УДК 004.056.55(045)

МЕТОДИ СТРУКТУРНОГО КОДУВАННЯ ДАНИХ У ЗАДАЧАХ СТЕГАНОГРАФІЇ

О. К. Юдін, д-р техн. наук, ***К. О. Курінь***

Національний авіаційний університет

kszi.ukr.net

Запропоновано спосіб приховування, який враховує метод двоознакового структурного кодування, й передбачає зміну значення структурних ознак зображення згідно зі змістом секретного повідомлення. Запропонований метод приховування секретного повідомлення в нерухомому зображенні реалізований програмно засобами Mathcad. Визначено основні метрики, які характеризують якість приховування. Розраховано числові значення цих характеристик для тестового зображення-контейнера.

Ключові слова: структурне кодування, структурні ознаки, стеганографічне приховування, стеганографічний контейнер.

The method of concealment, which takes into account the method of bi-signed structural coding, and foresees the change of value of structural signs of image in obedience to maintenance of secret message, is offered. The offered method of concealment of secret message in a static image is realized in program using the Mathcad. Basic characteristics which characterizes quality of concealment are defined. The numerical values of this characteristics are calculated for a test image-container.

Keywords: structural coding, structural signs, steganographical concealments, steganographical container.

Вступ

Інформація є одним з найважливіших ресурсів сучасного життя. Поширення глобальних комп'ютерних мереж зробило отримання доступу до неї надзвичайно простим.

Водночас легкість і швидкість такого доступу значно підвищили загрозу порушення безпеки даних за відсутності заходів відносно їх захисту, а саме загрозу неавторизованого доступу до інформації.

Задача надійного захисту авторських прав, прав інтелектуальної власності або конфіденційних даних від несанкціонованого доступу сьогодні ефективно розв'язується за допомогою стеганографічних методів.

Завданням стеганографії є приховування самого факту існування секретних даних при їх передачі, зберіганні або обробці.

Під прихованням існування інформації мається на увазі не лише неможливість виявлення в перехопленому повідомленні наявності секретних даних, але і взагалі унеможливлення виникнення будь-яких підозр із цього приводу [1].

Стеганографічний захист здійснюється різними способами.

Загальною ж ознакою таких способів є те, що приховуване повідомлення вбудовується в деякий об'єкт–контейнер, що не привертає увагу, який потім відкрито передається адресатові. Як секретне повідомлення і контейнер можуть виступати як звичайний текст, так і файли мультимедійного формату.

Процес тривіального стеганографічного перетворення описується залежностями:

$$E: C \times M \to S; \quad (1)$$

$$D: S \to M, \quad (2)$$

де S, M, C — множина контейнерів-результатів (стеганограм), секретних повідомлень та порожніх контейнерів відповідно.

Залежність (1) описує процес приховування інформації, залежність (2) — видобування прихованої інформації. Необхідною умовою при цьому є відсутність «перетинання», тобто, якщо $m_a \neq m_b$, причому $m_a, m_b \in M$, а (c_a, m_a). $(c_b, m_b) \in S$ то $E(c_a, m_a) \cap E(c_b, m_b) = 0$.

Крім того, необхідно, щоб потужність множини $|C| \geq |M|$. При цьому обидва адресати (відправник і одержувач) повинні знати алгоритм прямого (E) та оберненого (D) стеганографічного перетворення.

Існує велика кількість способів класифікації стеганографічних методів.

Згідно з одним з них за типом контейнерів розрізняють методи, що використовують текст, аудіодані, зображення та відеодані. Кожний виділений клас зорієнтовано на максимальне використання особливостей відповідного типу контейнерів. Наприклад, графічні методи використовують особливості зорової системи людини, такі як чутливість до контрасту, розміру, форми, кольору, місцеположення. Аудіометоди використовують модель людського слуху та основні психоакустичні принципи [1].

