Нанесение водяных знаков на программное обеспечение

Смирнов Денис, 344 гр.

Руководитель: ст. пр. Баклановский М.В.

Консультант: Сибиряков А.Е.

2018

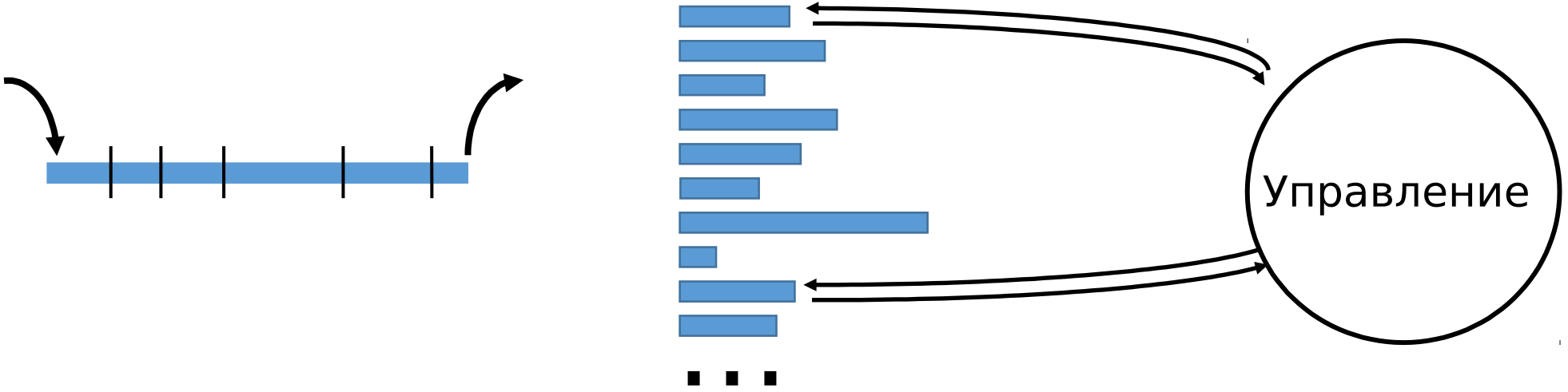
Задачи

- Сделать обзор техник нанесения водяных знаков на ПО
- Сделать обзор уже существующих решений
- Провести декомпозицию ЦВЗ на различные виды и спроектировать их реализацию
- Разобраться в МАКе и реализовать его простую версию под Windows
- Реализовать прототип ПО для нанесения ЦВЗ

Водяные знаки для ПО бывают

- Статические
  - Внедренные в данные приложения
  - Внедренные в код
- Динамические
  - Пасхальные яйца
  - Использующие трассу
  - Основанные на динамически созданных структурах данных

MAK



Идеи цвз

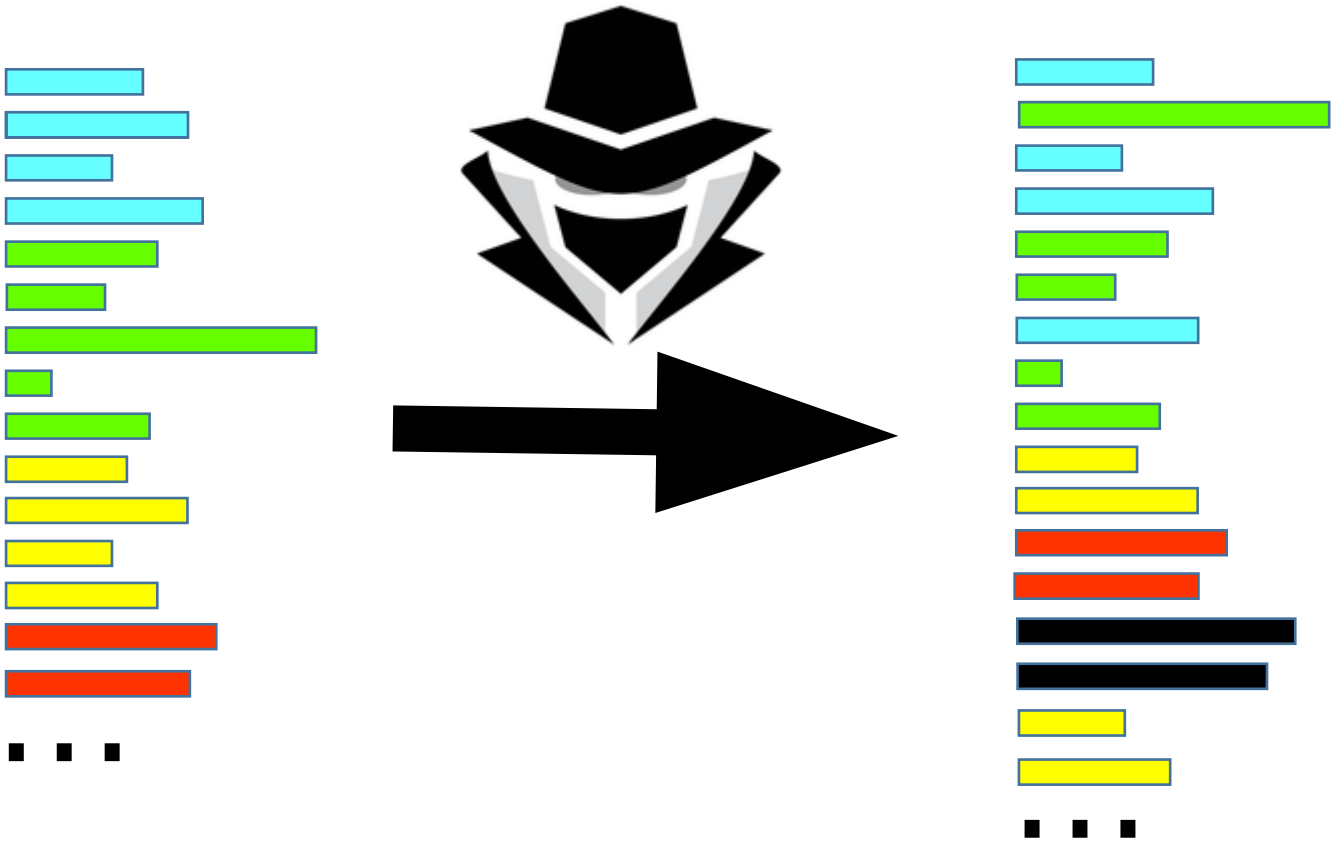
- Хорошо заметный цвз для отпугивания злоумышленников
- Цвз заведомо небольшого объема, предназначенный исключительно для цифровой подписи автора
- Цвз, обладающий большой информационной емкостью, для сохранения истории развития проекта
- Хрупкий цвз, идентифицирующий попытку взлома
- Хрупкий цвз, “взрывающий бомбу” в случае взлома

