10. Tokuno S. Granular Activated Carbon Filtration and Nitrification // Water Utilities Laboratory for the City
of Corpus Christi Texas. – 2000. – № 12. – P. 1–52.
11. Thiel P. Activated carbon vs anthracite as primary dual media filters – a pilot plant study/ P. Thiel, L. Zappia, P. Franzmann, B. Warton, M. Alessandrino, A. Heitz, P. Nolan, D. Scott, B. Hiller, D. Masters// 9th
Annual Water Industry Engineers and Operators Conference Bendigo Exhibition Centre 5 to 7 September. – 2006.– P. 8-14.
12. Baruth E. Water Treatment Plant Design // American Water Works Association, and American Society of Civil Engineers. Fourth ed. New York: McGraw – Hill Handbooks. – 2005. – P. 2–18.
13. Dvorak B.I. Drinking Water Treatment: Activated Carbon Filtration/ B.I. Dvorak, S.O. Skipton// Water Resource Management Drinking Water. – 2013. – № 11. – P. 1–12.
14. Howie E. Supplying adequate drinking water to the devikulam village/ E. Howie, R. McIntosh, W. McCumstie, C. Tan, A. Lederhose, J. Mahadik. // University of Queensland. – 2011. – P. 1–61.

СПОСІБ ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ПЕРЕДАЧІ КЛЮЧОВОГО ЕЛЕМЕНТУ СТЕГОКОНТЕЙНЕРА

Зажома В.М.,
начальник відділу персоналу
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України,
Черкаси, Україна

Козловська С.Г.,
старший викладач
Східноєвропейський університет економіки і менеджменту,
Черкаси, Україна

THE METHOD OF INCREASING THE RELIABILITY OF TRANSMISSION OF KEY ELEMENT OF STEGANOGRAPHY CONTAINER

Zazhoma V.M.,
Head of the Staff Department,
Cherkassy Institute of Fire Safety named after Heroes of Chornobyl of National University of Civil Defense of Ukraine,
Cherkasy, Ukraine

Kozlovska S.G.,
Senior Lecturer,
East European University of Economics and Management,
Cherkasy, Ukraine

Анотація.

Стеганографію сьогодні найчастіше використовують не для заміни криптографії, а для її доповнення. Так як, на відміну від криптографії, яка приховує вміст секретного повідомлення, стеганографія приховує саме його існування, то приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення ще і зашифровано, то воно має ще один, додатковий, рівень захисту.

Отже, вдосконалення стеганографічних методів захисту інформації є актуальною задачею сучасних наукових досліджень.

Об'єкт дослідження – методи підвищення надійності та достовірності передачі стеганоповідомлення.

Метою даної роботи є розробка способу забезпечення гарантованої передачі ключового елементу стеганографічного контейнера на основі застосування завадостійкого кодування.

Задача, яка розглядається в даній роботі, полягає в розробці та реалізації способу застосування завадостійкого кодування для підвищення достовірності передачі ключового елементу стеганографічного контейнера при реалізації стеганографічного методу на основі використання випадково визначеного ключового елементу пустого контейнера, значення якого забезпечує вибір способу вбудовування повідомлення в контейнер. Показано, що запропонований спосіб використання кодів Хеммінга показує ефективні результати переважно лише при однократних помилках.

Ключові слова: *стеганографічний метод, приховування інформації, алгоритм вбудовування, ключовий елемент, завадостійке кодування, інформаційне резервування.*

Abstract

Steganography is most often used today is not a replacement for cryptography and for its complement. Since, in contrast to cryptography, which hides the contents secret message, steganography hides its existence, hiding a message by steganography methods greatly reduces the probability of detection of the fact of transmission of messages. And even if this message is encrypted, it is still one extra layer of protection.

Therefore, improving the protection of information steganographic methods is an urgent task of modern scientific research.

Object of research - methods of improving the reliability and validity of the transfer of steganographic messages.

The goal of this work is to develop a method of providing a guaranteed transmission key element of the steganographic container on the basis of error-correcting coding.

Task, which is discussed in this paper is to develop and implement a method of using error-correcting coding to improve the reliability of the transmission of a key element of steganographic container during the implemen-tation of steganographic method on the basis of randomly defined key element of empty container, the value of which provides a choice of a method of embedding a message in the container. It is shown that the proposed method using Hamming codes showing effective results mainly only with unitary errors.

