Електронне наукове фахове видання "Ефективна економіка" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)

Ефективна ЕКОНОМІКА

Дніпровський державний аграрно-економічний університет

ДКС Центр Видавництво ТОВ «ДКС-центр»

Ефективна економіка № 5, 2017

УДК 004.056

В. О. Денисюк,
к. т. н., доцент, доцент кафедри економічної кібернетики,
Вінницький національний аграрний університет, м. Вінниця

СТЕГАНОГРАФІЧНИЙ АЛГОРИТМ ЗАХИСТУ ДАНИХ З ВИКОРИСТАННЯМ ФАЙЛІВ ЗОБРАЖЕНЬ

V. Denysiuk,
PhD, associate professor, associate professor of economic cybernetics department,
Vinnytsya national agrarian university, Vinnytsya

STEGANOGRAPHY ALGORITHM OF DATA PROTECTION BY IMAGE FILES

Розроблено стеганографічний алгоритм за методом LSB. Алгоритм підвищує рівень захисту інформації від несанкціонованого доступу. Конфіденційна інформація приховується у файлах зображень. Отримав подальший розвиток метод приховування даних у молодших бітах пікселів файлів зображень. Це не змінює візуальну якість зображення та ускладнює виявлення факту приховування інформації.

Steganography LSB-method algorithm is worked. An algorithm promotes the level of priv from an unauthorized division. Confidential information hides in the files of images. The method of concealment of data got further development in the junior bats of pels of files of images. It does not change visual quality of image and complicates the exposure of fact of information concealment.

Ключові слова: *економічна інформація, стеганографія, LSB-метод, алгоритм, захист інформації, файл зображення, приховування інформації.*

Keywords: *economic information, steganography, LSB– method, algorithm, priv, file of image, concealment of information.*

Постановка проблеми

Дуже часто при зберіганні та передачі інформації, а особливо економічної або фінансової інформації, виникає потреба у її приховуванні від сторонніх очей. Чим більша цінність інформації тим більшого захисту вона потребує. Наприклад, такі компанії як Apple або Samsung доводять різноманітними засобами у тому числі і судовими позивами, що використані ними технології є неповторними та інноваційними, що їхні права на використання цих можливостей є автономними. Відповідну інформацію можна використовувати для здобуття надприбутків і розвитку певних галузей.

Для гарантованого захисту вмісту повідомлення існує два різних підходи [1-3]:

1) блокування несанкціонованого доступу до інформації шляхом шифрування повідомлення;

2) повідомлення, яке передається, намагаються приховати так, аби його неможливо було знайти.

За першим підходом використовують криптографічні методи захисту. У криптограмах, як правило, відсутні структура

і закономірності, які властиві відкритим текстам. Тому, при проведенні моніторингу мереж телекомунікацій, вони легко автоматично виділяються з інформаційного потоку.

Другий підхід застосовує стеганографічні методи захисту, які значно знижують ймовірність її виявлення. На відміну від криптографічного захисту, коли у «зловмисника» існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, стеганографічні методи дозволяють вмонтувати інформацію, що передається, в невинні на вигляд послання так, щоб не можна було навіть запідозрити існування підтексту.

Шанси знайти приховане повідомлення невеликі, але на той випадок, якщо повідомлення буде виявлено, його можна ще додатково зашифрувати. У цьому випадку стеганографія являє собою більш високий рівень захисту інформації в порівнянні з методами криптографії.

Не існує абсолютно надійного способу зашифрувати інформацію. Кращий спосіб захистити її – це приховати сам факт її існування. Цим стеганографія перевершує криптографію [3].

Аналіз останніх досліджень і публікацій

Визначення суті технічної проблеми. Стеганографія (steganos – секрет, таємниця; graphy – запис) відома ще з стародавніх часів [2, 5], на тепер – це, по-перше, метод приховування певного повідомлення в іншому (яке є свідомо великим), таким чином, що неможливо побачити присутність або сенс прихованого повідомлення; по-друге, цифрова стратегія приховування файлу в мультимедійному форматі (наприклад: картинка, звуковий файл – WAV, MP3 або відео файл).

Науково-технічний прогрес дозволив стеганографії зайняти певну нішу у галузі захисту інформації, з’явився такий напрям в області захисту інформації, як комп’ютерна стеганографія. Комп’ютерна стеганографія – це фактично приховування одного файлу в іншому.