Більшість досліджень присвячена використанню як стеганоконтейнерів саме зображень. Це обумовлено такими причинами [1]:

– існуванням практичної необхідності захисту цифрових фотографій, картин, відео від протизаконного тиражування й розповсюдження;

– відносно великим обсягом цифрового представлення зображень;

– заздалегідь відомим (фіксованим) розміром контейнера, відсутністю обмежень, що накладаються вимогами приховання в реальному часі;

– наявністю в більшості реальних зображень текстурних областей, що мають шумову структуру і найкращим чином підходять для вбудовування інформації;

– слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, вмісту в ньому шуму, спотворень поблизу контурів.

Таким чином, одним з найважливіших завдань сучасної інформаційної безпеки є розробка і реалізація нових стеганографічних методів приховування даних у зображеннях.

Постановка завдання

Мета даної статті — розроблення способу приховування даних у нерухомих повнокольорових зображеннях з урахуванням методів структурного кодування.

До завдань дослідження належать:

– розроблення алгоритму приховування даних у нерухомому зображенні, формування математичної моделі стеганографічного перетворення;

– створення програмної моделі, яка реалізовує розроблену математичну;

– визначення основних показників якості приховування даних та проведення їх розрахунку для реалізованого методу.

Принцип приховування

Будь-яке зображення можна інтерпретувати через сукупність організованих у матрицю пікселів. Кольорове зображення C представляється через дискретну функцію, яка визначає вектор кольору $c(x, y)$ для кожного пікселя зображення (x, y), де значення кольору задає трикомпонентний вектор у колірному просторі.

Найбільш поширеним способом передавання кольору є модель RGB, у якій основні кольори — червоний, зелений і синій, а будь-який інший колір може бути представлений у вигляді зваженої суми основних кольорів.

Вектор кольору $c(x, y)$ у RGB-просторі представляє інтенсивність основних кольорів. Кожен вектор кольору являє собою восьмибітове ціле число. Розглянемо, яким чином можна здійснити вбудовування секретного повідомлення у контейнер за рахунок маніпуляцій колірними складовими $\{R(x, y), G(x, y), B(x, y)\}$.

Згрупуємо пікселі кожної компоненти колірної моделі RGB у блоки 8×8, що називаються *сегментами*. Якщо число рядків або стовпчиків вихідного зображення не кратне 8, то верхній рядок і правий крайній стовпчики повторюються потрібну кількість разів.

Таким чином, якщо розмір розширеного зображення-контейнера становить $m \times n$ пікселів, то сегменти будуть організовані в матрицю розмірністю $M \times N$, де $M = \frac{m}{8}$, а $N = \frac{3n}{8}$.

Як уже зазначалося, кожне з числових значень у сегменті представляється у вигляді 8-бітового двійкового числа, тобто просторово кожний сегмент можна представити у вигляді паралелепіпеду розмірністю $8 \times 8 \times 8$.

Десяткові значення представлення даних у сегменті «розростаються» у глибину на 8 біт. Кожен сегмент складається таким чином з восьми шарів.

Кожен p-й шар є сукупністю p-х бітів двійкового представлення яскравостей складових колірних компонент, де $p \in 0...7$.

Очевидно, що нульовий шар є сукупністю найменш значущих бітів (НЗБ) зображення.

Принцип просторової структуризації сегменту зображення та вигляд нульового шару цього сегменту зображені на рис. 1, *а*, *б*, відповідно

Очевидно, що порядок розташування бітів шару визначає певні структурні закономірності двійкових послідовностей (ДП), які утворюють цей шар.

Ці закономірності можна описати за допомогою структурних ознак [2].

Серед найбільш інформативних структурних ознак виділяють такі:

1. Вектор Λ — заборона на появу на певній позиції одиничного елемента

$$(\Lambda = \{\lambda_i\}, i = 1...m,$$

де λ_i — ознака появи на i-й позиції одиничного елемента, якщо $\lambda_i = 0$, то на i-й позиції заборонено поява одиничного елемента, якщо $\lambda_i = 1$, то навпаки); позиції, на яких заборонена поява одиниць, розбивають вихідну ДП на так звані допустимі зони (ДЗ).

2. Кількість серій одиниць ϑ в ДП.

Наприклад, значення структурних ознак для нульового шару сегменту зображення, показаного на рис. 1, *б*, наведено в табл. 1.