Keywords: *steganographic method, concealment of information, embedding algorithm, the key element, error control coding, information redundancy.*

Постановка проблеми. Сучасний стан розвитку обчислювальної техніки та нових каналів передачі даних зумовив появу нових стеганографічних методів, в основі яких покладені особливості представлення інформації в комп'ютерних файлах, обчислювальних мережах та інше. Як наслідок комп'ютерну стеганографію стали виокремлювати як окремий напрямок досліджень.

Загальнодоступність потужних та швидкодіючих апаратно-програмних засобів, що можуть бути використані для реалізації несанкціонованого доступу до конфіденційної інформації, яка захищена криптографічними алгоритмами є ще однією з причин стрімкого розвитку та поширення стеганографічних методів захисту інформації. Стеганографію сьогодні найчастіше використовують не для заміни криптографії, а для її доповнення. Так як, на відміну від криптографії, яка приховує вміст секретного повідомлення, стеганографія приховує саме його існування, то приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення ще і зашифровано, то воно має ще один, додатковий, рівень захисту.

Отже, вдосконалення стеганографічних методів захисту інформації є актуальною задачею сучасних наукових досліджень.

Аналіз публікацій і досліджень. Розробці нових та вдосконаленню існуючих стеганографічних методів захисту інформації шляхом організації та здійснення прихованого її обміну присвячено досить багато сучасних досліджень [1-4], тому що дане питання є актуальним і сьогодні при побудови систем передачі даних для забезпечення конфіденційності та цілісності передачі даних. Зокрема, в [1] наводиться класифікація стегосистем та методів вбудовування, опис та структура стеганографічної системи захисту інформації на основі теорії секретних систем, детально досліджується підвищення пропускної здатності стегоканалу, забезпечення стійкості та непомітності вбудовування.

Аналіз останніх досліджень і публікацій [2, 3] показує, що найбільшу популярність в комп'ютерній стеганографії здобули стеганографічні методи, які використовують у ролі носія прихованого конфіденційного повідомлення зображення. Це пояснюється тим, що зображення володіють великою надлишковістю. Одним із шляхів реалізації нових ефективних стеганографічних методів приховування інформації є розроблений метод вбудовування інформації в зображення, який здійснюється на основі використання випадково визначеного ключового елементу пустого контейнера, значення якого забезпечує вибір способу вбудовування повідомлення в контейнер [4]. Перевагою даного методу є відсутність необхідності передачі контейнера-оригінала для відтворення прихованого повідомлення зі стегоконтейнеру. Але, разом з тим, існує значний недолік – втрата чи спотворення значення ключового елементу при передачі стегоконтейнеру призводить до неможливості відтворення прихованого повідомлення. Саме вирішенню сформульованої вище проблемної задачі присвячене дане дослідження.

Метою даної роботи є розробка способу підвищення достовірності передачі ключового елементу стеганографічного контейнера на основі застосування завадостійкого кодування.

Виклад основного матеріалу. Для забезпечення надійності передачі ключового елементу та

підвищення надійності визначення елементів повідомлення в контейнері необхідно використовувати завадостійке кодування.

Завадостійке кодування необхідно використовувати в двох напрямках:

- для забезпечення гарантованої передачі ключового елементу контейнера необхідно застосовувати методи виправлення помилок ключового елемента на основі введення надлишковості. Задача вибору методу завадостійкого кодування ключового елементу на даний час не вирішувалася;

- для підвищення достовірності виокремлення повідомлення зі стеганографічного контейнера доцільно використовувати коди контролюючі помилки для побудови кодерів стегосистеми.

Дані пропозиції повинні використовуватися спільно з використанням методів підвищення достовірності повідомлення.

Основним недоліком розробленої стеганосистеми [4] є залежність отримання інформації від ключового елементу стеганографічного контейнеру, який визначає алгоритм приховування інформації, а значить і її отримання. Помилка в ключовому елементі призведе до використання іншого алгоритму отримання інформації і як наслідок до її втрати. Тому для забезпечення гарантованої передачі ключового елементу необхідно використовувати методи завадостійкого кодування.

Збільшення завадостійкості можливе за умови, коли потужність коду менша множини двійкових чисел.

Будь-яке число X в позиційних системах числення може бути представлене наступним чином [5]:

$$X_i = (x_{n-1}, x_{n-2}, x_{n-3}, \ldots, x_2, x_1, x_0),$$

де $x_j \in \{0,1\}; i \in \{0,1,\ldots, M < (2^n - 1)\}$.

