Алгоритм внедрения ЦВЗ основанный на дублировании значений точек внутри объектов картографического слоя

Недостатки алгоритма основанного на перестановке объектов

1. Низкая устойчивость к атакам путем вставки или удаления объектов слоя
2. Основан на алгоритме, использующем коллизии хэш-функции для поиска индексов ЦВЗ. Это требует подбора констант, которые также должны быть использованы при извлечении водяного знака. Также в силу того что применяется вычисление коллизий хэш-функции - трудно предсказываются случаи когда на какой-то конкретный индекс не будет не единой коллизии при заданном наборе констант и выбранной хэш-функции.

Внедрение ЦВЗ через алгоритм дублирования точек

1. ЦВЗ **W** является двоичным представлением десятичного числа.
2. Среди всех объектов картографического слоя находим объект с наибольшим числом точек. Число точек в нем необходимо запомнить как значение при котором будет изменяться алгоритм вычисления остатка - **MAX**.
3. Период дублирования точек в объекте вычисляется как 1) если **W_10 > count_points(Obj)**, то **W_10 mod MAX**, 2) если **W_10 <= MAX**, то **count_points(Obj) mod W_10**
4. После обработки всех объектов объект карты сохраняется и готов к передаче.
5. Дополнительно для WM перед внедрением можно применить алгоритм Арнольда.

Извлечение ЦВЗ

1. Алгоритм извлечения не требует знания никаких значений кроме ключа в случае применении алгоритма Арнольда
2. Для каждого объекта вычисляется период дублирования в нем точек. Зная число дублированных значений находим число точек в объекте перед дублированием.
3. Таким образом для каждого объекта будет найдена пара (loopPeriod, sizeBeforeLooping)
4. Сперва рассматривается случай когда искомое значение **W** было меньше или равно **MAX**. В этом случае задача сводится к решению системы **B_{i} mod x ≡ A_{i}**, в случае когда **W** превышало **MAX**, к решению системы **x mod B_{i} ≡ A_{i}**. **B_{i}** - sizeBeforeLooping, **A_{i}** - loopPeriod.
5. Для решения задачи в первом случае достаточно вычисления НОД, во втором случае применяется КТО.

Преимущества

1. Для решения любой из двух систем **в идеальном случае**, т.е. если сравнения не эквивалентны достаточно двух сравнений, следовательно алгоритм позволяет удалять объекты в большем количестве чем способен алгоритм перестановки объектов местами. Поскольку в исходном алгоритме минимальное число объектов в карте должно быть не меньше числа битов ЦВЗ. Здесь ЦВЗ может принимать любое сколь угодно большое значение, которое можно найти решая систему из двух сравнений.

Преимущества

2. Алгоритм полностью устойчив к атакам путем добавления объектов. Поскольку в добавленных объектах отсутствуют дублирования точек они не будут учитываться при решении систем сравнений, следовательно никак не повлияет на результат.

Преимущества

3. Алгоритм не использует коллизий, следовательно отсутствует вероятность, что тот или иной бит искомого ЦВЗ будет не вычислен.

Недостатки

1. Значение ЦВЗ вычисляется либо корректно, либо нет. Отсутствует возможность частичного извлечения водяного знака.

   Например, в случае добавления объекта с некорректным периодом дублирования для его числа точек.

   Рассматривая вариант решения ни одной системы, а множества систем, сравнения в которые будут попадать случайно выбранным образом из общего числа, можно использовать схему голосования большинства для выбора значения ЦВЗ.

Недостатки

1. Картографический слой должен содержать хотя бы пару объектов НОД для числа точек которых = 1. Требование теоремы КТО. Модули системы должны быть взаимно попарно простыми.