Прогрес в області глобальних комп'ютерних мереж і засобів мультимедіа привів до розробки нових методів безпеки передачі даних по каналах телекомунікацій і використання їх в неоголошених цілях. Ці методи, враховуючи природні неточності пристроїв дискретизації і надмірність аналогового відео або аудіо сигналу, дозволяють приховувати повідомлення в комп'ютерних файлах (контейнерах).

У сучасному інформаційному просторі стеганографічні системи активно використовуються для вирішення таких основних завдань [1]:

1) захист конфіденційної інформації від несанкціонованого доступу;

2) подолання систем моніторингу та управління мережевими ресурсами;

3) камуфлювання програмного забезпечення;

4) захист авторського права на деякі види інтелектуальної власності.

Найбільш ефективна задача стеганографії – захист інформації. Так, наприклад, одна секунда оцифрованого звуку з частотою дискретизації 44100Гц та 8-бітним рівнем відліку у стереорежимі дозволяє приховати за рахунок зміни найменш значимих молодших розрядів повідомлення у 10 Кбайт. Такий підхід дозволяє досягти змін у 1%, яких людина при прослуховуванні не здатна помітити, але при розшифруванні чи зчитуванні певним чином, дозволяє зберегти інформацію. Цей приклад дає ілюстрацію можливостей стеганографії. Також треба зазначити, що без спеціальних засобів збережену інформацію не можливо отримати із файла-контейнера.

Стеганографічні методи також спрямовані на протидію системам моніторингу та управління мережевими ресурсами промислового шпигунства, дозволяють протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери керування локальних і глобальних обчислювальних мереж. Для корпорацій та державних відомств, що зберігають важливі масиви даних, це одна із неоціненних функції стеганографії.

Іншим важливим завданням стеганографії є камуфлювання програмного забезпечення (ПЗ). У тих випадках, коли використання ПЗ незареєстрованими користувачами є небажаним, воно може бути закамуфльовано під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано в файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

Прикладом використання стеганографії у захисті авторського права від піратства є нанесення спеціальної мітки на комп'ютерні графічні зображення. Мітка залишається невидимою для очей людини, але розпізнається спеціальним ПЗ, яке вже використовується в комп'ютерних версіях деяких журналів. Даний напрямок стеганографії призначений не тільки для обробки зображень, але і для файлів з аудіо– та відеоі– нформацією й забезпечює захист інтелектуальної власності.

Важливим і перспективним є кожне із названих завдань стеганографії. Розуміння проблем захисту інформації та її безпеки полягає у подальшому розвитку питань і шляхів їх вирішення, які може запропонувати стеганографія.

Існуючі способи вирішення технічної проблеми. Для приховування інформації у цифровому вигляді за допомогою стеганографії існують спеціальні алгоритми. Внесення нової інформації у вже наявні файли (наприклад, мультимедійні) призводить до спотворенн, які перебувають нижче порогу чутливості людини, тому це не викликає помітних змін у сприйнятті вхідних файлів. Крім того, в оцифрованих об’єктах, які початково мають аналогову природу, завжди існує шум квантування, тому потім при відтворенні цих об’єктів з’являється додатковий аналоговий шум і нелінійні спотворення, які сприяють приховуванню інформації [3].

До недавнього часу для опису «класичної» моделі стеганографічної системи (стегосистеми), використовувалася запропонована 1983 Г.Сіммонсом «проблема ув'язнених», в якій ув’язнені приховано бмінюються інформацією про втечу. Модель полягає у тому, що два індивідуми хочуть обмінюватися секретними повідомленнями без втручання охоронця, який

контролює комунікаційний канал. Мають місце ряд припущень, які роблять цю проблему розв'язуваною. Перше припущення полегшує вирішення проблеми і полягає в тому, що учасники інформаційного обміну можуть розділяти секретне повідомлення (наприклад, використовуючи кодову клавішу) перед укладанням. Інше припущення, навпаки, ускладнює вирішення проблеми, так як охоронець має право не тільки читати повідомлення, але й модифікувати (змінювати) їх. У 1996 році було запропоновано використовувати нову єдину термінологію і основні терміни (конференція Information Hiding: First Information Workshop) [7, 9]. Стегосистема розуміється як сукупність засобів і методів, що використовуються для формування прихованого каналу передачі інформації.