Аналогічно представимо закодоване завадостійким кодом число Y:

$$Y_i = (y_{n-1}, y_{n-2}, y_{n-3}, \ldots, y_2, y_1, y_0),$$

де $y_j \in \{0,1\}; i \in \{0,1,\ldots,(2^n - 1)\}$.

Кодування і декодування позначимо як $X_u \to Y_u$ та $Y_u \to X_u$ відповідно.

Відстанню за Хеммінгом називається мінімальне значення функції на множині пар чисел Y_u і Y_v, де $(u \neq v)$ [5]:

$$d_{\min}(Y_u, Y_v) = d.$$

Код дозволяє виявляти і виправляти деяку кількість помилкових символів. Кількість виявлених помилкових символів визначається як

$$K_o \leq d - 1.$$

Кількість виправлених помилкових символів визначається як

$$K_u \leq \frac{d-1}{2}.$$

Так як коди Хеммінга достатньо просто реалізуються як програмно так і апаратно було-б доцільно використати їх для підвищення достовірності передачі ключового елементу стеганографічного контейнера.

Доцільно розглянути коди Хеммінга на основі матричного представлення операцій кодування і розкодування номерів блоків стеганографічного контейнера.

Будь-який код Хеммінга $G_{(n,k)}$ в загальному вигляді може бути заданий породжуючою матрицею [5]:

$$G_{(n,k)} = \begin{vmatrix} 1\,0\,0\,0\ldots 0 & b_{11}\,b_{12}\,b_{13}\,b_{14}\ldots b_{1r} \\ 0\,1\,0\,0\ \ldots 0 & b_{21}\,b_{22}\,b_{23}\,b_{24}\ldots b_{2r} \\ 0\,0\,1\,0\ \ldots 0 & b_{31}\,b_{32}\,b_{33}\,b_{34}\ldots b_{3r} \\ 0\,0\,0\,1\ \ldots 0 & b_{41}\,b_{42}\,b_{43}\,b_{34}\ldots b_{4r} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ 0\,0\,0\,0\ \ldots 1 & b_{k1}\,b_{k2}\,b_{k3}\,b_{k4}\ldots b_{kr} \end{vmatrix} \quad (1)$$

Для визначення значень перевірочних елементів правої частини матриці необхідно виходити з основних властивостей систематичних кодів [5]. Так як кожен рядок одиничної матриці $k \times k$ має лише одну одиницю, то вага кожного рядка приписаної матриці не повинна бути меншою за $d-1$, а сума по модулю два двох рядків не повинна бути меншою за $d-2$ для гарантованого виправлення однократної помилки. Крім того комбінації правої частини матриці повинні бути лінійно незалежними.

Розглянемо для прикладу код $G_{(7,4)}$. Відповідно до виразу (1), один із варіантів породжуючої матриці, може бути представлений як

$$G_{(7,4)} = \begin{vmatrix} 1\,0\,0\,0\,1\,0\,1 \\ 0\,1\,0\,0\,1\,1\,1 \\ 0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1 \end{vmatrix}. \quad (2)$$

Відповідно до виразу (2) при кодуванні буде виконуватись матричне перетворення:

$$F^{k}_{(7,4)} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_1 \oplus x_2 \oplus x_3 \\ x_4 \oplus x_3 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_4 \end{pmatrix}.$$

За аналогією будуються матричні моделі пристроїв кодування та виявлення і виправлення помилок для будь-яких кодів Хеммінга. Наприклад,

$$G_{(8,5)} = \begin{vmatrix} 1\,0\,0\,0\,0\,1\,0\,1 \\ 0\,1\,0\,0\,0\,1\,1\,1 \\ 0\,0\,1\,0\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1 \\ 0\,0\,0\,0\,1\,0\,1\,0 \end{vmatrix}$$

для коду матричне перетворення описується моделлю

$$F^{k}_{(8,5)} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\ x_1 \oplus x_2 \oplus x_4 \end{pmatrix}.$$

Розглянемо результати виявлення і виправлення помилок наведеними кодами Хеммінга $G_{(7,4)}$ та $G_{(8,5)}$ в залежності від кратності помилки. Дані результати наведені в табл. 1.

Таблиця 1

Контроль помилок кодами Хеммінга в залежності від їх кратності

		Кратність помилки					
		1	**2**	**3**	**4**	**5**	**6**
$G_{(7,4)}$	кількість	7	21	35	35	21	7
	виявлено	7	21	–	–	–	–
	виправлено	7	–	–	–	–	–
$G_{(8,5)}$	кількість	8	28	56	70	56	28
	виявлено	8	28	–	–	–	–
	виправлено	8	–	–	–	–	–

Аналіз табл. 1 показує, що коди Хеммінга доцільно використовувати, коли переважають лише однократні помилки. При кратності помилок більше двох їх виправлення стає неможливим, а при більшій кратності помилок зростає процент їх пропуску.

