення відповідно до введеного ключа, вбудовування закодованого повідомлення у контейнер, передача заповненого контейнеру до отримувача, зворотні перетворення з метою видобуття повідомлення з контейнеру. Зрозуміло, що при невірному введенні ключа, повідомлення вірно не видобувається. Розглянемо кожен з етапів більш докладно.

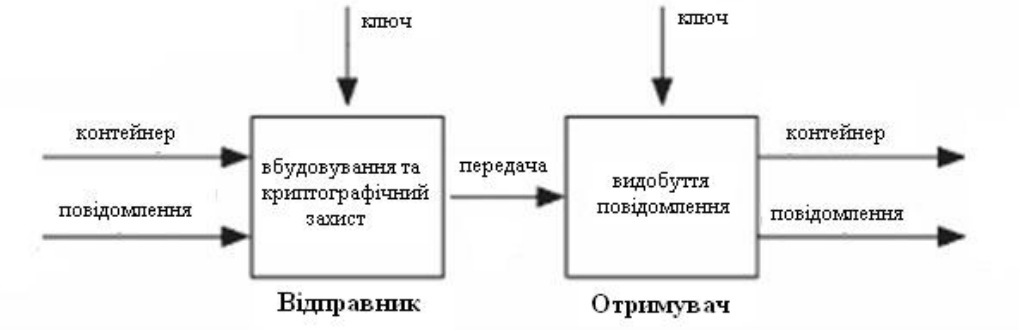
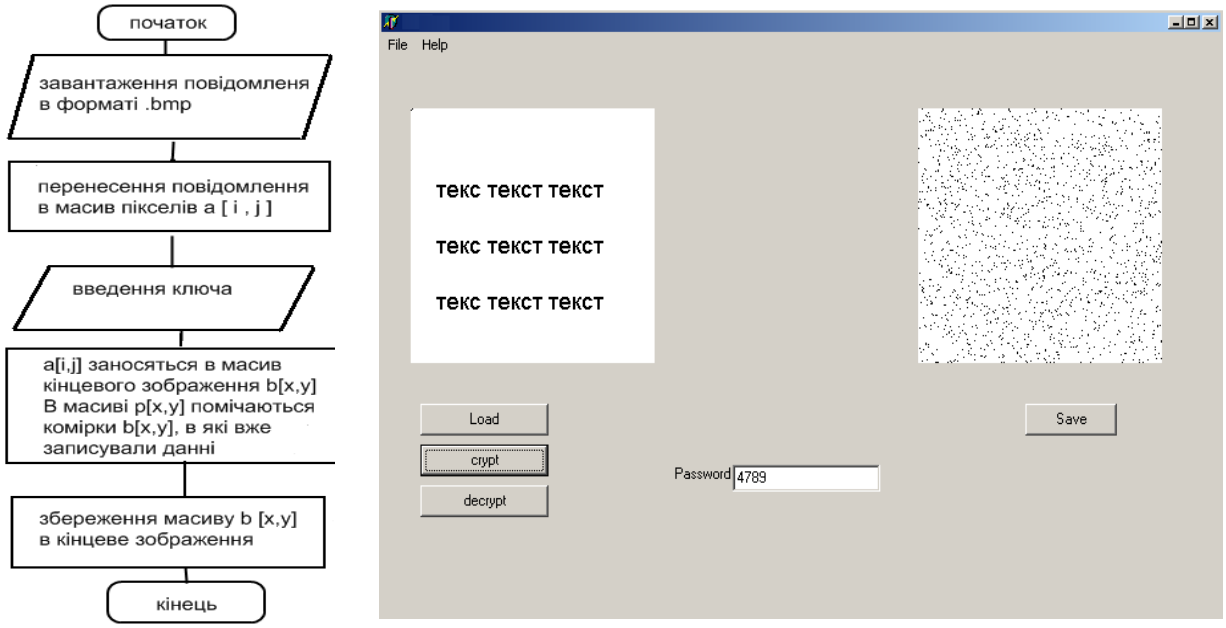


Рис. 1 – Структурна схема стеганографічної системи захисту повідомлень

Реалізація криптографічного захисту вхідного повідомлення

Було розроблено алгоритм потокового побітного кодування текстових повідомлень, представлених у вигляді bmp-зображення, схожий до представленого нами у [3]. Цей алгоритм відрізняється можливістю використання 32 бітного ключа, до складу якого можуть входити як цифри, так і будь-які інші символи з таблиці ASCII.

