ВИКОРИСТАННЯ МЕТОДУ ФАЗОВОГО КОДУВАННЯ ДЛЯ ПРИХОВУВАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В АУДІОФАЙЛАХ

Ковальчук С. О., Кухарська Н. П.
Львівський державний університет безпеки життєдіяльності

Розглянуто перспективи застосування стеганографічних методів для захисту інформації. Зроблено огляд методів, що використовують у ролі стеганоконтейнерів файли аудіоданих. Подано алгоритм методу фазового кодування, який реалізовано у середовищі системи комп'ютерної алгебри MathCad.

Ключові слова: стеганографія, захист інформації, аудіофайл, метод фазового кодування.

The article tells about the prospects of using steganographic methods of information protection and provides the review of methods that use audio files in a form of steganocontainers. Besides it dwells upon the algorithm of phase encoding method that is implemented in computer algebra system MathCad.

Keywords: steganography, information protection, audio files, method of phase coding.

Мережева безпека стає все більш актуальною з огляду на зростаючі обсяги даних, які пересилаються каналами локальних і глобальних мереж. Для захисту інформації від несанкціонованого доступу та використання необхідно забезпечити конфіденційність і цілісність даних, особливо якщо вони є надзвичайно важливі, наприклад, стосуються ведення секретних переговорів, є номерами рахунків, кодами доступу, тощо.

Захист інформації може бути забезпечено криптографією, стеганографією, або одночасно криптографією і стеганографією [1]. При використанні криптографії інформація модифікується, перетворюється. У результаті перетворень приховується зміст повідомлення. На даний час криптографічні засоби можуть затягнути процес отримання зловмисником доступу до конфіденційних даних (через необхідність розшифрування даних), але навряд чи зупинить його. Стеганографія, в свою чергу, приховує сам факт передачі або зберігання інформації. Це досягається шляхом впровадження інформації з обмеженим доступом в різні мультимедійні об'єкти (контейнери). Приховування реалізовується таким чином, щоб, по-перше, не були втрачені властивості і деяка цінність приховуваної інформації, а по-друге, неминуча модифікація інформаційного носія, не тільки не знищила смислові функції, але і на певному рівні абстракції навіть не змінила їх.

Як контейнери використовують файли різних форматів, мережеві пакети і т. д. Відповідно до обраного типу контейнера обираються методи приховування інформаційних потоків. Розглянемо методи приховування даних в аудіосигналах [2].

1) Кодування найменш значущих бітів (часова область).

Даний метод є найпростішим серед методів приховування даних у аудіосигналах. Його суть полягає у заміні найменшого значущого біту у кожній точці вибірки із аудіосигналу, представленого у двійковій послідовності, на біт приховуваного повідомлення. Використання цього методу характеризується високою пропускною здатністю каналу, платою за що є ледь відчутний низькочастотний шум.

2) Метод розширення спектра (часова область).

Цей метод майже ідентичний до методу приховування даних у нерухомих зображеннях Секретне повідомлення розподіляється по частотах несучого сигналу рівномірно, так щоб співвідношення сигнал (повідомлення)/шум у каналі було дуже низьким і не викликало підозр щодо наявності повідомлення. Сигнал-контейнер, в даному випадку, обирається набагато більший за обсягом у порівнянні з секретним повідомленням.

3) Приховування даних із використанням ехо-сигналу.

Даний метод вбудовує повідомлення у аудіосигнал-контейнер шляхом введення у нього ехо-сигналу. Дані приховуються за допомогою зміни параметрів ехо-сигналу: початкової амплітуди, швидкості затухання та зсуву. Коли зсув між оригінальним сигналом та ехо-сигналом зменшувати, то починаючи з певного значення, слухова система людини стає нездатною виявити різницю між двома сигналами, а ехо-сигнал сприймається лише як додатковий резонанс. Цей метод непростий у реалізації, тому що описане значення зсуву дуже

важко визначити. Воно значною мірою залежить від якості початкового сигналу і, зрозуміло, від слухача.

4) Метод фазового кодування (частотна область).