При побудові стегосистеми необхідно враховувати:

1) зловмисник має повне уявлення про стегосистему і деталі її реалізації, єдиною інформацією, яка залишається невідомою, є ключ, за допомогою якого тільки його власник може встановити факт наявності і зміст прихованого повідомлення;

2) якщо зловмисник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому отримати подібні повідомлення в інших даних до тих пір, доки ключ зберігається у таємниці;

3) потенційний зловмисник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

У якості контейнера (повідомлення) може використовуватися будь-яка інформація призначена для приховування таємних повідомлень. Повідомленням може бути як текст або зображення, так і, наприклад, аудіодані (файли мультимедіа) тощо. Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер (стег) – контейнер, що містить вбудовану інформацію. Вбудоване (приховане) повідомлення – повідомлення, вбудовується в контейнер. Стеганографічний канал або просто стегоканал – канал передачі стег. Стегоключ або просто ключ – секретний ключ, необхідний для приховування інформації. В залежності від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) в стегосистеми може бути один або декілька стегоключів.

За аналогією з криптографією, за типом стегоключа стегосистеми можна поділити на системи з секретним ключем та системи з відкритим ключем.

У стегосистеми з секретним ключем використовується один ключ, який повинен бути визначений або до початку обміну секретними повідомленнями, або переданий по захищеному каналу. Такий варіант вибору ключа є менш ефективним, оскільки зловмисник, перехопивши цей ключ отримує подальший доступ до даних.

У стегосистеми з відкритим ключем для вбудовування і отримання повідомлення використовуються різні ключі, такі, що за допомогою обчислень неможливо вивести один ключ з іншого. Тому один ключ (відкритий) може передаватися вільно по незахищеному каналу зв'язку. Крім того, дана схема добре працює і при взаємній недовірі відправника і одержувача. Тому вибір такого ключа є більш корисним і забезпечує високий рівень захисту.

Отже, стегосистема має відповідати таким вимогам:

1) властивості контейнера повинні бути модифіковані таким чином, щоб зміни неможливо було виявити при візуальному контролі, що визначає якість приховування повідомлення (для безперешкодного проходження стегоповідомлення каналами зв'язку воно не повинно привернути увагу);

2) стегоповідомлення повинно бути стійким до спотворень, в тому числі і до зловмисних (у процесі передачі зображення, звука або використання інших контейнерів можуть відбуватися різні трансформації зі зменшення або збільшення, перетворення в інший формат, ущільнення, в тому числі і з використанням алгоритмів з втратою даних тощо);

3) для збереження цілісності вбудованого повідомлення необхідно використовувати коди з виправленням помилок;

4) для підвищення надійності вбудоване повідомлення має бути продубльовано.

Різноманітні алгоритми реалізації задовільняють перерахованим вимогам.

На тепер найбільш поширеним, але найменш стійким є метод заміни найменших значущих бітів або LSB-метод (Least Significant Bit, найменший значущий біт). Він полягає у використанні похибки дискретизації, яка завжди існує в оцифрованих зображеннях, аудіо– або відеофайлах. Дана похибка дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя). Тому модифікація молодших бітів в більшості випадків не викликає значної трансформації зображення і не виявляється візуально.

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

Для вбудовування цифрових водяних знаків використовуються більш складні методи.

Постановка завдання

Метою роботи є підвищення рівня захисту інформації від несанкціонованого доступу за рахунок приховування її у мультимедійних файлах. У процесі розробки алгоритму завершеного ПЗ, що реалізує кодування інформації і приховування її в графічному файлі, слід розв’язати такі задачі:

1) визначити структуру стегомоделі;

2) обрати конкретний метод;

3) розробити алгоритм за обраним методом;

4) написати програмний код;

5) розробити дружній (зручний) користувацький інтерфейс;

Додатково на кожному із етапів треба передбачити дії по перевірці чи тестуванню розробленого програмного продукту, а за його результатами – корекцію, налагодження, документування та надання рекомендацій користувачам. Також треба вважати на значний об'єм повної реалізації поставлених цілей та спрямувати зусилля на реалізацію пп. 1-3 у даній роботі, а реалізацію пп.4-5 залишити на майбутні дослідження.

Дослідження стеганографічного алгоритму

Проведемо детальний аналіз методів вбудовування прихованої інформації. Всі алгоритми можна поділити на такі [6]:

1) синтаксичні методи вбудовування прихованої інформації в текстові файли;

2) лексичні методи вбудовування прихованої інформації в текстові файли;

3) мімікрія;

4) методи вбудовування прихованої інформації в графічні файли.

