6. Монарев В. А. Сдвиговой метод стегоанализа // Вестник СибГУТИ. 2012. № 4. С. 62–68.
7. <http://bows2.ec-lille.fr/> — The 2nd BOWS Contest (Break Our Watermarking System). 2007.

УДК 621.391.037.372

ОПРЕДЕЛЕНИЕ РАЗМЕРА СТЕГАНОГРАФИЧЕСКОГО СООБЩЕНИЯ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ БИНАРНОГО СТЕГОАНАЛИТИЧЕСКОГО КЛАССИФИКАТОРА

Е. В. Разинков, А. Н. Альмеев

Работа посвящена количественному стегоанализу — определению размера сообщения, встроенного в стеганографический контейнер. Предложен подход к определению размера скрытого сообщения с помощью бинарного стегоаналитического классификатора, приведена формула вычисления математического ожидания ошибки стегоаналитика. Задача определения оптимальной стратегии стегоаналитика сформулирована в виде задачи минимизации.

Ключевые слова: *количественный стегоанализ, бинарная классификация.*

Помимо задачи обнаружения скрытой информации, одна из актуальных задач, стоящих перед стегоаналитиком, — оценка размера скрытого стеганографического сообщения. Атаки, направленные на определение размера скрытого сообщения, называются количественными. Наилучшие на сегодняшний день методы обнаружения скрытой информации основаны на использовании бинарных универсальных классификаторов [1]. Современные количественные стегоаналитические атаки основываются на модификации этих методов [2].

Интерес представляет непосредственное применение бинарных стегоаналитических классификаторов для оценки размера скрытого сообщения. Разработка метода такого применения бинарного классификатора без модификации и исследование его свойств значительно упростили бы использование новых результатов, получаемых в области бинарной стегоаналитической классификации, в количественном стегоанализе.

Через C обозначим множество цифровых объектов, будем считать, что стегоаналитик располагает бинарным классификатором

$$Detect : C \rightarrow \{0, 1\},$$

для каждого цифрового объекта $c \in C$ возвращающего 0, если объект классифицирован как неизменённый контейнер, или 1, если объект классифицирован как стего.

Задача состоит в построении на основе имеющегося бинарного классификатора количественной стегоаналитической атаки

$$Estimate : C \rightarrow [0; 1],$$

возвращающей относительный размер скрытого сообщения, встроенного в цифровой объект $c \in C$, — отношение количества изменённых коэффициентов к общему количеству коэффициентов, доступных для изменения.

Бинарный стегоаналитический классификатор может быть использован для определения размера сообщения в случае, когда стегоаналитик располагает некоторым множеством цифровых объектов, в которые были встроены скрытые сообщения одного размера. Возникновение такой ситуации на практике кажется маловероятным, но

стегоаналитик может создать подобные условия при наличии лишь одного цифрового изображения высокого разрешения.

Пусть в цифровое изображение размера n встроено сообщение относительного размера $\theta \in [0; 1]$. Стегоаналитик разрезает перехваченное цифровое изображение на k частей и подаёт каждую из них на вход бинарному классификатору как отдельное изображение. Естественно предположить, что внесённые скрывающим преобразованием искажения равномерно распределены в пространственной области изображения и относительный размер сообщения, встроеного в каждую из k частей, также равен θ , размер же каждой части — n/k . Каждую из частей стегоаналитик подаёт на вход бинарному стегоаналитическому классификатору.

Наименьшие возможные вероятности ошибки первого рода α и ошибки второго рода β бинарного стегоаналитического классификатора удовлетворяют следующему неравенству [3]:

$$\alpha \log_2 \frac{\alpha}{1-\beta} + (1-\alpha) \log_2 \frac{1-\alpha}{\beta} \leq D_{KL}(P_0||P_1), \quad (1)$$

где P_0 — распределение контейнеров; P_1 — распределение стего; $D_{KL}(P_0||P_1)$ — относительная энтропия между этими распределениями. Будем считать, что стегоаналитик располагает наилучшим возможным бинарным классификатором, для которого неравенство (1) обращается в равенство.

В соответствии с [4], для небольших значений θ , которые характерны для использования стеганографии на практике, получаем

$$\alpha \log_2 \frac{\alpha}{1-\beta} + (1-\alpha) \log_2 \frac{1-\alpha}{\beta} = D_{KL}(P_0||P_1) \approx \frac{n}{2k} \theta^2 I(0),$$

где $I(0)$ — информация Фишера — коэффициент пропорциональности, характеризующий источник стеганографических объектов [5]. Из этого уравнения можем найти $p = 1 - \beta$ — вероятность того, что часть изображения будет классифицирована как стего.

Пусть m частей изображения были классифицированы как стегообъекты, тогда стегоаналитик оценивает p значением m/k , а относительный размер сообщения θ — значением

$$\theta' = \sqrt{\frac{2k}{nI(0)} \left(\alpha \log_2 \frac{\alpha k}{m} + (1-\alpha) \log_2 \frac{(1-\alpha)k}{k-m} \right)}.$$

Таким образом, можно вычислить математическое ожидание ошибки стегоаналитика для заданного размера изображения n , относительного размера секретного сообщения θ , коэффициента $I(0)$, вероятности ошибки первого рода α и стратегии стегоаналитика, заключающейся в выборе k — количества частей, на которые разрезается цифровое изображение, по следующей формуле:

$$M[\Delta\theta] = \sum_{m=0}^k \binom{k}{m} p^m (1-p)^{k-m} \left| \theta - \sqrt{\frac{2k}{nI(0)} \left(\alpha \log_2 \frac{\alpha k}{m} + (1-\alpha) \log_2 \frac{(1-\alpha)k}{k-m} \right)} \right|.$$

Задача нахождения оптимальной стратегии стегоаналитика сводится к выбору значения k , минимизирующего математическое ожидание ошибки:

$$M[\Delta\theta] \rightarrow \min.$$

Предложенный подход к использованию бинарных стегоаналитических классификаторов в количественном стегоанализе позволяет исследовать влияние свойств изображений, особенностей классификатора, размера изображения, размера скрытого сообщения и стратегии стегоаналитика на стойкость стеганографической системы к количественным атакам, вычислять оптимальную стратегию стегоаналитика в зависимости от этих факторов.

ЛИТЕРАТУРА

1. *Kodovsky J. and Fridrich J.* Steganalysis of JPEG images using rich models // Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIV. San Francisco, CA, January 22–26, 2012. V. 8303. P. 0A 1–13.
2. *Kodovsky J., Fridrich J.* Quantitative steganalysis using rich models // Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XV. San Francisco, CA, February 3–7, 2013. V. 8665. DOI: 10.1117/12.2001563.
3. *Cachin C.* An information-theoretic model for steganography // LNCS. 1998. V. 1525. P. 306–318.
4. *Ker A. et al.* Moving steganography and steganalysis from the laboratory into the real world // 1st Information Hiding and Multimedia Security Workshop. Montpellier, France, June 17–19, 2013. P. 45–58.
5. *Filler T. and Fridrich J.* Fisher information determines capacity of ε -secure steganography // LNCS. 2009. V. 5806. P. 31–47.