

Розробка програмного забезпечення методу приховання інформації у мережі на основі стеганографії

А.В. Чорна, студент,
О.А. Смірнов, доцент, канд. техн. наук, Є.В. Мелешко, канд. техн. наук
Кіровоградський національний технічний університет

Дослідження проблем розробки, удосконалювання й застосування методів захисту інформації в процесі її зберігання й передачі привертає увагу безлічі дослідників, тому що розробка нових і вдосконалювання наявних методів захисту має велике значення для розвитку інфокомунікаційних систем.

У сучасних системах захисту інформації величезну роль грають не тільки методи криптографії, але й методи стеганографії. Якщо класичне завдання криптографії полягає в тому, щоб сховати від третіх осіб зміст повідомлення, то класичне завдання стеганографії – сховати сам факт передачі повідомлення. Зазначене завдання стеганографії вирішується за допомогою впровадження повідомлень у необразливі на вид об'єкти даних, називані контейнерами, передача яких є звичайною справою й не викликає підозр. Ключовим поняттям стеганографії є стегосистема, тобто сукупність засобів і методів, використовуваних для організації схованого каналу передачі даних. Існує й ряд інших актуальних завдань, які належать стеганографії, наприклад, захист авторських прав, що також базується на впровадженні в авторські цифрові документи схованих повідомлень, що ідентифікують автора або законних одержувачів.

Ціль роботи полягає в розробці нових методів впровадження інформації й визначенні границь стійкості стеганографічних систем. Об'єктом досліджень є процес формування стегосистеми для цифрових зображень. Предмет досліджень складається реалізації стеганографічних систем, що володіють у деякому максимально можливому ступені тими властивостями, які властиві зробленим стегосистемам.

Методи дослідження. У процесі проведення досліджень були використані основні положення й методи теорії інформації, теорії ймовірностей, алгоритми стиску даних, алгоритми криптографії й експерименти на комп'ютері.

Наукова новизна результатів роботи: 1) побудовано статистичну модель зображення, що дозволяє оцінювати ймовірності значень молодших біт пікселів; 2) розроблено й досліджено стеганографічну систему, що дозволяє вбудовувати й витягати інформацію на основі побудованої статистичної моделі зображення; 3) на основі результатів зроблених стегосистем розроблений комбінаторний метод впровадження інформації в зображення.

Практична цінність отриманих результатів: 1) для досить розповсюджених графічних форматів даних (BMP, TIFF, PNG, PCX, TGA і ін.) побудовані методи впровадження схованої інформації; 2) розроблені конструкції стегосистем можуть бути легко реалізовані на практиці для більшості графічних форматів даних, що використовують методи стиску, що не спотворюють; 3) запропоновані стеганографічні методи дозволили скорегувати убік зменшення оцінку розв'язної здатності відомих методів стегоаналізу.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.