При використанні синтаксичного метода у текстових файлах секретна інформація частіше за все кодується шляхом зміни кількості пробілів, використанням невидимих символів, регістра літер, шляхом зміни табуляції тощо. Цей метод дозволяє легко вбудувати повідомлення у довільний текст, незалежно від його вмісту, призначення і мови. Такі системи легко розробляти і виконуються вони автоматично. Але, на жаль, синтаксичні методи легко й зламуються. Також великим недоліком синтаксичних методів є те, що їх не можна використовувати при передачі великої кількості прихованої інформації.

Найбільш широко використовуються в стеганографії системи на основі лексичної структури тексту. Процедура передачі повідомлення з використанням цього методу містить послідовність кроків:

1) відправник і отримувач мають однакову кількість синонімів, які підтримуються одним і тим же електронним словником; відправник обирає контейнер (текстовий файл);

2) відправник перетворює секретне повідомлення в двійкову послідовність використовуючи криптографічні методи;

3) відправник послідовно аналізує текстовий файл, знаходить перше слово, для якого існує N синонімів;

4) відправник обчислює першу частину значення $\log_2 N$, яка визначає число символів секретного повідомлення, що може бути вбудовано в контейнер шляхом вибору відповідного синоніму;

5) аналогічні дії виконує отримувач – аналізує слова в контейнері на предмет належності до множини синонімів; якщо поточне слово відноситься до одного із множини синонімів, він визначає потужність цього N; ціла частина $\log_2 N$ визначає кількість біт, які закодовані на основі поточної множини синонімів.

Іншим поширеним методом передачі прихованої інформації є мімікрія. Мімікрія генерує текст, використовуючи синтаксис та Contex Free Grammar (CFG – один із способів опису мови, яка складається з синтаксичних слів, фраз, вузлів, де може бути прийнято рішення, яке слово чи фразу далі вставляти у текст). Мімікрія створює бінарне дерево, яке базується на можливості CFG, і будує текст, обираючи ті з гілок дерева, які кодують кожний біт. Недоліком цього методу є неможливість передачі великих об'ємів інформації, низька продуктивність методу і невисокий ступінь захисту.

Методи, що працюють з графічними файлами, використовують у якості контейнера графічні файли. Ці методи дозволяють вбудовувати не тільки текстову інформацію, але і зображення та інші файли. Єдиною умовою є те, що об'єм прихованого повідомлення не повинен перевищувати розмір зображення-контейнера. Для досягнення цієї мети, кожна програма використовує свою технологію, але всі вони зводяться до заміни певних пікселів у зображенні. Характерним прикладом цієї групи методів є метод LSB.

Метод LSB. Суть цього методу полягає в заміні останніх значущих бітів у контейнері (зображення, аудіо або відеозапису) на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути непомітною для органів чуття людини.

Існує метод розширення палітри, що працює тільки для формату GIF. Він буде найбільш ефективним при використанні зображення-контейнера з палітрою невеликих розмірів. Суть його полягає у тому, що збільшується розмір палітри, а це дає додатковий простір для запису необхідних байт на місці байт кольорів. Якщо врахувати що мінімальний розмір палітри становить 2 кольори (6 байт), то максимальний розмір секретного повідомлення може бути $256 \times 3 - 6 = 762$ (байт). Недолік методу – низька криптозахищеність, прочитати приховане повідомлення можна за допомогою будь-якого текстового редактора, якщо повідомлення не було додатково зашифровано [4].

Практично в будь-якому типі мультимедіа-файлів після області з даними міститься прапор, після якого може знаходитися службова інформація. Якщо дописати приховуване повідомлення після даного прапора, то при перегляді або прослуховуванні помітити це буде неможливо. Так як, для неущільнених типів файлів легко встановити розмір, знаючи параметри (розподільна спроможність зображень, частота дискретизації, розрядність, тривалість – для звуку), повідомлення за допомогою даного методу краще приховувати в ущільнених форматах (MP3, AVI тощо). Існує ціла множина методів стеганографії, ща є простими у реалізації, і які можна використовувати практично до всіх типів файлів мультимедіа. Вони стійкий і має високу перепускну спроможність, але їх легко помітити і видалити [1-3, 5].

Вибір стегомоделі і її елементів. Як зазначалося вище, в якості контейнерів зазвичай використовуються цифрові зображення, аудіо– і відеофайли. Результат вбудовування (стего) передається по каналу зв'язку, який контролює порушник. Основна задача порушника полягає в визначенні наявності інформації, що вбудована в прехоплений цифровий об'єкт [8, 10].

