МОДЕЛЬ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В КОНТЕЙНЕРАХ МУЛЬТИМЕДІЙНИХ ДАНИХ

Картушин О.А., Харченко Н.А., Томак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Надійний захист інформації від несанкціонованого доступу є актуальною, але не вирішеною в повному обсязі проблемою. Застосування новітніх засобів автоматизації та зв'язку вимагають більш швидких та надійних засобів і методів захисту інформації. Одним з можливих рішень задачі підвищення інформаційних систем є застосування методів цифрової стеганографії [1]. Використовуючи методи стиснення інформації, методи криптографії руйнують закономірності вбудовування інформації, що приводить до збільшення часу обробки даних, що в умовах передачі даних в режимі реального часу є майже неможливим. Для подолання даної проблеми доцільно використовувати методи цифрової стеганографії при яких об'єм даних не змінюється і не руйнується закономірність вбудовування інформації. Пропонується використовувати методи цифрової стеганографії для перспективних автоматизованих систем обробки інформації, при роботі з мультимедійними видами трафіку, центрах обробки кризисної інформації та іншим сферах, де необхідно впроваджувати надійний рівень захисту інформації. Таким чином тематика досліджень, які полягають в підвищенні захисту та достовірності інформації в системах управління для перспективних автоматизованих систем обробки галузево-важливої інформації в умовах наявності зловмисника є актуальною.

Метою доповіді є побудова моделі підвищення пропускної спроможності каналу передачі мультимедійних даних на основі стеганографічного перетворення в умовах дії зловмисника.

Цифрова або digital стеганографія представляє собою процес утаєння факту приховування корисного інформаційного повідомлення (відкритого тексту) в іншому повідомленні, що реалізується з метою забезпечення конфіденційності передачі даних. Причому процес приховування даних, буде подібним до процесу компресії і відмінним від операції шифрування. Його метою є не обмежувати чи регламентувати доступ до файлу – контейнера, а в значній мірі гарантувати, що вбудовані дані залишаться непошкодженими (немодифікованими) і такими, що підлягають відновленню [3].

Приховання значних обсягів інформації потребує місткого контейнера, розмір якого має значно перевищувати обсяг прихованих даних. Для підвищення ефективності процесу, перед вбудовуванням інформації, її зазвичай шифрують, а контейнер готують, оптимізуючи для приховування даних.

При розробці системи приховування важливої інформації необхідно враховувати можливість навмисних змін контейнера зловмисниками. Під час передачі контейнер (відео, зображення тощо) може бути трансформований, наприклад, змінено його розмір або формат. Для забезпечення цілісності прихованого повідомлення може знадобитися використання завадостійкого кодування. Використання зображень як контейнерів є перспективним напрямком

розвитку стеганографії, що є частиною стратегії захисту важливої інформації. В деяких випадках стеганографія може бути альтернативою криптографічним методам [4].

В доповіді вказано, що методи цифрової стеганографії мають ряд недоліків: низька стійкість до атак, невеликий обсяг стеганографічної ємності, незадовільне значення пропускної спроможності та є нестійкими при передачі зображень та активних атак зловмисника можлива втрата даних.

Обгрунтовано необхідність упровадження удосконалених методів цифрової стеганографії в системах захисту інформації [2].

Сформульовано рекомендації щодо підвищення пропускної здатності стеганографічних методів за рахунок використання підходів до вбудовування інформації в область частотних або просторово-частотних перетворень. На основі проведених досліджень розроблено метод підвищення ефективності функціонування прихованого каналу передавання відеоінформаційних ресурсів, який базується на використанні комбінованого стеганографічного перетворення. Відмінність розробленого методу полягає у підвищення пропускної спроможності скритого каналу передачі відеоінформаційних ресурсів в середньочастотні коефіцієнти в зображення-контейнер у якому відсутні монотонність та різкі перепади яскравості за допомогою вейвлет-перетворення та дискретно косинусного перетворення.

Розраховано показники якості розробленого стеганографічного методу. Даний метод має пропускну спроможність каналу в середньому на 1,5 раз вищу ніж інші методи приховування інформації.

Розроблений метод є стійким до відомих активних атак та стеганографічного аналізу зі сторони зловмисника.

Список літератури

1. Barannik V., Khimenko V., Barannik N., Method of indirect information hiding in the process of video compression. Radioelectronic and Computer Systems. 2021. №. 4. PP. 119 131. https://doi.org/10.32620/reks.2021.4.

2. V. Barannik, M. Babenko, A. Berchanov, V. Barannik, R. Onyshchenko and L. Kolodiichuk, "Method of Mini Segments Encoding in Difference Space Using Haar Wavelet," 2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT), Lviv, Ukraine, 2023, pp. 1-4, doi: 10.1109/AICT61584.2023.10452674.

3. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія та практика / А. Ю. Пузиренко — Київ: МК - Пресс, 2016. — 288 с.

4. V. Barannik, Y. Babenko, V. Barannik, V. Kolesnyk and D. Zhuikov, "Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 66-71, doi: 10.1109/ATIT58178.2022.10024193.