У праці [2] описано метод двоознакового структурного кодування (ДСК) двійкових даних. Суть даного методу полягає у формуванні кодуномера ДП із заданим значенням структурної ознаки.

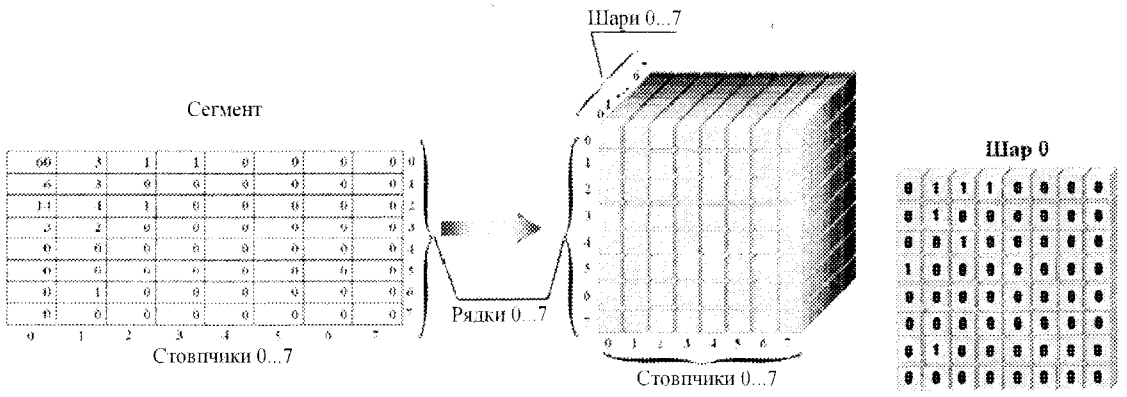

Рис. 1. Принцип просторової структуризації сегменту зображення (*а*) та вміст нульового шару (*б*)

Таблиця 1

Приклади значень структурних ознак

Структурні ознаки									
	ϑ								Λ
1-а ДЗ	1	1	2	1	0	0	0	0	
	0	1	1	1	0	0	0	0	0
	0	1	0	0	0	0	0	0	0
	0	0	1	0	0	0	0	0	0
	1	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	1
	0	0	0	0	0	0	0	0	1
2-а ДЗ	0	1	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	1

Код-номер ДІІ A формується згідно з теоремою про нумерацію двоознакових структурних двійкових чисел [2] для заданих параметрів послідовності: вектора обмежень на позиції одиниць Λ і вектора Θ обмежень на кількість серій одиниць у допустимих зонах.

Процедура двоознакового кодування є оберненою. Тобто за кодом-номером при наявності значень структурних ознак можна абсолютно однозначно відновити вихідну двійкову послідовність.

Запропонуємо метод приховування даних, що використовує викладені вище структурні властивості зображень.

1. Порожнє зображення-контейнер розбивається на сегменти за правилом, описаним вище.

2. Для кожного i, j-го сегменту зображення, де $i \in 0...M-1, j \in 0...N-1$, визначаються структурні ознаки: вектор заборон на появу одиничного елементу $\Lambda_{i,j,p}$ для кожного p-го шару, де $p \in 0...7$, кількість серій одиниць у кожному l-му ($l \in 0..7$) стовпчику p-го шару $(\vartheta_l)_{i,j,p}$, вектор $(\Theta_l)_{i,j,k}$ обмежень на число серій одиниць у допустимих зонах кожного стовпчика.

3. Визначимо значення кодів-номерів для стовпчиків кожного шару всіх сегментів зображення. Процедуру ДСК у даному випадку можна формально описати правилом:

$$(NUM_l)_{i,j,p} = F[A, \Lambda_{i,j,p}, (\Theta_l)_{i,j,p}].$$

4. Внесемо зміни у значення однієї зі структурних ознак — вектора обмежень на позиції одиниць Λ. Припустимо, що необхідно приховати в зображенні секретне повідомлення *MES* довжиною L символів.