Для підвищення надійності засобів інформаційно-обчислювальної техніки використовують апаратне та інформаційне резервування [6].

Проте в явному вигляді інформаційне резервування значення ключового елемента буде вносити зміни контейнеру в старші розряди, що призведе до спотворення стеганографічного контейнеру. Можна скористатися ідеєю вибору одного елемента із декількох, точніше однозначно побудувати одне значення ключового елементу з декількох наперед вибраних елементів.

$$x_i = \begin{cases} 1 & \ddot{y}\hat{e}\grave{u}\hat{i} \quad x_{i.1} + x_{i.2} + x_{i.3} > 1 \\ 0 & \ddot{y}\hat{e}\grave{u}\hat{i} \quad x_{i.1} + x_{i.2} + x_{i.3} < 2 \end{cases} \tag{3}$$

$$x_i = \begin{cases} 1 & \ddot{y}\hat{e}\grave{u}\hat{i} \quad x_{i.1} + x_{i.2} + x_{i.3} + x_{i.4} + x_{i.5} > 2 \\ 0 & \ddot{y}\hat{e}\grave{u}\hat{i} \quad x_{i.1} + x_{i.2} + x_{i.3} + x_{i.4} + x_{i.5} < 3 \end{cases} \tag{4}$$

$$x_i = \begin{cases} 1 & \ddot{y}\hat{e}\grave{u}\hat{i} \quad x_{i.1} + x_{i.2} + x_{i.3} + x_{i.4} + x_{i.5} + x_{i.6} + x_{i.7} > 3 \\ 0 & \ddot{y}\hat{e}\grave{u}\hat{i} \quad x_{i.1} + x_{i.2} + x_{i.3} + x_{i.4} + x_{i.5} + x_{i.6} + x_{i.7} < 4 \end{cases}$$

Необхідною умовою для однозначної побудови ключового елементу є непарна кількість наперед вибраних ключових елементів.

Так як кількість вхідних даних для побудови ключового елементу є частково надлишковою, то в результаті побудови можлива корекція деяких помилок. Розглянемо це питання більш детально.

Нехай $x_{i.1} = 0$; $x_{i.2} = 0$; $x_{i.3} = 0$.

Виявлення помилок в залежності від їх кратності наведено в верхній частині табл. 2 та наведено результати корекції помилок для всіх значень $x_{i.1}$, $x_{i.2}$ і $x_{i.3}$ в залежності від помилок і їх кратності. В нижній частині таблиці наведено узагальнені дані щодо кількості виправлення помилок в залежності від їх кратності.

Таблиця 2

Коректність формування біта ключового елементу згідно (3)

Однократна помилка				Двохкратна помилка				Трьохкратна помилка			
дані	біт	помилка	біт	дані	біт	помилка	біт	дані	біт	помилка	біт
000	0	001	0	000	0	011	1	000	0	111	1
000	0	010	0	000	0	101	1				
000	0	100	0	000	0	110	1				
001	0	001	0	001	0	011	0	001	0	111	1
001	0	010	1	001	0	101	0				
001	0	100	1	001	0	110	1				
010	0	001	1	010	0	011	0	010	0	111	1
010	0	010	0	010	0	101	1				
010	0	100	1	010	0	110	0				
011	1	001	0	011	1	011	0	011	1	111	0
011	1	010	0	011	1	101	1				
011	1	100	1	011	1	110	1				
100	0	001	1	100	0	011	1	100	0	111	1
100	0	010	1	100	0	101	0				
100	0	100	0	100	0	110	0				
101	1	001	0	101	1	011	1	101	1	111	0
101	1	010	1	101	1	101	0				
101	1	100	0	101	1	110	1				
110	1	001	1	110	1	011	1	110	1	111	0
110	1	010	0	110	1	101	1				
110	1	100	0	110	1	110	0				
111	1	001	1	111	1	011	0	111	1	111	0
111	1	010	1	111	1	101	0				
111	1	100	1	111	1	110	0				
Помилок **24** Виправлено **12**				Помилок **24** Виправлено **12**				Помилок **8** Виправлено **0**			

В табл. 3 наведено узагальнені дані щодо кількості виправлення помилок в залежності від їх кратності при формуванні біта ключового елементу згідно виразу (4) для всіх значень $x_{i.1}$, $x_{i.2}$, $x_{i.3}$, $x_{i.4}$ і $x_{i.5}$.

