УДК 004.415.24:004.056.5

ПРИХОВУВАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У ДОКУМЕНТІ МЕТОДОМ ЗМІНИ КІЛЬКОСТІ ПРОПУСКІВ МІЖ СЛОВАМИ ВИРІВНЯНОГО ЗА ШИРИНОЮ ТЕКСТУ

Крижановська О.Л.

Кухарська Н.П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук

ЛДУ БЖД

На сучасному етапі розвитку інформаційних систем і технологій, глобальних комп’ютерних мереж і засобів мультимедіа як ніколи є актуальною проблема передачі інформації з обмеженим доступом незахищеними каналами зв’язку. При цьому необхідним є виконання такоївимоги: інформація, яка передається від одного абонента іншому, не має стати доступною третій особі. Для розв’язання сформульованої задачі інформаційної безпеки недостатньо зробити інформацію недоступною для порушника; часто треба приховати сам факт її передачі чи зберігання. Цим і займається наука стеганографія.

Розглянемо процедуру стеганографічного приховування інформації у текстовому файлі методом зміни кількості пропусків між словами. Згідно цього методу конфіденційна інформація вбудовується у відкритий текст шляхом вкраплення додаткових символів пропуску, місцезнаходження яких визначається на основі алгоритму[1], який нагадує алгоритм манчестерського кодування.

Розглянемо суть методу на нижче наведеному прикладі.

Фрагмент порожнього текстового контейнера подано на рис.1. Приховуване повідомлення – “життя”.Стеганографічнийзахист конфіденційної інформації передбачає розгляд ASCII-кодів символів конфіденційного повідомлення у двійковому їх представленні.Тоді текст приховуєтьсяокремими бітами.

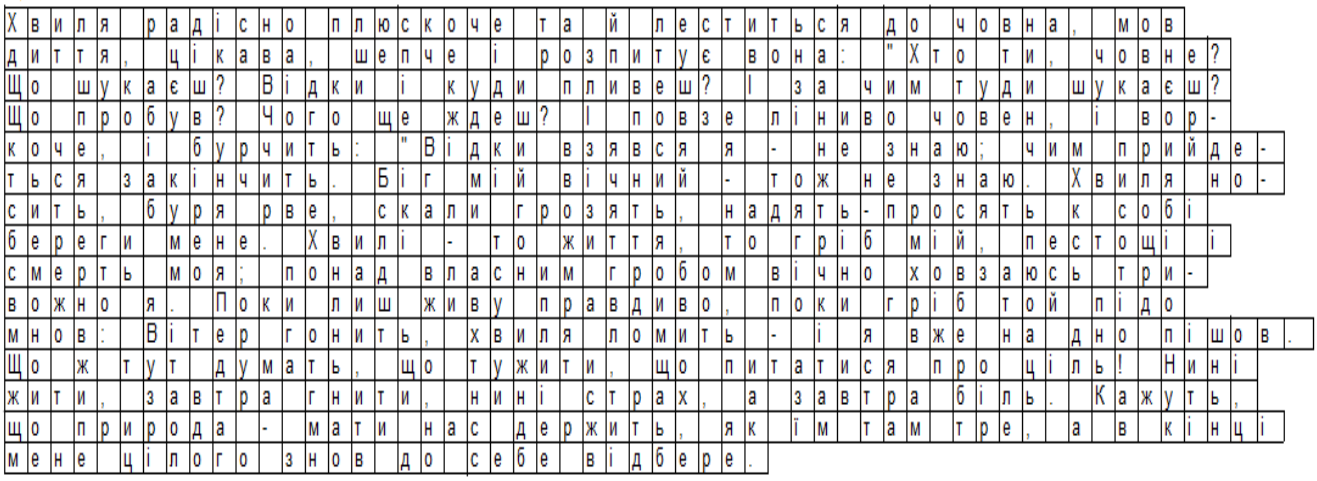

Рис 1. Фрагмент порожнього (до вбудовування) текстового контейнера

Згідно алгоритму методу зміни кількості пропусків між словами визначається рядок текстового контейнера, що має найбільшу кількість символів. У нашому випадку це 11-ий рядок. До нього дані не вбудовуватимуться.До всіх інших рядків (назвемо їх короткими) між словами додаватиметься така кількістьпропусків, щоб на виході отримати текст вирівняний за шириною.

Процедура вбудовуваннякожного біту даних конфіденційного повідомлення до текстового контейнера передбачає виокремленняукоротких рядкахпар пропусків, якимивідділяютьсяслова. Додатковий пропуск додається на початок або в кінець слова, в залежності від значення приховуваного біту: після першого пропуску, якщо приховується біт із значенням 1 або після другого, якщо біт, який слід приховати, дорівнює 0.

Фрагмент результату вбудовування з використанням розробленої MathCad-програми повідомлення до текстового контейнера наведено на рис.2. У даному фрагменті приховано 24 біти повідомлення, що відповідає його першим трьом символам ("жит"). Так, у 1-му рядку приховано біти 011, у 2-му – 001, у 3-му –110(маємо символ "ж"), у 4-му – 001,у 5-му – 0, у 6-му – 1, у 7-му – 11(маємо символ "и"), у 8-му – 010 у 9-му – 01, у 10-му – 111 (маємо символ "т").

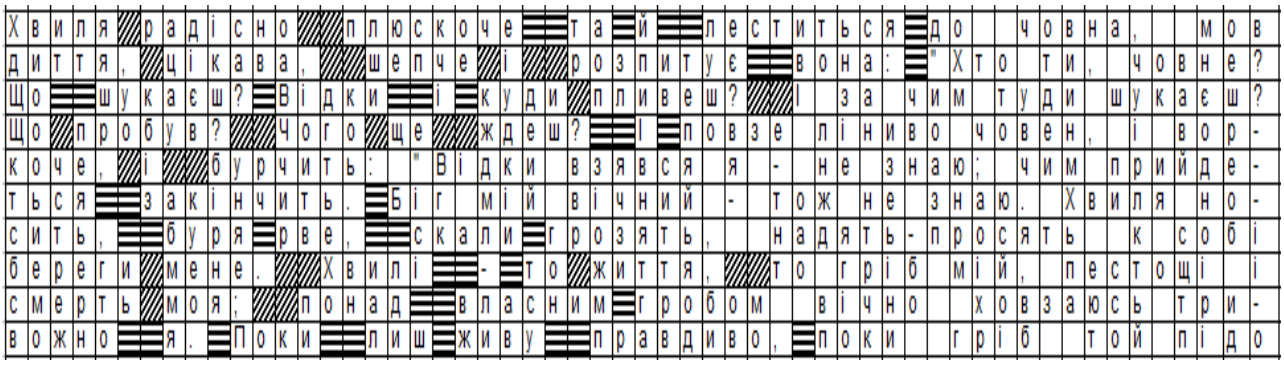

Рис. 2. Фрагмент тексту заповненого методом зміни кількості пропусків між словами вирівняного за шириною (кожна тріадапропусків позначених приховує нульовий біт повідомлення, а тріада пропусків позначених – одиничний біт)

Пропускна здатність цієїстеганосистеми– 0,8%.

Розглянутий методє ефективним за умови, що текст представлено у форматі ASCII. Деякі приховані дані можуть виявитися втраченими після роздрукування тексту.

ЛІТЕРАТУРА

1. Bender W. Techniques for Data Hiding / Bender W.,GruhlD., MorimotoN., Lu A. // IBM Systems Journal. – 1996. –№ 35. – PP. 313-336.
2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : Изд-во "МК-Пресс", 2006. – 288 с.