УДК 004.415.24:004.056.5

ПРОГРАМНИЙ ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ОСНОВІ МЕТОДУ БЛОКОВОГО ПРИХОВУВАННЯ ЇЇ В ЗОБРАЖЕННІ

Піліпіха О. В.

Кухарська Н. П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук, доцент

Останнім часом для створення захищених каналів обміну даними все частіше використовують методи комп'ютерної стеганографії (КС). Впровадити приховані канали передачі даних в інформаційні потоки, що традиційно циркулюють в інформаційно-комунікаційних системах: соціальних мережах, службах обміну та передачі мультимедійних даних тощо – ось, яка основна ідея побудови стеганографічних систем зв'язку.

Ключовими положеннями сучасної КС є [1]:

- методи приховування повинні забезпечувати автентичність і цілісність файлу-контейнера;
- передбачається, що зловмиснику повністю або частково відомі можливі стеганографічні методи;
- безпека інформаційних технологій ґрунтується на збереженні основних властивостей відкрито переданого файлу після вбудовування в нього на основі стеганографічних перетворень повідомлення і деякої невідомої інформації – ключа;
- навіть якщо факт приховування повідомлення і стане відомий зловмиснику, то отримати саме повідомлення є надзвичайно складною обчислювальною задачею.

Результати досліджень [2] показали, що переважна більшість відомих стеганографічних програм заснована на застосуванні цифрових зображень як файлів-контейнерів. Це пояснюється [2,3]:

- Надлишковістю цифрового представлення цифрових зображень, що дає можливість приховувати значні об'єми стегоданих або підвищувати стійкість (робастність) отримуваних стеганограм до відомих методів пасивного стегоаналізу.
- Наявністю у більшості цифрових зображень областей, що мають шумоподібну структуру, наприклад, зображення хмар, трави, піску. Застосування зазначених областей дозволяє маскувати факт приховання повідомлень при формуванні стеганограм.
- Необхідністю використання обчислювально складних методів статистичного моделювання даних цифрових зображень для виявлення стеганограм.

Робота присвячена розробці комплексу програм на основі стеганографічного методу

блокового приховування [3].

Передбачувана область використання створеного комплексу – передача засобами мережі Інтернет даних, таємність яких повинна зберігатися протягом нетривалого проміжку часу (кілька днів).

Для забезпечення більшої кількості даних, що можна вбудувати, був обраний 24-бітний BMP формат зображення-контейнера.

Метод блокового приховування даних є модифікацією методу заміни найменш значущих біт (НЗБ). У НЗБ-методі вбудовування приховуваних повідомлень здійснюється в молодші значущі біти файлу-контейнера. Вважається, що молодші біти графічної інформації, представленої у форматах файлів без втрат, не несуть істотних відомостей про зображення, так як знаходяться на рівні шуму. Тому людина не здатна помітити зміни в цих бітах. Фактично молодші біти є похибкою в будь-якому медіа форматі, для якого число біт у відліку дорівнює або більше восьми. Для таких форматів неможливо візуально визначити наявність прихованого повідомлення. Переваги методу полягають в простоті реалізації і великому обсязі вбудованих даних, а також, у повній непомітності вбудованого повідомлення. Недоліком методу є те, що приховане повідомлення легко зруйнувати.

Згідно алгоритму методу блокового приховування зображення-оригінал розбивається на блоки довільної конфігурації, які не перетинаються. Кількість блоків дорівнює кількості біт повідомлення. У кожному блоці приховуватимемо один секретний біт описаним нижче чином. Для кожного блоку обчислюватимемо біт парності, додаючи за модулем 2 усі наймолодші значущі біти. Якщо значення біта парності не дорівнюватиме значенню поточного біта повідомлення, то інвертуватимемо один, обраний випадковим чином, НЗБ блоку, у результаті чого отримаємо повну відповідність значень приховуваних бітів та бітів парності.

Зауважимо, стеганографічний метод блокового приховування має нижчу пропускну здатність у порівнянні з НЗБ-методом. У той же час він має свої переваги. Зокрема, існує можливість модифікувати значення такого пікселя в блоці, зміна якого призведе до мінімальної зміни статистики контейнера [3].

ЛІТЕРАТУРА

1. Барсуков В. С. Еще раз о стенографии – самой современной из древнейших наук / В. С. Барсуков, А. В. Шувалов // Специальная техника. – 2004. - № 2. – С. 51-65.
2. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / Fridrich J. – 1st Edition.. – New York : Cambridge University Press, 2009 – p. 437.
3. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : Изд-во "МК-Пресс", 2006. – 288 с.