Узагальнені результати розрахунку коректності формування біта ключового елементу згідно виразу (4)

	Кількість помилок	Виправлено помилок
Однократні	170	104
Двохкратні	408	272
Трьохкратні	340	126
Чотирьохкратні	170	66
П'ятикратні	34	0
Всього	1122	568

Одержані дані розрахунків щодо кількості виправлення помилок в залежності від їх кратності показують ефективність застосування запропонованого способу інформаційного резервування при формуванні значення ключового елемента для кратності помилок від одно до чотирьохкратних, на відміну від застосування кодів Хеммінга, які ефективні лише для однократних помилок.

Висновки. Отже, проведені дослідження щодо застосування завадостійкого кодування для підвищення достовірності передачі ключового елементу стеганоконтейнера при реалізації стеганографічного методу на основі використання випадково визначеного ключового елементу пустого контейнера, значення якого забезпечує вибір способу вбудовування повідомлення в контейнер дають можливість стверджувати, що запропонований спосіб використання кодів Хемінга показує ефективні результати переважно лише при однократних помилках.

Реалізований спосіб забезпечення гарантованої передачі ключового елементу стегоконтейнера на основі інформаційного резервування показав коректність його використання при формуванні біта ключового елементу для виявлення та виправлення помилок при збільшенні їх кратності від одно до чотирьохкратних, а простота його реалізації дозволяє провести його технічну реалізацію на засобах обчислювальної техніки. Основна ідея реалізації інформаційного резервування полягає у визначенні значення одного елемента в залежності від декількох наперед вибраних елементів.

Визначено, що необхідною умовою для однозначної побудови ключового елементу є непарна кількість наперед вибраних ключових елементів. А так як кількість вхідних даних для побудови ключового елементу є частково надлишковою, то в результаті його побудови можлива корекція деяких помилок.

Перелік посилань

1. Смирнов А.А. Методы и средства компьютерной стеганографии с применением сложных дискретных сигналов для защиты информации в компьютерных системах и сетях: монография / А.А. Смирнов – К.: Изд. «КОД» – 2012. – 350 с.

2. Бабич І.В. Огляд стеганографічних методів перетворення інформації в зображеннях / Бабич І.В., Паламарчук С.А., Паламарчук Н.А., Овсянніков В.В. // Захист інформації. – 2012. – № 1. – С. 18-24.

3. Стасюк О.І. Сучасні стеганографічні методи захисту інформації / Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. // Захист інформації. – 2011. – № 1. – С. 1-7.

4. Бабенко В.Г. Метод вбудовування стегоповідомлення на основі ключового елементу / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко // Автоматизированные системы управления и приборы автоматики: Всеукраинский межведомственный научно-технический сборник. – Х.: Харьковский Национальный университет радиоэлектроники. – 2014. – Вып. 168. – С. 53-58.

5. Петров В. П. Проектирование цифровых систем контроля и управления/ В. П. Петров. – М. : Машиностроение, 1967. – 459 с.

6. Матвеевский В.Р. Надежность технических систем. Учебное пособие – Московский государственный институт электроники и математики. М., 2002 г. – 113 с.

References

1. Smirnov, A.A. Methods and tools for computer steganography using complex discrete signals for protection of information in computer systems and networks. Monograph. Kyiv: publishing house "KOD", 2012. 350p. (Ukr)

2. Babych, I.V., Palamarchuk, S.A., Palamarchuk, N.A., Ovsyannikov, V.V. Overview of steganographic methods of converting information in images. Information protection. 2012. No. 1. P. 18-24. (Ukr)

3. Stasyuk, O.I., Gnatyuk, S.O., Dovgych, N.I, Litosh, M.S. Modern steganographic methods of information protection. Information protection. 2011. No. 1. P. 1-7. (Ukr)

4. Babenko, V.G., Zazhoma, V.M., Nesterenko, O.B. The method of embedding steganographic messages based on key elements. Automated control systems and automation equipment. 2014. Vol. 168. P. 53-58. (Ukr)

5. Petrov, V.P. Design of digital control systems. Moscow: Mashinostroenie, 1967. 459p. (Rus)

6. Matveevskiy V.R. The reliability of technical systems. Study Guide. Moscow-th-State Institute of Electronics and Mathematics. 2002. 113p. (Rus)