Кожен символ кодується восмибітовим кодом ASCII, десяткове значення якого змінюється в межах від 0 до 255. Разом з тим кожне значення $\Lambda_{i,j,p}$ являє собою вектор, на кожній з восьми позицій якого знаходиться 0 або 1.

Тобто даний вектор можна інтерпретувати як двійкове число (перша позиція у векторі визначає молодший біт), десяткове представлення якого також змінюється в межах від 0 до 255.

У процесі приховування замінимо десяткові значення векторів обмежень на позиції одиниць для кожного нульового шару сегментів зображення на значення ASCII-кодів символів повідомлення *MES*:

$$\Lambda^*_{[k/n],[k/N],0} = MES_k,\ k \in 0...L-1.$$

Зазначимо, що довжина повідомлення має задовольняти умову: $L \le M \times N$.

5. Визначимо значення закодованих двійкових послідовностей згідно з отриманими кодами номерів та структурних ознак з урахуванням внесених змін. Процедуру двоознакового структурного декодування (ДСДк) у цьому випадку можна формально описати правилом:

$$A^* = F^{-1}[(NUM_l)_{i,j,p},\ \Lambda^*_{i,j,p},(\Theta_l)_{i,j,p}].$$

Відновлені ДП складають структуру заповненого стеганоконтейнера.

Викладений вище принцип приховування секретних даних можна проілюструвати рис. 2.

Для відновлення секретного повідомлення достатньо розрахувати значення вектора обмежень на позиції одиниць для кожного нульового шару сегментів отриманого зображення-контейнера.

За рахунок того, що зміни вносяться у структурну ознаку, яка описує бітовий вміст шарів зображення, що визначають сукупність найменш значущих бітів, теоретично спотворення, які виникають у зображенні після приховування секретних даних, мають бути візуально непомітні.

Оцінка якості стеганосистеми

Для порівняльного оцінювання якості стеганографічних засобів розроблюють різні показники, що дають кількісні оцінки. У табл. 2 наведено низку показників, використовуваних під час оцінювання спотворень, що вносяться стеганоперетвореннями до зображення [1].

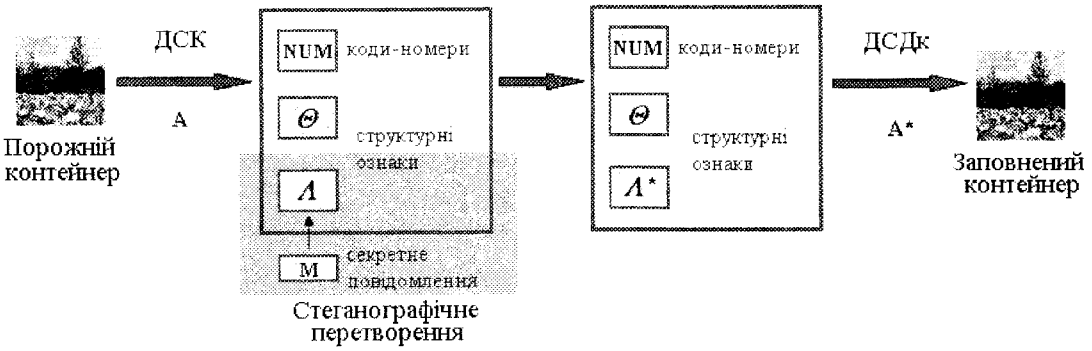

Рис. 2. Метод приховування даних у нерухомому зображенні з урахуванням ДСК

Таблиця 2

Показники візуального спотворення

Різницеві показники спотворення	
Максимальна різниця (Maximum Difference)	$MD = \max_{x,y} \lvert C_{x,y} - S_{x,y} \rvert$
Середня абсолютна різниця (Average Absolute Difference)	$AD = \frac{1}{XY} \sum_{x,y} \lvert C_{x,y} - S_{x,y} \rvert$
Нормована середня абсолютна різниця (Normalized Average Absolute Difference)	$NAD = \sum_{x,y} \lvert C_{x,y} - S_{x,y} \rvert \Big/ \sum_{x,y} \lvert C_{x,y} \rvert$
Середньоквадратична помилка (Mean Square Error)	$MSE = \frac{1}{XY} \sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2$
Нормована середньоквадратична помилка (Normalized MSE)	$NMSE = \sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2 \Big/ \sum_{x,y} \left(C_{x,y}\right)^2$

