УДК 681.3

ПРИНЦИПЫ АССОЦИАТИВНОЙ СТЕГАНОГРАФИИ

И. С. Вершинин

Рассматривается стеганографический метод защиты данных с использованием аппарата маскирования, применяемого при двумерно-ассоциативной обработке стилизованных бинарных изображений.

Ключевые слова: *ассоциативная стеганография, двумерно-ассоциативное маскирование, защита картографической информации.*

Защита данных с использованием аппарата маскирования, применяемого при двумерно-ассоциативной обработке стилизованных бинарных изображений, относится к области стеганографии. Двумерно-ассоциативное маскирование следует рассматривать как частный случай т. н. трафаретного способа классической стеганографии.

Применительно к картографии, развиваемый подход стегозащиты обладает свойством безусловной стойкости (совершенной секретности по К. Шеннону). Выполнение критерия Шеннона означает, что в каждом сокрытом сообщении при полном переборе ключей может быть распознано любое из возможных сообщений. Поэтому метод, безусловно, стоек независимо от вычислительной сложности полного перебора ключей.

Рассматриваемый метод относится к классу вероятностных способов защиты. Случайность вносится использованием специальных механизмов пространственной кластеризации объектов, маскирования их бинарных представлений и рандомизации. Имена и координаты объектов кодируются в цифровом виде. Разряды кодов, представленные в алфавите почтовых индексов, рассматриваются как бинарные изображения. Над ними выполняется специальная процедура маскирования. Случайно сгенерированный набор масок служит секретным ключом.

Предметом защиты в данном случае является набор тематических карт-кластеров как случайно формируемых по карте таблиц в терминах «коды объектов — коды координат». Защищённые карты образуют «верхние слои» геоинформационных систем.

Суть рассматриваемого подхода заключается в следующем. Исходное бинарное изображение подвергается избирательному воздействию стохастических помех (рандомизации). При этом не затрагиваемые помехами части объектов выбираются случайным образом с выполнением некоторого условия. Но их точное знание (что является ключом) позволяет правильно идентифицировать объекты в целом методом двумерно-ассоциативного поиска.

В рассматриваемом случае кодовые знаки (цифровые символы) представляются в виде двоичных матриц определённых размеров. Каждый символ развёртывается в цепочку соответствующей длины. Метод предусматривает внедрение псевдослучайного процесса в передаваемое сообщение, оставляя истинным ограниченное подмножество бит в каждом знаке со случайным распределением этого подмножества по битовой сетке эталона.

В данном случае ключом является набор масок всевозможных цифр. Размер ключа определяется числом цифр, размерами матриц и не зависит от объёма сообщения. Наличие гаммы никак не сказывается на факте санкционированного распознавания, но создаёт непреодолимую преграду для противника.

Рассматриваются базовый алгоритм маскирования и его свойства [1], достижимая стойкость защиты объектов картографии развиваемым методом при действии разного рода атак, связь размеров ключа со стойкостью и вычислительной сложностью

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.