Існують різні варіації методів вбудовування інформації на основі фазового кодування. Суть методів модифікації фази полягає в зміні фази кожної частотної складової дискретного сигналу. Для цього вихідний сигнал розбивають на серію коротких сегментів, що містять однакову кількість елементів (відліків). Кількість елементів повинна бути більша ніж кількість біт у переданому повідомленні удвічі. До кожного сегмента застосовують дискретне перетворення Фур'є, у результаті якого для кожного сегмента утворюються масиви фаз і амплітуд. Для збереження скритності повідомлення необхідно запам'ятати різницю фаз між сусідніми сегментами, так як слухова система людини більш чутлива до різниці фаз, ніж до абсолютних значень фази. Приховування повідомлення реалізують на основі модифікації фаз першого сегменту. Вбудовування інформації здійснюють шляхом заміни вихідного значення фази на значення, що дорівнює $-\pi/2$, якщо приховуваний біт повідомлення є нулем, і на значення $\pi/2$, якщо біт повідомлення дорівнює одиниці. Щоб зберегти первинну різницю фаз, необхідно до отриманого масиву фаз першого сегмента додати раніше обчислений масив різниць між першим і другим масивом фаз, і так далі для кожного масиву фаз. Для відновлення звукового сигналу слід виконати зворотне дискретне перетворення Фур'є для масивів амплітуд і модифікованих масивів фаз.

Розглянемо процедуру фазового кодування поетапно [2]:

1) Звукова послідовність $\boldsymbol{S}[\boldsymbol{i}]$, $(1 \le \boldsymbol{i} \le \boldsymbol{I})$ розбивається на серію $\boldsymbol{N}$ коротких сегментів (блоків) $\boldsymbol{S_n}[\boldsymbol{i}]$, $(1 \le \boldsymbol{n} \le \boldsymbol{N})$, де i – номер відліку сигналу, I – розмірність сигналу, n – номер сегменту.

2) До кожного $\boldsymbol{n}$-го сегмента сигналу $\boldsymbol{S_n}[\boldsymbol{i}]$ застосовується $\boldsymbol{K}$-точкове ДПФ, де $\boldsymbol{K} = \boldsymbol{I}/\boldsymbol{N}$, та створюються масиви фаз $\phi_{\boldsymbol{n}}(\omega_{\boldsymbol{k}})$ і амплітуд $\boldsymbol{A_n}(\omega_{\boldsymbol{k}})$ для $1 \le \boldsymbol{k} \le \boldsymbol{K}$

3) Запам'ятовується різниця фаз між кожними сусідніми сегментами для $1 < \boldsymbol{n} \le \boldsymbol{N}$:

$$\Delta\phi_{\boldsymbol{n}}(\omega_{\boldsymbol{k}}) = \phi_{\boldsymbol{n}}(\omega_{\boldsymbol{k}}) - \phi_{\boldsymbol{n}-1}(\omega_{\boldsymbol{k}}); \quad \Delta\phi_1(\omega_{\boldsymbol{k}}) = 0.$$

4) Двійкова послідовність даних повідомлення подається як $\phi_{data} = \pi/2$ або $\phi_{data} = -\pi/2$, відображуючи відповідно «1» або «0»: $\phi'_1(\omega_{\boldsymbol{k}}) = \phi_{data}$.

5) З урахуванням різниці фаз відтворюється новий масив фаз для $\boldsymbol{n} > 1$:

$$\left\| \begin{array}{c} \phi'_1(\omega_{\boldsymbol{k}}) = \phi_{data} \\ \phi'_2(\omega_{\boldsymbol{k}}) = \phi'_1(\omega_{\boldsymbol{k}}) + \Delta\phi_2(\omega_{\boldsymbol{k}}) \\ \Lambda \\ \phi'_{\boldsymbol{n}}(\omega_{\boldsymbol{k}}) = \phi'_{\boldsymbol{n}-1}(\omega_{\boldsymbol{k}}) + \Delta\phi_{\boldsymbol{n}}(\omega_{\boldsymbol{k}}) \\ \Lambda \\ \phi'_{\boldsymbol{N}}(\omega_{\boldsymbol{k}}) = \phi'_{\boldsymbol{N}-1}(\omega_{\boldsymbol{k}}) + \Delta\phi_{\boldsymbol{N}}(\omega_{\boldsymbol{k}}) \end{array} \right\|$$

6) Відновлення звукового сигналу проводиться шляхом застосування оберненого ДПФ до первинної матриці амплітуд і модифікованої матриці фаз.

Недоліком описаного методу є дещо низька пропускна здатність.

Розроблений нами в середовищі універсальної математичної системи MathCad програмний комплекс, що реалізовує описаний вище підхід фазового кодування даних в аудіосигналах, може бути придатним як для корпоративного, так і для особистого використання з метою приховування конфіденційної інформації під час пересилання її каналами комп'ютерної мережі.

Література

1. Юдін О. К. Захист інформації в мережах передачі даних : підручник / Юдін О. К., Конахович Г. Ф., Корченко О. Г. – К. : Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.
2. Конахович Г. Ф. Компьютерная стеганография / Конахович Г. Ф., Пузыренко А. Ю. – К. : МК-Пресс, 2006. – 288 с.