На стійкість стеганографічної системи критично впливає правило вибору елементу стеганографічного контейнеру, модифікованого в процесі вбудовування інформації. Під елементом контейнеру слід розуміти атомарну частину цифрового об'єкту, модифіковану в процесі вбудовування інформації.

Задача полягає у добудовуванні методу оптимального вибору елементів контейнеру для вбудовування інформації. Це дозволить максимізувати стеганографічні системи при заданому розмірі прихованого повідомлення, чи перепускну здатність стегосистеми при заданій швидкості.

Різні елементи контейнеру можуть бути об'єднані в групи, що не перетинаються, таким чином, що елементи однієї групи будуть мати подібні властивості і розподіл.

Розглядаємо контейнер як набір із *m* групи елементів. Кожна група характеризується кількістю елементів, що містяться в ній за певним законом розподілу – k_i. C_i – область припустимих значень елементів контейнеру, які входять в *i*-ту групу. Модифікація одного елементу *i*-ої групи дозволяє вбудувати q_i біт, де $q_i = \log_2 C_i$. Таким чином, розглядається цифровий об'єкт (контейнер, стего) у вигляді векторів елементів контейнера.

Нехай x_i – кількість модифікованих елементів *i*-ой групи, $0 \le x_i \le k_i$, сума x_i та q_i дорівнюватиме *n*.

Нехай $f_i(c)$ – функція щільності розподілу елементів *i*-ої групи незмінного стеганографічного контейнеру. Прихована інформація має високу ентропію, так як часто буває зашифрованою чи стисненою. Ця властивість прихованого повідомлення дозволяє знайти функцію щільності розподілу елементів *i*-ої групи контейнеру з вбудованою інформацією $\bar{f}_i(c_i, x_{i0})$, де x_i – кількість незмінних елементів:

$$\bar{f}_i(c_i, x_i) = \frac{k_i - x_i}{k_i} f_i(c) + \frac{x_i}{k_i} \cdot \frac{1}{|c_i|} \quad (1)$$

Позначимо через *P(S)* імовірність того, що у якості стегано-контейнеру буде обраний цифровий об'єкт *S*:

$$P(S) = \prod_{i=1}^{m} \prod_{j=1}^{ki} \bar{f}_i(c_j^i) \quad (2)$$

Імовірність $\bar{P}(S)$ того, що у результаті вбудовування інформації буде отримано стего *S*, обчислюється аналогічно:

$$\bar{P}(S) = \prod_{i=1}^{m} \prod_{j=1}^{ki} \bar{f}_i(c_j^i, x_i) \quad (3)$$

Наведені рівняння дозволяють оцінити стійкість стеганографічної системи за допомогою інформаційно-технічного підходу і відносної ентропії (відстань Кульбака-Лейблера – міра того, наскільки відмінні між собою два ймовірнісних розподіли) [12]:

$$D(P||\bar{P}) = \sum_S P(S) \log_2 \frac{P(S)}{\bar{P}(S)} \quad (4)$$

Чим менше величина $D(P||\bar{P})$, тим вище стійкість стегосистеми. Задача оптимального розподілу приховуваного повідомлення в стеганографічному контейнері зводиться до знаходження такого вектору $\{x_i\}$, $0 \le x_i \le k_i$, при якому величина $D(P||\bar{P})$ була б мінімальною. Ця задача буде вирішена, коли функція $f_i(c)$ буде відома.

Огляд існуючих методів вирішення задачі показав, що найбільш перспективними за інформаційною ємністю є контейнери у вигляді файлів зображень у форматі BMP. Методи, що використовують графічні файли, є найбільш вигідними і перспективними, оскільки практично не обмежують по об'єму переданих даних, все залежить від обраного контейнеру. Також вони надають високий ступінь захисту. Тому їх і краще використовувати у подальших реалізаціях.

Для стеганографічного алгоритму доцільно використовувати LSB-метод та BMP-файли зображення у якості контейнерів. BMP-файл можна умовно поділити на 4 частини:

1) заголовок файлу;
2) заголовок зображення;
3) палітра;
4) саме зображення.

Для поставлених цілей треба знати тільки те, що записано в заголовку. Перші два байти заголовка – це сигнатура BMP, далі в подвійному слові записаний розмір файлу в байтах, наступні 4 байти зарезервовані і повинні містити нулі, в наступному подвійному слові записано зсув від початку файлу до байтів зображення. У 24-бітному BMP-файлі кожен піксель кодується трьома байтами RGB.

