ПОДХОД К ПРОТИВОДЕЙСТВИЮ АТАКАМ НА ЦИФРОВОЙ ВОДЯНОЙ ЗНАК, ВНЕДРЕННЫЙ В LUT-КОНТЕЙНЕР

к.т.н., доц. К.В. Защелкин, Е.Н. Иванова, ОНПУ, г. Одесса

Цифровой водяной знак (ЦВЗ) представляет собой данные, внедряемые в информационный объект с целью контроля его использования. Технология ЦВЗ основана на применении стеганографических приемов, в рамках которых скрывается факт наличия ЦВЗ в информационном объекте (контейнере). При этом ЦВЗ может быть считан из контейнера при наличии стего-ключа, определяющего правила доступа к элементам ЦВЗ [1]. Центральной проблемой теории ЦВЗ является противодействие активным стеганографическим атакам, которые заключаются во внесении атакующей стороной в контейнер искажений, не нарушающих целевой функции контейнера, однако разрушающих находящуюся в нем внедренную информацию. В работах [2, 3] был предложен метод внедрения ЦВЗ в аппаратные контейнеры с LUT-ориентированной архитектурой (Look Up Table – таблица поиска). Метод позволяет внедрять двоичную информацию в LUT-контейнер, подвергая элементарные единицы контейнера локальным изменениям, не меняя при этом его глобальную функциональность. Основой метода является процедура, состоящая в инвертировании значений текущего обрабатываемого блока LUT и выполнении распространения инверсии на входы всех блоков LUT, подключенных к выходу текущего блока.

В данной работе предлагается один из возможных подходов к противодействию активным атакам на ЦВЗ, внедренный в LUT-контейнер в соответствии с указанным выше методов. Подход основан на предположении, что атакующая сторона может выполнить процедуру, симметричную процедуре встраивания информации, подвергнув блоки LUT контейнера локальным изменениям, не меняя его функциональность. Для выявления и предотвращения такой возможности предлагается ввести в состав стего-ключа номер опорного разряда блока LUT, который должен принимать либо фиксированное, либо псевдослучайное значение, заданное на этапе внедрения ЦВЗ. Равенство опорного разряда заданному значению является дополнительным условием включения блока LUT в стего-путь. В этом случае, анализ опорного разряда при извлечении ЦВЗ позволяет выявить факт искажения ЦВЗ и восстановить его истинные значения.

Список литературы: 1. *Cox I.* Digital Watermarking and Steganography / *I. Cox, M. Miller, J. Bloom, J. Fridrich*. – Burlington: Morgan Kaufmann Publishers, 2008. – 592 p. **2.** *Защелкин К.В.* Метод внедрения цифровых водяных знаков в аппаратные контейнеры с LUT-ориентированной архитектурой / *К.В. Защелкин, Е.Н. Иванова* // Информатика и математические методы в моделировании. – Одесса. – 2013. – Том. 3, № 4. – С. 369 – 384. **3.** *Защелкин К.В.* Метод стеганографического скрытия данных в LUT-ориентированных аппаратных контейнерах / *К.В. Защелкин, Е.Н. Иванова* // Електротехнічні та комп'ютерні системи. – Київ. –2013. – Вип. 12 (88). – С. 83 – 90.