Закінчення табл. 2

Різницеві показники спотворення	
L^p-норма (L^p-*norm*)	$L^p = \left(\frac{1}{XY} \sum_{x,y} \left\| C_{x,y} - S_{x,y} \right\|^p \right)^{1/p}$
Відношення сигнал/шум (Signal to Noise Ratio)	$SNR = \sum_{x,y} \left(C_{x,y} \right)^2 \Big/ \sum_{x,y} \left(C_{x,y} - S_{x,y} \right)^2$
Максимальне відношення сигнал/шум (Peak Signal to Noise Ratio)	$PSNR = XY \max_{x,y} \left(C_{x,y} \right)^2 \Big/ \sum_{x,y} \left(C_{x,y} - S_{x,y} \right)^2$
Якість зображення (Image Fidelity)	$IF = 1 - \sum_{x,y} \left(C_{x,y} - S_{x,y} \right)^2 \Big/ \sum_{x,y} \left(C_{x,y} \right)^2$
Кореляційні показники спотворення	
Нормована взаємна кореляція (Normalized Cross-Correlation)	$NC = \sum_{x,y} C_{x,y} S_{x,y} \Big/ \sum_{x,y} \left(C_{x,y} \right)^2$
Якість кореляції (Correlation Quality)	$CQ = \sum_{x,y} C_{x,y} S_{x,y} \Big/ \sum_{x,y} C_{x,y}$
Інші показники	
Структурний зміст (Structural Content)	$SC = \sum_{x,y} \left(C_{x,y} \right)^2 \Big/ \sum_{x,y} \left(S_{x,y} \right)^2$
Нормоване відношення сигма/помилка (Normalized Sigma to Error Ratio)	$NSER = \frac{1}{\max(SER)} \sum_b SER_b$, де $SER_b = \sigma_b^2 \Big/ \left[\frac{1}{n} \sum_{\text{блок } b} \left(C_{x,y} - S_{x,y} \right)^2 \right]$
Подібність гістограм (Histogram Similarity)	$HS = \sum_{c=0}^{255} \left\| f_C(c) - f_S(c) \right\|$, де $f_C(c)$ — відносна частота градації кольору C у зображенні з 256 рівнями кольорів

Більшість показників спотворення або критеріїв якості, що використовуються при візуальній обробці інформації, належать до групи різницевих показників спотворення.

Ці показники грунтуються на відмінності між контейнером-оригіналом (неспотворений сигнал) і контейнером-результатом (спотворений сигнал). До другої групи входять показники, засновані на кореляції між оригінальним і спотвореним сигналами (так звані кореляційні показники спотворення).

У наведених співвідношеннях через $C_{x,y}$ позначається піксель порожнього контейнера з координатами (x, y), а через $S_{x,y}$ — відповідний піксель заповненого контейнера.

У параметрі *SER* зображення попередньо розбивається на N блоків по n пікселів розміром $X \times Y$, де X і Y — кількість рядків і стовпчиків у блоці відповідно (блок 8×8 пікселів) [1].

У багатьох випадках більш корисною є нормалізована оцінка якості.

Використовувати оцінку якості Q відповідно до рекомендацій сектора радіозв'язку МСЕ — ITU-R Rec. 500 [1]:

$$Q = \frac{5}{1 + N \times \varepsilon}, \qquad (3)$$

де ε — обчислене спотворення; N — нормувальний коефіцієнт, який зазвичай обирається таким, щоб характеристика спотворення відображувала відповідну якісну оцінку.

У табл. 3 наведено оцінки, відповідне зорове сприйняття і якість.

Оцінка якості приховування

Розрахуємо показники візуального спотворення згідно з формулами, наведеними в табл. 2, та показник сприйняття спотворень людиною відповідно до формули (3) для розробленого методу. Для порівняльного аналізу розглянемо також відповідні показники для зображення-контейнера, сформованого за допомогою одного з найбільш застосовних на сьогодні методів приховування даних у зображенні — методу Коха та Жао [1] (табл. 4).

