Гунявий Д.А., студент,
Джулій В.М., к.т.н., доцент,
Чешун В.М., к.т.н., доцент
Хмельницький національний університет

ОЦІНКА СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

Стеганосистема цифрового водяного знаку (ЦВЗ) повинна будуватись так, щоб мінімізувати імовірність виникнення помилок, оскільки будь-яка помилка може привести до неправильної роботи стеганодетектора. Щодо запобігання виникненню помилок надважливою є стійкість ЦВЗ. Схема оцінювання стійкості ЦВЗ до зовнішніх дій схематично представлена на рисунку 1 (з використанням дискретного вейвлет-перетворення - ДВП).

Рисунок 2 – Схема оцінки стійкості цифрових водяних знаків

Оцінка стійкості ЦВЗ до зовнішніх дій включає наступні етапи:

1. Впровадження ЦВЗ. При проведенні досліджень на предмет порівняння стійкості ЦВЗ до різних зовнішніх дій, необхідне забезпечення однакових початкових умов для впровадження ЦВЗ [1]. Дана вимога пред'являється, в першу чергу, до стеганоконтейнеру. ЦВЗ може бути будь-яким, а його тотожність при використанні різних стеганоалгоритмів може не виконуватися. Якщо ЦВЗ виробляється випадковим чином, то результати будуть більш якісними. Об'єми ЦВЗ роблять рівними, так як ця вимога впливає на властивості ЦВЗ (стійкість тощо).

2. Зовнішня дія на стеганоконтейнер з ЦВЗ. Зовнішня дія на стеганоконтейнер може бути довільною і повною, тобто на весь стеганоконтейнер [1,2]. Важливо дотримувати однаковий рівень або діапазон інтенсивності дії при проведенні порівняльного аналізу.

3. Вилучення ЦВЗ. Вилучення ЦВЗ проводиться відповідно до методу вбудовування, об'єм зчитаного ЦВЗ повинен відповідати об'єму вбудовуваного. Застосовувати додаткові заходи при відтворенні даних ЦВЗ не можна, навіть якщо ці заходи передбачаються при вилученні використаним стеганографічним алгоритмом.

4. Оцінка стійкості ЦВЗ. Стійкість ЦВЗ оцінюється за допомогою різних методів [2]. Наприклад, використовується коефіцієнт помилкових бітів (Bit Error Rate), який застосовується при оцінці модифікацій бітової послідовності [3]:

$$BER\left(S,S^{''}\right)=\frac{\sum p_i}{N}$$

де N – загальна кількість біт, p_i=1, якщо $s_i \neq s_i^{''}$ і p_i=0, якщо $s_i \neq s_i^{''}$, де s_i – біт початкового зображення, $s_i^{''}$ – біт кінцевого зображення.

При $BER(S,S^{''})$=0 вбудовані і вилучені дані ЦВЗ співпадають. При $BER(S,S^{''})$=1 будь-який біт вхідного зображення відрізняється від вихідного (має місце «негатив»). Вважають, що при $BER(S,S^{''})\geq 0.5$ вбудовані дані втрачено.

5. Рівень викривлення. Властивість ЦВЗ, вбудованого в стеганоконтейнер, протистояти різним атакам, які пов'язані з різними причинами (алгоритм впровадження цифрового водяного знака, коефіцієнт сили вбудовування P, зовнішня дія, тощо).

У протилежність зовнішнім атакам, властивості яких можна відтворити для будь-яких стеганоконтейнерів ЦВЗ, вбудованих різними стеганографічними алгоритмами, параметри P і метод впровадження є унікальними для будь-якого стеганографічного алгоритму [3]. Створюючи єдині початкові умови, які використовуються при порівняльному аналізі стійкості ЦВЗ, зазвичай стежать за таким параметром рівня модифікацій, які з'являються при вбудовуванні ЦВЗ.

Список використаних джерел та літератури

1. Дурняк Б. В., Музика Д. В., Сабат В. І. Стеганографічні методи захисту документів. Львів : Укр. акад. друкарства, 2014. 159 с.
2. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. Київ : Вид-во DIRECTLINE, 2019. 714 с.

Belim S. V., Vilkhovskiy D. E. Method of detecting hidden data transmission via the Koch-Zhao steganographic algorithm. Journal of Physics: Conf. Series 1210 (2019) 012012. doi:10.1088/1742-6596/1210/1/012012.