На рис. 2а наведено блок-схему розробленого алгоритму кодування, тестова програмна реалізація якого наведена на рис. 2б.



а) **б)**

Рис. 2. Блок-схема алгоритму кодування повідомлення та загальний вигляд тестової програми в процесі кодування

В робочому вікні розміщене поле для вводу ключа, який може набувати довільного значення розміром 32 біти. Згідно цього ключа генератор псевдовипадкових чисел генерує послідовність перестановки пікселів початкового повідомлення у закодоване. Початкове зображення вноситься в масив для обробки a[i, j]. Пікселі з основного масиву зображення a[i, j] почергово заносяться в масив кінцевого зображення b[x, y] (x, y-випадкові величини). В масиві p[x, y] помічаються комірки b[x, y], в які вже записувались данні. З масиву b[x, y] дані формуються у кінцеве зображення, яке передається по відкритому каналу.

Декодування відбувається в зворотному порядку згідно заданого ключа. В випадку вводу вірного ключа ми отримаємо початкове повідомлення, а у випадку коли ключ невірний – отримується шумове зображення схоже на закодоване.

Даний метод кодування має високу надійність внаслідок великої кількості можливих перестановок (оцінка надійності наведена нижче), але передача закодованого зображення звичайно викличе увагу зловмисників, хоч це зображення і можна прийняти за звичайний шум. Тому факт передачі такого закодованого повідомлення бажано приховати, що буде здійснено за допомогою методів стеганографії.

Реалізація стеганографічного захисту вхідного повідомлення

Стеганографічна частина запропонованого методу захисту повідомлень призначена головним чином для приховування факту криптографії, тому відсутня необхідність використання складного трудомісткого методу стеганографії. Достатньо обрати один з відомих, який є чи не найпростішим.

Для реалізації стеганографічного захисту повідомлень було обрано метод найменших значущих бітів (Least Significant Bit, LSB) [4]. Цей метод є найбільш поширеним в цифровій стеганографії. Розглянемо

LSB метод на прикладі 24-бітного BMP-зображення. Кожен піксель такого зображення кодується 1-м байтом, що визначає інтенсивність кольору зображення. Науково підтверджений факт, що система людського зору найменш чутлива до змін інтенсивності кольору. Заміна молодшого біту пікселя дозволяє помістити в зображення закодовану інформацію та візуально не змінює зображення. Використаємо цю властивість у нашому методі.

Розроблена програмна реалізація методу та результати її роботи наведені на рис. 3, 4.

