УДК 681.12

В. Ю. Грущенко

ЗАСІБ ДЛЯ РОЗПОДІЛУ СЕКРЕТУ

Вінницький національний технічний університет

Анотація

Запропоновано засіб для розподілу секрету, що базується на розподілу певної інформації у декілька контейнерів з метою посилення конфіденційності даних.

Ключові слова: стеганографія; захист авторських прав; конфіденційність; *LSB-метод*; розподіл секрету

Abstracts

A secret sharing tool based on the distribution of a specific information into multiple containers to enhance data confidentiality is proposed.

Keywords: steganography; copyright protection; privacy; LSB method; secret sharing

Вступ

Питання розроблення ефективних методів захисту цифрової інформації, зокрема методів комп'ютерної стеганографії та стеганоаналізу, актуальні та мають важливе значення для держави й суспільства [1,2].

Метою роботи є розроблення засобу для розподілу секрету у декілька контейнерів, що унеможливить потенційного зловмисника ознайомитись з секретом, оскільки для повного отримання доступу необхідно буде мати всі контейнери.

Результати дослідження

У разі перехоплення інформації зловмисником він не зможе ознайомитися з інформацією, що при

До того ж впровадження таким чином інформації легко виявити стеганографічними атаками [3].

Використовується поєднання декілька методів приховування інформації. Безпосередньо для зображення використовується метод LSB, а розподіл секрету здійснюється за схемою Шаміра.

Для більшої міри захисту інформації, прихованої в зображенні методом заміни, можна застосовувати криптографічні методи, які будуть шифрувати повідомлення перед його вкрапленням, а також застосовану схему розподілу секрету Шаміра, накладаючи при цьому ключ [4].

Порогова схема Шаміра побудована навколо концепції поліноміальної інтерполяції зображена на рис 1.

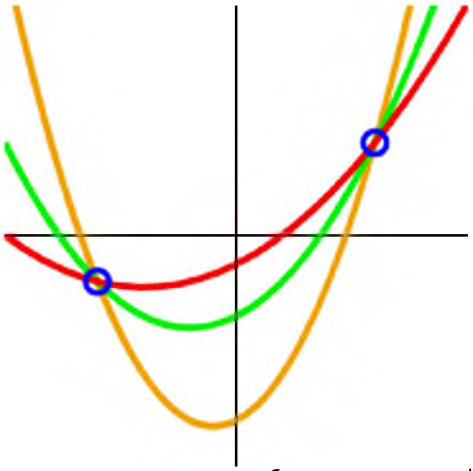

Рис.1 Через дві точки можна провести необмежене число поліномів степеня 2

Для генерації частин секрету необхідно вирахувати значення в n різних точках.

$$k_1 = F_1 = \left(a_{k-1} \cdot 1^{k-1} + a_{k-2} \cdot 1^{k-2} + \cdots + a_1 \cdot 1 + M\right) mod\, p \quad (1)$$
$$k_n = F_n = \left(a_{k-1} \cdot n^{k-1} + a_{k-2} \cdot n^{k-2} + \cdots + a_1 \cdot n + M\right) mod\, p$$

де M - це розподілений секрет, а a_{k-1}, a_{k-2}, a_1 коефіцієнти - деякі випадкові числа.

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

Запропоновано метод для розподілу секрету, що базується на розподілу інформації у декілька контейнерів з метою посилення конфіденційності даних.

З точки зору безпеки важливою властивістю цієї схеми є те, що зловмисник не повинен дізнатися абсолютно нічого, навіть якщо у нього є хоча б частина контейнерів. Наявність частин не повинно давати ніякої інформації.З точки зору безпеки це є семантичної безпекою.

Висновки

Отримані в роботі результати дозволяють значно підвищити стійкість стеганографічної системи до атак.

Розроблено програмний засіб з використанням методу LSB, що підвищує рівень захисту інформації від несанкціонованого доступу за рахунок приховування її у мультимедійних файлах, а саме у файлах зображень, метод розподілу секрету дозволить посилити та забезпечити конфіденційність даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави / С.В.Мельник, С.В.Кондакова // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. – К. : Наук.-вид. відділ НА СБ України, 2010.
2. Міжнародні стандарти "Управління інформаційною безпекою": ISO/IEC 27000. Міжнародний стандарт ISO/IE
3. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
4. Image Steganography: Concepts and Practice/ Mehdi Kharrazi , Husrev T. Sencar , and Nasir Memon/31 c.

Грущенко Владислав Юрійович — студент групи 1БС-18мс, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vladyslavh98@gmail.com

Науковий керівник: ***Лукічов Віталій Володимирович***— к. т. н., старший викладач, Вінницький національний технічний університет, м. Вінниця

Hrushchenko V. Y. — student of 1BS-18ms group, Faculty of Information Technologies and Computer Engineering, Vinnitsa National Technical University, Vinnitsya, e-mail: vladyslavh98@gmail.com

Supervisor: ***Lukichov V. V.*** — candidate of Technical Sciences, senior Lecturer, Vinnitsa National Technical University, Vinnitsa