Таблиця 3

ITU-R Rec. 500. Оцінки якості за шкалою від 1 до 5

Оцінка	Спотворення	Якість
5	Непомітне	Відмінна
4	Помітне, не подразнювальне	Добра
3	Несуттєво подразнювальне	Задовільна
2	Подразнювальне	Незадовільна
1	Надзвичайно подразнювальне	Вкрай незадовільна

Таблиця 4

Оцінювання якості приховування секретного повідомлення в зображенні-контейнері

Метод	Розроблений метод	Метод Коха–Жао
Максимальна різниця (Maximum Difference)	1	23,318
Середня абсолютна різниця (Average Absolute Difference)	0,244	6,881
Нормована середня абсолютна різниця (Normalized Average Absolute Difference)	$1{,}887\times10^{-3}$	0,065
Середньоквадратична похибка (Mean Square Error)	0,244	63,424
Нормована середньоквадратична похибка (Normalized Mean Square Error)	$1{,}14\times10^{-5}$	$3{,}636\times10^{-3}$
L^p-норма (L^p-*norm*), $p=2$	0,494	7,964
Відношення сигнал/шум (Signal to Noise Ratio)	$8{,}77\times10^{4}$	275,042
Максимальне відношення сигнал/шум (Peak Signal to Noise Ratio)	$2{,}661\times10^{5}$	1025
Якість зображення (Image Fidelity)	0,9999886	0,9963642
Нормована взаємна кореляція (Normalized Cross-Correlation)	0,9992171	1,024106
Якість кореляції (Correlation Quality)	165,331	169,601
Структурний зміст (Structural Content)	1,0001	0,9507077
Нормоване відношення сигма/помилка (Normalized Sigma to Error Ratio)	68,261	33,368
Подібність гістограм (Histogram Similarity)	11500	16380
Оцінка якості згідно з МСЕ — ITU-R Rec. 500	4,879	3,576

Запропоновані методи були реалізовані програмно засобами Mathcad. В якості контейнера використовувалося повнокольорове зображення розмірністю 128×128 пікселів.

Висновки

У результаті наукового дослідження був запропонований метод стеганографічного приховування даних у нерухомому зображенні. Наукова новизна дослідження полягає в тому, що цей спосіб приховування, який враховує метод двознакового структурного кодування, й передбачає зміну значення структурних ознак зображення згідно зі змістом секретного повідомлення. Метод приховування секретного повідомлення в нерухомому зображенні реалізований програмно засобами Mathcad. Визначені основні метрики, які характеризують якість приховування. Числові значення цих характеристик були розраховані для тестового зображення-контейнера.

Отримані результати дають змогу зробити такі висновки: якість приховування при розміщенні бітів секретного повідомлення в зображенні згідно із запропонованим методом вища, ніж у випадку використання методу Коха–Жао.

Про це свідчить таке: різницеві показники порівняно з методом Коха–Жао зменшуються, якість зображення зростає, відношення сигнал/ шум збільшується, ступінь кореляції між пікселями первісного та заповненого контейнерів максимально наближається до одиниці. Показники якості згідно зі стандартом МСЕ—ITU-R Rec. 500 свідчать про приховування бітів секретного повідомлення, враховуючи метод якості зображення контейнера залишається відмінним, а викривлення майже непомітним (4,879).

ЛІТЕРАТУРА

1. *Конахович Г. Ф.* Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, Ф. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

2. *Юдін О. К.* Кодування в інформаційно-комунікаційних мережах : монографія / О. К. Юдін. — К. : НАУ, 2007. — 308 с.

3. *Юдін О. К.* Структурно-логічна модель кодера стиску інформаційного потоку даних / О. К. Юдін, Ю. Б. Чеботаренко, К. О. Курінь // Вісник Інженерної академії України. — К., 2010. — 4 вид. — С. 151–157.

Стаття надійшла до редакції 20.03.2012