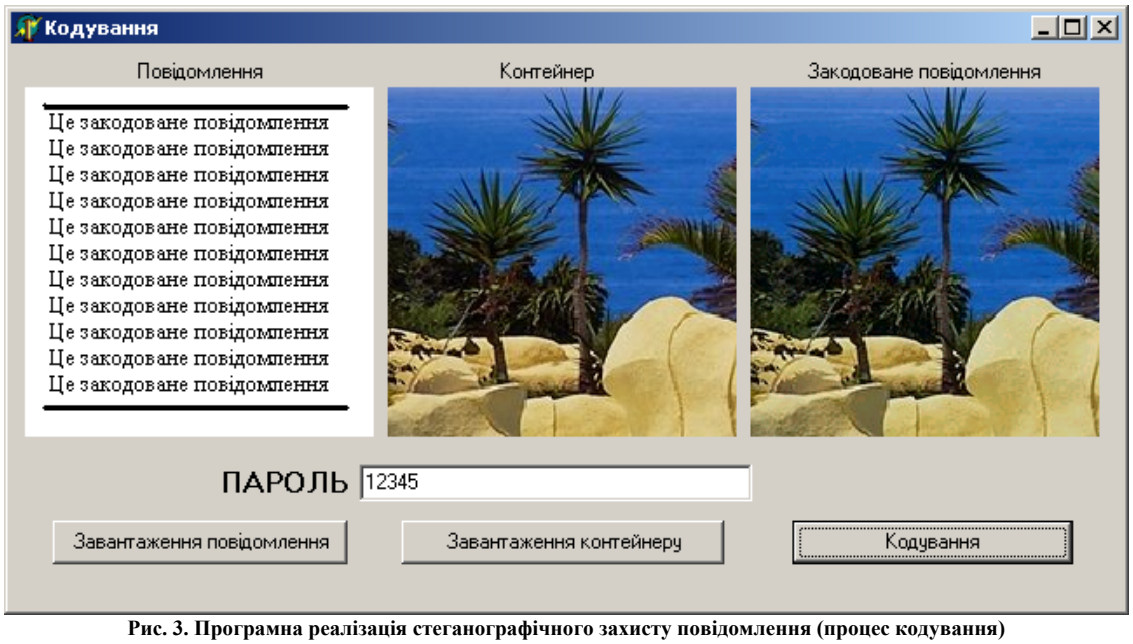


Рис. 3. Програмна реалізація стеганографічного захисту повідомлення (процес кодування)

Робота програми полягає в наступному. Завантажується вхідне повідомлення та контейнер у вигляді bmp-зображень. Після введення ключа (пароля) та натискання кнопки “Кодування” програма проводить криптографічне кодування повідомлення та вбудовує його у контейнер. Результат цих дій відображається на екрані та з’являється діалог для збереження отриманого наповненого контейнеру. Збережений файл (також bmp-зображення) передається через відкритий канал до отримувача. Як видно з рис. 3, пустий та наповнений контейнери візуально не відрізняються один від одного. Тому факт криптографії цілком прихований.

Після отримання повідомлення, воно завантажується у другий модуль програми і після введення ключа відбувається видобуття повідомлення. Якщо введено невірний ключ, вірного декодування повідомлення не відбувається, що відображено на рис. 4.

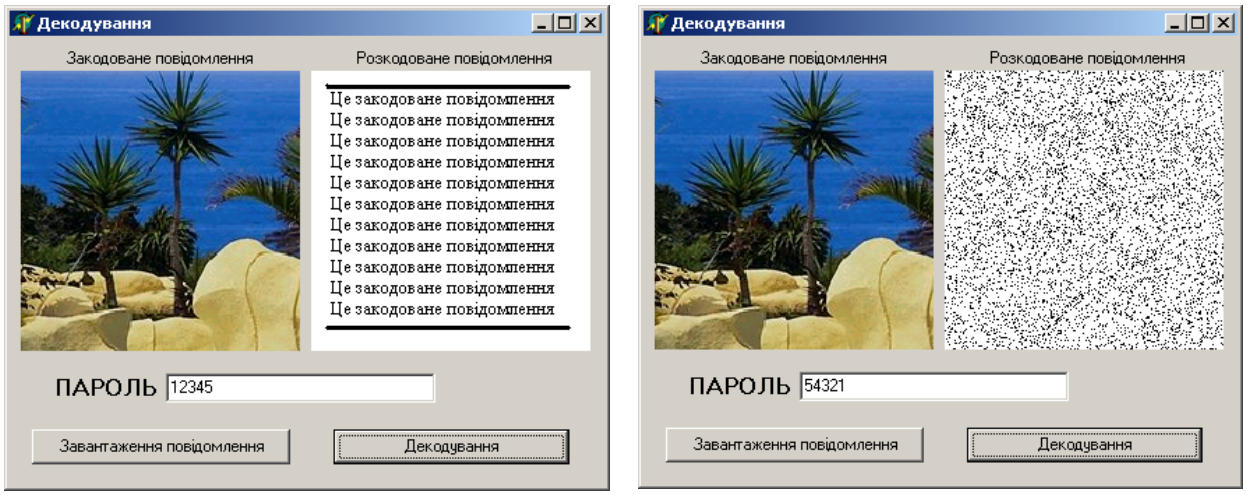


Рис. 4. Приклади декодування повідомлення при вірному та невірному введенні ключа

Таким чином, розроблена система стеганографічного захисту повідомлень є дієздатною.

