ЗАЩИТА ЦЕЛОСТНОСТИ ДАННЫХ ЭЛЕКТРОННЫХ КАРТ СТЕГАНОГРАФИЧЕСКИМ МЕТОДОМ

Блинова Е. А., Урбанович П. П.

Белорусский государственный технологический университет,
Минск, Беларусь, e-mail: eugenia.blinova@gmail.com

В настоящее время актуальной является задача защиты файлов электронных карт (ЭК). Одно из ее решений основано на встраивании (осаждении) различных цифровых меток на основе стеганографии [1]. Это не только обеспечивает целостность пространственных данных и их атрибутов, но и позволяет подтвердить авторство.

ЭК – набор компьютерных файлов, содержащих пространственные данные в векторном формате, визуализируемые на основе правил, содержащихся в этих файлах. Изготовление ЭК требует значительных затрат, таких, например, как оцифровка растровых карт и их уточнение на местности. Координаты объектов карт могут быть описаны языком разметки WKT (Well Known Text), который является подмножеством языка разметки XML. Описание WKT допускает использование объектов типа Point, LineString, Polygon, MultiPolygon и других типов объектов, в том числе – наборов объектов определенного типа. Формат описания путей позволяет осаждать скрытую информацию размещением дополнительных элементов в пространственных данных [2].

Стеганографический алгоритм внедрения дополнительных вершин состоит в следующем. Определяется количество полиномов в файле пространственных данных, их вид и количество вершин, а также количество точек, осаждаемых в первом полиноме файла данных. Это происходит следующим образом. Вычисляется значение хеш-функции от объединения следующих значений: количество строк, значение атрибутивных столбцов в первом полиноме, тип пространственных данных, стартовая точка, площадь пространственной фигуры и каких-либо дополнительных данных, которые могут идентифицировать автора ЭК, например, наименование организации, отметка времени, тип хеш-функции и пр. Значение хеш-функции считывается посимвольно и разделяется на пары значений [m, n]. На каждом нечетном ребре пространственной фигуры устанавливается дополнительная точка в отношении m к n. Для остальных полиномов подсчет значений хеш-функции вычисляется с учетом объединения значений атрибутивных столбцов текущего полинома, значения пространственного столбца предыдущего полинома с уже осажденными данными. Таким образом, при осаждении скрытой информации полиномы связаны друг с другом, что позволяет исключить удаление объектов, а также контролировать правильность и целостность значений атрибутивных столбцов пространственных данных.

Библиографические ссылки

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации/ П.П. Урбанович. – Минск: БГТУ.– 2016. – 219 с.

2. Блинова, Е.А. Применение стеганографических методов для защиты данных электронных карт Е.А. Блинова, П.П. Урбанович // Управление информационными ресурсами: материалы XIV междунар. науч.-практ. конф., Минск, 20 дек. 2017 г. / Акад. упр. при Президенте Респ. Беларусь; под общ. ред. М.Г. Жилинского; редкол.: Д.В. Мазарчук (отв. ред.) [и др.]. – Минск, 2017. – С. 154-155.

This document has been edited with Infix PDF Editor - free for non-commercial use.
To remove this notice, visit: www.iceni.com/unlock.htm