УДК 004.56+003.26

М.Г. Савельева, ассист. (БГТУ, г. Минск)

СТОЙКОСТЬ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ К ОТДЕЛЬНЫМ МЕТОДАМ СТЕГОАНАЛИЗА

Даже при оптимальных условиях для атаки задача извлечения скрытого сообщения из контейнера может оказаться очень сложной. Однозначно утверждать о факте существования скрытой информации можно только после ее выделения в явном виде. Иногда целью стеганографического анализа является не восстановление алгоритма, а поиск, например, конкретного стеганоключа, используемого для выбора битов контейнера в стеганопреобразовании [1].

Основной целью стеганоанализа является моделирование стеганографических систем и их исследование для получения качественных и количественных оценок надежности использования стеганопреобразования, а также построение методов выявления скрываемой в контейнере информации, ее модификации или разрушения [2].

Для оценки стойкости некоторых стеганографических методов было использовано мсходное изображение-контейнер имеет размер 2281×3197 пикселей (7 292 357 пикселей всего). Для стеганографических преобразований были выбраны пространственные Pixel Value Difference (PVD) и Mid Position Value (MPV).

Метод PVD (Pixel Value Difference – разность значений пикселей) учитывает тот факт, что на гладких участках (где значение яркости меняется незначительно) изменение будет более заметно, нежели на участках, содержащих более значительные перепады яркости [3, 4].

Встраивание происходит следующим образом. Исходное изображение разбивается на блоки по 2 пикселя, а скрытые данные кодируются как разность значений внутри этих блоков. Также, требуется определить закон, по которому будут выбираться блоки для встраивания. Для каждого выбранного блока вычисляется модуль разности значений пикселей, чтобы определить диапазон допустимых значений. Чем больше различие яркости внутри блока, тем шире выбранный диапазон. Для удобства работы ширина диапазона устанавливается как степень двойки. Блоки, изменение которых может привести к выходу за пределы допустимых значений яркости пикселей (от 0 до 255), не используются.

Для извлечения данных изображение снова разбивается на блоки по 2 пикселя. В соответствии с предварительно известными правилами выбора блоков и их последовательностью обхода для каждого блока

вычисляется разница значений пикселей и определяется диапазон, в который она попадает. Затем происходит проверка на выход за пределы диапазона от 0 до 255: если при максимальной разнице, попадающей в диапазон, один из пикселей принимает значение больше 255 или меньше 0, то такой блок пропускается, так как он был отброшен аналогичной проверкой на этапе встраивания. Из оставшихся блоков извлекаются данные: количество бит, встроенных в блок, определяется по ширине диапазона и извлекается, начиная с наименее значимого.

Метод MPV (Mid Position Value – значение средней позиции) основан на изменении значения пикселя, который находится в середине определенного блока пикселей. В первом этапе на выбранный контейнер воздействует преобразование Арнольда, что приводит к перемешиванию битов данных и нарушению обычной ориентации пикселей. Затем применяется техника среднего значения позиции для встраивания битов данных из секретного изображения в перемешанный контейнер. После, к полученному изображению применяется обратное преобразование Арнольда [5].

При условии, что метод PVD внедряет 1 бит на 2 пикселя, метод MPV внедряет 1 бит на блок 2×2 пикселей относительная стеганографическая емкость исходного изображения-контейнера представлена в таблице. В контейнер было внедрено сообщения размером 56 бит, 504 бит, 5000 бит с помощью различных стеганографических методов. На полученные в результате преобразования стегоконтейнеры был проведен ряд атак: RS, SPA, $\chi 2$.

Метод RS (Regular-Singular) использует анализ пикселей изображения-контейнера, основанный на оценке регулярности групп пикселей. Суть метода состоит в следующем. Все изображение разбивается на группы по n пикселов G(x, x2, …, xn), где n четно, например по 2 пиксела, находящихся рядом по горизонтали. Для группы пикселов определяется функция регулярности или «гладкости» f(G), в качестве такой функции можно выбрать, например, дисперсию значений внутри группы, либо просто сумму перепадов значений смежных пикселов.

Метод SPA (Sample Pair Analysis) анализа основан на статистических отношениях между парами соседних пикселей изображений. SPA анализирует отношения между яркостными значениями соседних пикселей в изображении.

На основе статистических данных о распределении пиксельных значений метод выявляет аномальные шаблоны, которые могут свидетельствовать о наличии скрытой информации.

Идея атаки $\chi 2$ заключается в поиске этих близких значений и под-

счете вероятности встраивания на основе того, как близко располагаются значения частот четных и нечетных элементов анализируемого контейнера.

Таблица – Результат проведения исследования

Размер сообщения	Метод стеганографического преобразования	Относительная стеганографическая емкость			
		исходного стеганоконтенейра	при RS-атаке	при SPA - атаке	при атаке χ^2
56	PVD	$0{,}14 \cdot 10^{-4}$	0,0257	0,0347	0,3020
	MPV	$0{,}31 \cdot 10^{-4}$	0,0257	0,0347	0,3019
504	PVD	$1{,}38 \cdot 10^{-4}$	0,0258	0,0347	0,3024
	MPV	$2{,}76 \cdot 10^{-4}$	0,0259	0,0347	0,3024
5000	PVD	$13{,}71 \cdot 10^{-4}$	0,0263	0,0350	0,3044
	MPV	$27{,}43 \cdot 10^{-4}$	0,0263	0,0351	0,3044
Исходное сообщение			0,0257	0,0346	0,3019

После проведенных исследований, можно сделать вывод, что все рассмотренные атаки не смогли обнаружить сообщение (или его размер) в стегоконтейнере, так как, результат проведения атаки на стегоконтейнер очень близок к результату атаки на исходный (незаполненный) контейнер.

Таким образом методы PVD и MPV имеют высокую степень устойчивости к методам стегоанализа RS, SPA, $\chi 2$.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский [и др.]. – М.: Вузовская книга, 2009. – 220 с.

3. Wu D. C., Tsai W. H. A steganographic method for images by pixel-value differencing //Pattern recognition letters. – 2003. – Т. 24. – №. 9-10. – С. 1613-1626.

4. Zhang X., Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security // Pattern Recognition Letters. – 2004. – Т. 25. – №. 3. – С. 331-339.

5. Mukherjee S., Roy S., Sanyal G. Image steganography using mid position value technique //Procedia computer science. – 2018. – Т. 132. – С. 461-468.