Оцінка криптостійкості розробленого методу

Головними параметрами, за якими оцінюється ефективність методів захисту інформації, є надійність захисту (криптостійкість) та завадостійкість до часткових втрат інформації. Оцінимо кожен з вказаних параметрів.

Розроблена система має два ступеню захисту: стеганографічний та криптографічний.

Стеганографічний захист, як уже зазначалось, призначено для приховування факту наявності прихованого повідомлення і ми обрали існуючий відомий простий метод. Тому його криптостійкість досить низька при знанні зловмисником алгоритму LSB і оцінювати її ми не будемо.

Оцінимо криптографічний ступінь захисту. Вхідними даними є зображення розміром n x m. Розмір зображення, що відповідає формату аркуша паперу А4 при роздільній здатності 100 точок на дюйм та полях по 5мм, складає 787x1130 точок. Отже, маємо матрицю вхідних елементів розміром 787x1130. В процесі шифрування здійснюються перестановки елементів матриці. Загальна кількість можливих перестановок буде визначатися виразом (n x m)!. При заданому розмірі матриці кількість можливих перестановок дорівнює (787x1130)!=889310!. Величина даного числа робить неможливим дешифрування шляхом повного перебору варіантів перестановок ні за який прийнятний час, так як при швидкодії сучасних надкомп'ютерів це займе мільйони років. Якби перестановки здійснювалися за дійсно випадковим законом, то даний метод забезпечував би абсолютну криптостійкість, при використанні кожного разу при шифруванні нової випадкової послідовності розмірністю (n x m) елементів. Проте перестановки здійснюються псевдовипадковим чином, послідовність яких задається генератором псевдовипадкових чисел з нормальним законом розподілу. Ініціалізація генератора псевдовипадкових чисел здійснюється 32-розрядним ключем. Даний ключ фактично і буде визначати криптостійкість методу. При використанні 32-бітного ключа маємо 256^{32} можливих комбінацій перестановок. При забезпеченні швидкості дешифрування 1 комбінація за 1 с, повний перебір можливих комбінацій займе десятки років. Результатом дешифрування є зображення, тому для здійснення автоматичного дешифрування шляхом повного перебору необхідно вирішити проблему розпізнавання зображень, тобто зробити висновок, чи є даний набір елементів в даній послідовності деяким змістовним повідомленням, що цілком може зробити людина, але не комп'ютер. Тому суттєво збільшити швидкість автоматичного дешифрування при повному переборі на даний час є неможливим.

Таким чином, даний метод забезпечує криптостійкість закриття інформації в десятки років. Для уникнення накопичення статистичних даних для здійснення розкриття необхідно використовувати кожного разу в процесі шифрування новий випадковий ключ. Збільшення розміру ключа дозволяє підвищити криптостійкість методу.

Оцінка завадостійкості методу

Операції кодування здійснюються над даними картинного типу, які характеризуються надлишковістю. Так, наприклад, при використанні шрифту розміром 28, літера А буде передаватися матрицею 25x25 точок (рис. 5). Окрім цього, в процесі шифрування здійснюється розсіювання елементів матриці по всьому полю зображення випадковим чином за нормальним законом розподілу. Використання надлишковості зображень та їх розсіювання робить даний метод закриття інформації завадостійким до впливу зосереджених та розосереджених завад та втрат. Так, при втраті до 50 % елементів закодованого зображення є можливість відновити початкове повідомлення, як це видно на прикладі літери А

Рис. 5. Приклад втрати частини інформації про літеру А

Висновки

Розроблено та реалізовано систему стеганографічного захисту повідомлень.

Проведено оцінку параметрів розробленої системи, яка показала високий ступінь криптостійкості (десятки років) та завадостійкості (до 50 відсотків втрати інформації) системи.

Література

1. Баричев С. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия-Телеком, 2002. – 175 с.

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

3. Красиленко В. Захист інформації при факсимільному передаванні документів / В.Г.Красиленко, О.О. Лазарєв, К.В. Огородник // Збірник праць НПК «Прогресивні інформаційні технології в науці та освіті». – Вінниця, 2007. – С. 167-170.

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

Надійшла до редакції
04.2.2013 р.