Удосконалена система стеганографічного захисту інформації

УДК 004.056.55:003.26

Олександр Мельник

Національний авіаційний університет, Україна, melnyk.mail@icloud.com

Сьогодення характеризується великою кількістю різного мультимедійного контенту: аудіозаписи, відеозаписи, цифрові зображення, тощо. Звісно при такому великому обсязі контенту є така інформація, що виділяється та становить цінність. Стеганографічні алгоритми використовуючи непримітні об'єкти – контейнери (мультимедійні об'єкти) дозволять приховати цінну інформацію, а оскільки більша частина інформації знаходиться у вільному доступі то такі об'єкти інформаційного простору можливо використовувати, як контейнери. Хоча й існує велика кількість стеганографічних алгоритмів присутня потреба розробки більш ефективних алгоритмів приховування інформації, що можуть забезпечити невидимість, стійкість до активних атак та збільшення розмірів інформації, що буде прихована. Тому дана робота є актуальною.

Метою даної роботи є удосконалення стеганографічної системи захисту інформації для підвищення ефективності вбудовування секретної інформації. Типова систему стеганографічного захисту інформації складається з таких елементів: 1) абоненти А і В перед початком сенсу зв'язку погоджують множину контейнерів K: $K=\{K_1,...K_n\}$, де K_i − один з вибраних контейнерів, $i=\overline{1,n}$, $n\in N$; 2) абонент А приховує секретне повідомлення M у множину контейнерів K використовуючи обраний стеганографічний алгоритм Z та отримує множину стеганоконтейнерів $K^{'}$: $K^{'}=F_{cod}(K,M,Z)$, де $K^{'}=\{K_1^{'},...K_n^{'}\}$, де $K_i^{'}$ − один з отриманих стеганоконтейнерів, $i=\overline{1,n}$, $n\in N$, F_{cod} − процедура вбудовування секретного повідомлення у множину контейнерів K; 3) відкритим каналом зв'язку абонент А передає множину стеганоконтейнерів $K^{'}$ абоненту В; 4) абонент В відновлює секретне повідомлення M використовуючи множину контейнерів K та множину стеганоконтейнерів $K^{'}$: $M=F_{dec}(K,K^{'},Z)$, де F_{dec} − процедура вилучення секретного повідомлення M. Запропоновано у якості стеганографічного алгоритму Z використовувати алгоритм найменш значущого біта та нові процедури F_{cod} та F_{dec}. У даних процедурах буде розраховуватись об'єм та місце вбудовуваання повідомлення, яке буде приховуватися у обраний контейнер. Це дозволить гнучко керувати вбудовуванням секретної інформації.

У роботі наведено удосконалену систему стеганографічного захисту, що може бути використана у системах захисту інформації для підвищення їхньої ефективності.

Науковий керівник – доцент НАУ, Володимир Щербина