метода [2], влияние помех на эффективность распознавания скрытых сообщений [3]. Предлагаются различные методы ослабления этого влияния.

ЛИТЕРАТУРА

1. *Райхлин В. А., Вершинин И. С.* Моделирование процессов двумерно-ассоциативного маскирования распределенных точечных объектов картографии // Нелинейный мир. 2010. № 5. С. 288–296.
2. *Вершинин И. С.* Стойкость ассоциативной защиты распределенных объектов картографии // Нелинейный мир. 2011. № 12. С. 822–825.
3. *Вершинин И. С., Гибадуллин Р. Ф.* Изменение результатов распознавания на множестве замаскированных бинарных матриц при действии аддитивных помех // Вестник КГТУ им. А. Н. Туполева. 2012. № 4-1. С. 198–206.

УДК 003.26

НОВЫЙ ВЫСОКОТОЧНЫЙ СТЕГОАНАЛИЗ РАСТРОВЫХ ИЗОБРАЖЕНИЙ[1]

В. А. Монарев

Предложен новый подход для обнаружения информации в растровых изображениях. Предполагается, что для внедрения информации использовалась либо ±1-стеганография, либо LSB-замещение. Предлагается новый сценарий обнаружения информации, в котором наблюдателю известны пиксели изображения, куда производилось внедрение. Показано, что обнаружение информации возможно уже при 0,001 bpp (“bits per pixel”) внедрении.

Ключевые слова: *стегоанализ, стеганография, LSB-внедрение.*

Стегоанализ файлов изображений в форматах, не искажающих качество (`bmp`, `pgm`, `tiff` и др.), разделяется на два подхода: количественный (когда метод позволяет определить приблизительное количество внедрённой информации) и обычный (метод определяет факт наличия или отсутствия скрытой информации). К самым известным количественным методам относятся RS [1], simple pairs [2], WS [3], improved WS [4]. Все эти методы позволяют обнаружить скрытую информацию, если она была внедрена с помощью LSB-замещения. Недавно предложен новый количественный стегоанализ, который обнаруживает скрытую информацию в цветных изображениях эффективнее, чем ранее существовавшие методы [6]. Для обнаружения же ±1-стеганографии используется, как правило, обычный стегоанализ, который фактически производит классификацию изображений, разделяя их на два класса: пустые и непустые [5]. В случае LSB-внедрения возможно эффективно обнаружить до 0,1 bpp, и до 0,01 bpp — в случае LSB-замещения. Для классификации используются стандартные методы SVM и LDA.

В данной работе предполагается, что внедрение скрытой информации производится с помощью либо LSB-внедрения, либо ±1-стеганографии. Предполагается также, что известны пиксели, куда производилось внедрение, но неизвестны содержание и размер внедряемой информации, т. е. имеется устройство, с помощью которого производилось сокрытие информации (ключ для выбора случайных пикселей находится в устройстве). По заданному файлу необходимо определить, могла ли быть в него встроена информация с помощью данного устройства. Метод относится к количествен-

[1]Работа поддержана грантом РФФИ № 14-01-31484-мол_а.

ным методам. Из полученных экспериментальных результатов следует, что метод позволяет определять наличие информации, если внедрено более 0,001 bpp.

Пусть $X = \{x_1, \ldots, x_n\}$, где $x_i \in \{0, 1, \ldots, 255\}$, — пиксели исходного изображения. Обозначим через $\overline{S}(Y)$ вектор spam-характеристик, вычисленный для множества $Y \subset X$ (подробно см. [5]). Обозначим через Y_p случайное множество ($Y_p \subset X$), такое, что $|Y_p|/|X| = p$. Полагаем также, что обозначение Y_p предполагает не только выбор случайного подмножества заданного размера, но и внедрение скрытой информации с помощью ±1-стеганографии (или LSB-замещения). Обозначим через $D(\cdot\cdot)$ евклидову метрику; Z_p — множество ($Z_p \subset X$) тех пикселей, куда производилось бы внедрение при внедрении p бит на пиксель.

Алгоритм 1. Оценка количества внедрённой информации

1: Вычисляем $\overline{S}(X)$, $\overline{S}(Z_{0{,}001})$, $\overline{S}(Z_{0{,}0015})$, …, $\overline{S}(Z_{0{,}5})$.
2: Вычисляем по 10 векторов $\overline{S}(Y_p^i)$, $i = 0, \ldots, 9$, для каждого значения p = 0,001, 0,0015, …, 0,5.
3: Находим

$$\arg\min_p = \left\{ \frac{D(\overline{S}(X), \overline{S}(Z_p))}{D\left(\overline{S}(X), \sum_{i=0}^{9} \overline{S}(Y_p^i)/10\right)} \right\}$$

4: Полагаем, что np равно количеству внедрённых бит информации.

Поясним принцип работы алгоритма. Хорошо известно, что spam-характеристики очень чувствительны к ±1-стеганографии, и если предположить, что мы знаем, куда информация была внедрена, то легко понять, что spam-характеристики этих пикселей отличаются от spam-характеристик случайно выбранных пикселей (Y_p), если параметр p отличается от искомого параметра (количества внедрённой информации).

Для проверки эффективности метода были взяты 1000 черно-белых изображений с сайта [7]. Рассмотрены три варианта внедрения: 0,001 bpp, 0,005 bpp и 0,01 bpp (±1-стеганография и LSB-замещение). Для каждого из случаев подсчитана минимальная средняя ошибка. Ошибки равны 12, 6 и 4 % соответственно для LSB-замещения и 7, 4 и 3 % для ±1-стеганографии. Таким образом, можно сделать вывод, что метод эффективно обнаруживает скрытую информацию для внедрения 0,001 bpp независимо от метода внедрения.

ЛИТЕРАТУРА

1. *Fridrich J., Du R., and Long M.* Steganalysis of LSB encoding in color images // Proc. ICME 2000, New York City, New York, 2000. V. 3. P. 1279–1282.
2. *Dumitrescu S., Wu X., and Wang Z.* Detection of LSB steganography via sample pair analysis // LNCS. 2002. V. 2578. P. 355–372.
3. *Fridrich J. and Goljan M.* On estimation of secret message length in LSB steganography in spatial domain // Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. San Jose, California, 2004. V. 5306. P. 23–34.
4. *Ker A. and Böhme R.* Revisiting weighted stego-image steganalysis // Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. San Jose, 2008. V. 6819. Doi: 10.1117/12.766820.
5. *Pevny T., Bas P., and Fridrich J.* Steganalysis by subtractive pixel adjacency matrix // IEEE Trans. Info. Forensics and Security. 2010. V. 5(2). P. 215–224.

6. *Монарев В. А.* Сдвиговый 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

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

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

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

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