Усі BMP-контейнери потрібно розділити на два класи: «чисті» і «зашумлені». У «чистих» картинках простежується зв'язок між молодшим бітом, який ми змінюємо, і рештою 7-ма бітами елементів кольору, а також простежується істотна залежність самих молодших бітів між собою. Впровадження повідомлення в «чисту» картинку руйнує існуючі залежності, що дуже легко виявляється пасивним спостерігачем. Якщо ж картинка «зашумлена» (наприклад, отримана зі сканера або фотокамери), то визначити вкладення стає на порядок складніше. Таким чином, в якості файлів-контейнерів для LSB-методу рекомендується використовувати файли які не були створені на комп'ютері спочатку. LSB-метод з використанням BMP-

контейнера полягає в наступному: замінюються молодші біти в байтах, що відповідають за кодування кольору.

Припустимо:

00011011 – це черговий байт нашого секретного повідомлення;

...11101111-01001110-01111101-0101100100… – це байти в зображенні.

Тоді кодування буде виглядати так:

1) розбити байт секретного повідомлення на, наприклад, 4 двобітові частини

00-01-10-11;

2) замінити отриманими фрагментами двійку молодших бітів зображення

...11101**00**– 01001**01**-01111**10**-01011**11**....

Така заміна в загальному випадку не помітна людському оку. Більш того, багато старих пристроїв виведення, навіть не зможуть відобразити такі незначні зміни. Зрозуміло, що можна змінювати не тільки 2 молодших біта, але і будь-яку їх кількість. Тут є наступна закономірність – чим більша кількість біт замінюється, тим більший обсяг інформації можна заховати, але й тим більші похибки у вихідному зображенні це викличе.

Робота спрощеного алгоритму за LSB-методом така:

1) початок роботи програми, отримання вхідних даних – файлу-контейнеру;

2) отримуючи на вході файл з даними їх потрібно певним чином обробити і перетворити в послідовність бітів, для подальшого вбудовування в графічний файл;

3) розбиття отриманих байтів зображення на нові пари, по кілька бітів в кожному каналі; у результаті отримується новий відтінок, дуже схожий на попередній; цю різницю важко помітити навіть при великій площі заливки, і згідно результатів досліджень, заміна двох молодших бітів не сприймається людським оком; також можна зайняти три розряди, але це трошки спотворить якість картинки; даний процес виконується у циклі, щоб рівномірно програти потрібні біти по файлу, і щоб вбудовування не кидалося в очі, це значно підвищує безпеку збереженої так інформації і відносно зберігає якість вхідного контейнера-картинки;

4) при записі/читанні файлу можуть виникнути помилки, слід передбачити уникання і перевірку їх; саме цей крок і буде контролювати процес перевірки;

5) при умові, що при перевірці отримано позитивне значення – знайдено збій, сміття тощо, – буде виконуватися послідовність кроків для її уникнення (п.6) і вже потім повторно відбувається прогін по умові, і повернення до головної частини процесу кодування даних;

6) обробка помилки та вибір шляху її виправлення;

7) при завершені роботи і вбудовуванні всіх необхідних даних у зображення, слід коректно переписати файл-контейнер, передбачити додатковий файл для декодування.

Алгоритм також реалізує зворотній процес та витягнення даних з файлу і має аналогічний вигляд.

Висновки

Отримані в роботі результати дозволяють значно підвищити перепускну здатність стеганографічної системи, при фіксованій стійкості чи підвищити стійкість стегосистеми при заданій перепускній здатності. Ціль наступних дослідів полягає в адаптації запропонованої моделі до доступного формату цифрового зображення.

Розроблено алгоритм за методом LSB, що підвищує рівень захисту інформації від несанкціонованого доступу за рахунок приховування її у мультимедійних файлах, а саме у файлах зображень.

Наукова новизна отриманих результатів полягає в тому, що отримав подальший розвиток метод приховування даних у молодших бітах значення пікселів файлів зображень (по 1-му, 2-м або 3-м бітам приховуваного повідомлення на піксель контейнера), що не змінює візуальну якість зображення і унеможливлює тим самим виявлення факту приховування інформації.

