УДК 004.932.2

СИСТЕМИ ЗАХИСТУ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ

Зарічний П.Б., Коленко В.В.

Науковий керівник – ст. викл. каф. «Інформаційних систем», канд. техн. наук Нарожний О.В.

Сучасний прогрес в області глобальних комп'ютерних мереж і засобів мультимедіа привів до розробки нових методів, призначених для забезпечення безпеки передачі даних по каналах телекомунікації. Ці методи, враховуючи природні неточності пристроїв оцифровки і надмірність аналогового відео або аудіо сигналу, дозволяють приховувати повідомлення в комп'ютерних файлах. Дані методи приховують сам факт передачі інформації. Аналіз інформаційних джерел комп'ютерної мережі Internet дозволяє зробити висновок, що в даний час стеганографічні системи активно використовуються для вирішення наступних основних завдань:

1. Захист конфіденційної інформації від несанкціонованого доступу;
2. Подолання систем моніторингу і управління мережевими ресурсами;
3. Камуфляжі програмного забезпечення;
4. Захист авторського права на різні види інтелектуальної власності.

Мета роботи: Створити систему захисту авторських прав на основі стеганографічних алгоритмів з використанням цифрових водяних знаків.

Стеганографічні вставки, або цифрові водяні знаки (ЦВЗ) застосовуються, для того, щоб комп'ютерний файл, що є об'єктом авторського права, не міг бути змінений без відома автора, щоб він містив всю необхідну інформацію про правомірне використання, якщо авторська власність піддається якійсь зміні, то разом з нею змінюється і видимий водяний знак. Вбудовування цифрових водяних знаків, є основою для систем захисту авторських прав. Вони є спеціальними мітками, що впроваджуються у файл, в цифрове зображення або цифровий сигнал в цілях контролю їх правомочного використання. У загальному випадку типова схема ЦВЗ виглядає таким чином:

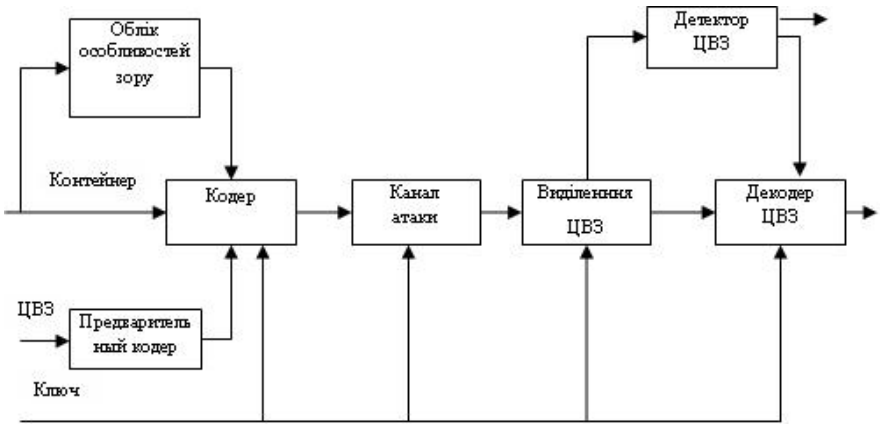

Рис.1 Схема типової стегосистеми впровадження ЦВЗ

Для збільшення працездатності стегосистем необхідно впровадити ряд поліпшень:

1.Необхідно правильний вибір параметрів псевдовипадкової послідовності, по відношенню атак типу додавання шуму. ЦВЗ повинен виявлятися при достатньо сильній низькочастотній фільтрації. Отже, база сигналу повинна бути велика. що знижує пропускну спроможність стегоканала. 2. Спосіб захисту прав власності полягає в побудові необоротного алгоритму ЦВЗ. ЦВЗ повинен бути адаптивним до сигналу і вбудовуватися за допомогою однонаправленої функції. 3. Впровадженні ЦВЗ деякої тимчасової оцінки, наданою третьою довіреною стороною. У разі появи конфлікту особа, яка має на зображенні ранішу тимчасову оцінку, вважається дійсним власником інформації. 4. Іншим методом захисту від подібних атак є блоковий детектор. Модифіковане зображення розбивається на блоки розміром 12x12 або 16x16 пікселів, і для кожного блоку аналізується всі можливі перекручення. Тобто пікселі в блоці піддаються поворотам, перестановкам і т.д. Стегосистеми водяних знаків повинні виконувати завдання захисту авторських прав на електронні повідомлення при різних спробах активного порушника спотворення або видалення вбудованої в них аутентифікаційної інформації. Системи ЦВЗ повинні забезпечувати аутентифікацію відправників електронних повідомлень.

Необхідно зафіксувати алгоритми вбудовування і витягання ЦВЗ. Оскільки використання ЦВЗ не регламентується спеціальними законами. За допомогою метода оборотного приховання даних у файлах (Reversible Data Hiding, RDH) можна реалізувати впровадження ЦВЗ, що зберігають зображення. Суть його полягає в тому, що у файл вбудовуються непомітні контрольні дані, що містять інформацію про його змінну частину, тобто про весь файл за винятком ЦВЗ. Спосіб зберігання подібних даних усередині контрольованого файлу, пропонований RDH, представляється вельми зручним. При витяганні з файлу ЦВЗ його можна привести до первинного вигляду. Крім того, завжди можна переконатися, чи проводилися із зображенням, що захищалося, які-небудь зміни

після вставки даних. Актуальність проблеми інформаційної безпеки, а саме захисту авторських прав за допомогою стеганографічних алгоритмів постійно зростає і стимулює пошук нових методів захисту інформації. Величезним каталізатором цього процесу є лавиноподібний розвиток комп'ютерних мереж загального використання Internet, зокрема такі не розв'язані суперечливі проблеми Internet, як захист авторського права, захист прав на особисту таємницю, організація електронної торгівлі, протизаконна діяльність хакерів. Контроль контента потокової мультимедійної інформації. Забезпечення захисту інтелектуальної власності електронної інформації з урахуванням сучасних вимог неможливе без застосування даного напряму стеганографії.

СПИСОК ЛІТЕРАТУРИ

1. Генне О.В., Основные положения стеганографии // Защита информации. Конфидент, N3, 2000
2. Грибунин В.Г., Цифровая стеганография, СОЛОН-Пресс, 2002
3. Городецкий В.И., Самойлов В.В., Стеганография на основе цифровых изображений // Информационные технологии и вычислительные системы, №2/3, 2001, с. 51-64.