У якості перспективних розробок увага буде приділена обиранню ПЗ середовища створення програмного коду, генерація самого програмного коду за запропонованим алгоритмом (з можливою корекцією алгоритму) та розробці дружнього користувацького інтерфейсу для використання втаємничення різноманітної економічної, фінансової чи технічної інформації.

Література.

1. Барсуков В.С., Романцов А.П. Компьютерная стеганография вчера, сегодня, завтра [Электронный ресурс]. – Режим доступа: http://www.bnti.ru/showart.asp?aid=330&lvl=03.07.06 (дата звернення 18.05.2017). – Назва з екрана.

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

3. Стеганография [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org /wiki/Стеганография#.D0.9C.D0.B5.D1.82.D0.BE.D0.B4_LSB. (дата звернення 18.05.2017). – Назва з екрана.

4. Тігулев М. Стеганография в GIF [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/128327 (дата звернення 18.05.2017). – Назва з екрана.

5. Стеганозавр [Электронный ресурс]. – Режим доступа: http://www.gagin.ru/internet/8/12.html (дата звернення 18.05.2017). – Назва з екрана.

6. Ярмолик С.В. Стеганографические методы защиты информации/ С.В.Ярмолик, Ю. Н. Листопад // Информатизация образования. – 2005. – N 1. – С. 64-74.

7. Cachin C. An information-theoretic model for steganography [Electronic resourse]/ Christian Cachin // [Information and Computation, 2004], vol. 192, pp. 41-56. – Mode of access: http://www.sciencedirect.com/science/article/pii/S0890540104000409 (Accessed 18 May 2017). – Title from the screen.

8. Cox I. Digital Watermarking and Steganography/ Cox Ingermar, Miller Matthew, Bloom Jeffrey, Fridrich Jessica, Kalker Ton. – London: Elsevier, 2008. – 593 p.

9. Pfitzmann B. Information Hiding Terminology [Electronic resourse]/ Birgit Pfitzmann// [Information Hiding, 1996], vol. 1174, pp. 347-350. – Mode of access: https://www.bibsonomy.org/bibtex/2a2a3c63d0ffb9905c76e9842a2419cbb/dblp (Accessed 18 May 2017). – Title from the screen.

10. Wayner P. Disappearing Cryptography: Information Hiding: Steganography and Watermarking / Wayner Peter.– London: Elsever, 2009. – 440 p.

References.

1. Barsukov, V.S. and Romantsov, A.P. (2006), “Computer steganography yesterday, today, tomorrow”, *Tehnika dlja specsluzhb*, [Online], available at: http://www.bnti.ru/showart.asp?aid=330&lvl=03.07.06 (Accessed 18 May 2017).

2. Konahovich, G.F. and Puzyirenko, A.Y. (2006*), Kompyuternaya steganografiya. Teoriya i praktika*, [Computer steganography. Theory and practice], MK-Press, Kyiv, Ukraine.

3. “Steganography”, *Vikipedija*, [Online], available at: https://ru.wikipedia.org/wiki/Стеганография#.D0.9C.D0.B5.D1.82.D0.BE.D0.B4_LSB. (Accessed 18 May 2017).

4. Tihulev, M. (2011), “Steganography in GIF”, *Habrahabr*, [Online], available at: http://habrahabr.ru/post/128327/ (Accessed 18 May 2017).

5. Tihulev, M. (1998), ”Steganosaur”, *Zhurnal “Internet”*, [Online], vol.98-3(8), available at: http://www.gagin.ru/internet/8/12.html (Accessed 18 May 2017).

6. Yarmolyk, S.V. (2005), “Steganography methods of priv”, *Ynformatyzatsyia obrazovanyia*. – vol. 1, pp. 64-74.

7. Cachin, C., (2004), “An information-theoretic model for steganography”, *Information and Computation*, [Online], vol.192, available at: http:// http://www.sciencedirect.com/science/article/pii/ S0890540104000409 (Accessed 18 May 2017).

8. Cox, I. Miller, M. Bloom, J. Fridrich, J. and Kalker, T. (2008), *Digital Watermarking and Steganography*, Elsevier, London, UK.

9. Pfitzmann, B.(1996), “Information Hiding Terminology”, *Information Hiding*, [Online], vol. 1174, available at: https://www.bibsonomy.org/bibtex/2a2a3c63d0ffb9905c76e9842a2419cbb/dblp (Accessed 18 May 2017).

10. Wayner, P. (2009), *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*, Elsevier, London, UK.

Стаття надійшла до редакції 16.05.2017 р.