Идеи реализаций

- Связные списки
- Решётка Кардано
- Цепочка условных переходов
- Лишние опкоды и “дырки” в инструкциях

Реализации состоят из большого числа фрагментов

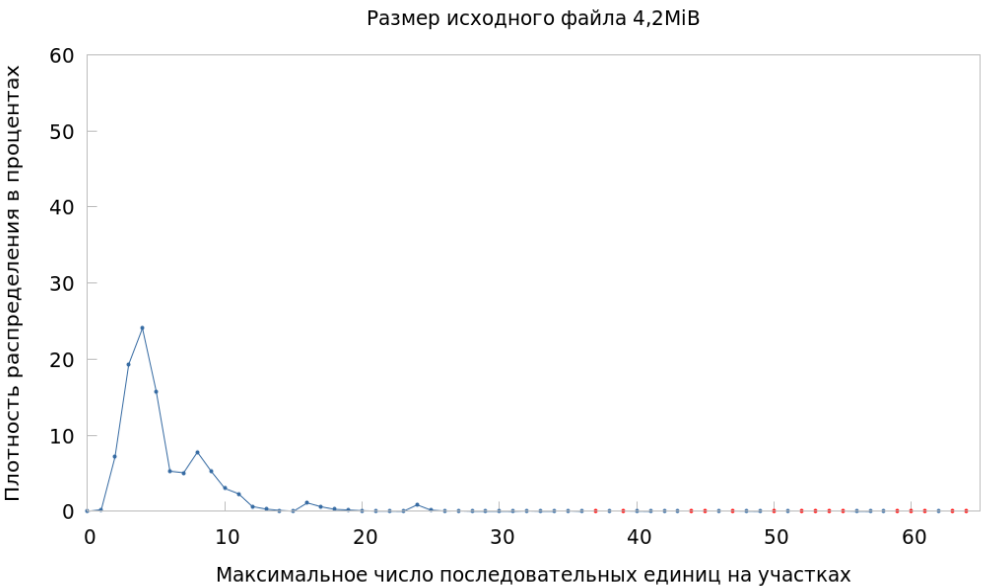
Каркасный водяной знак



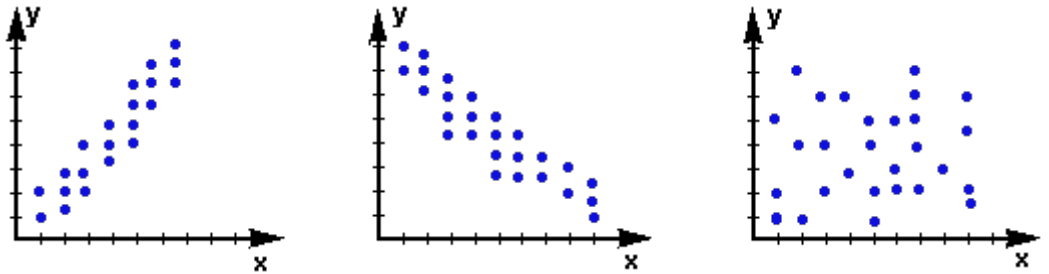
Идея решения

- Разобьем весь файл на части
- Введем набор случайных величин, порождаемых различными битовыми паттернами, и посчитаем их на каждой из этих частей
- Если каждая часть может быть однозначно идентифицирована по кортежу из распределений, то проблема решена
- Изменим каждую часть так, чтобы это условие выполнялось

Распределение макс. числа последовательных единиц и нулей



Корреляция



Слева направо:

- положительная корреляция
- отрицательная корреляция
- корреляция отсутствует

$$\mathbf{r}_{XY} = \frac{\mathbf{cov}_{XY}}{\sigma_X \sigma_Y} = \frac{\sum (X - \bar{X})(Y - \bar{Y})}{\sqrt{\sum (X - \bar{X})^2 \sum (Y - \bar{Y})^2}}.$$

$\overline{X} = \frac{1}{n} \sum_{t=1}^{n} X_t \quad \overline{Y} = \frac{1}{n} \sum_{t=1}^{n} Y_t$ — среднее значение выборок

Результаты

Главные результаты

- Сделан обзор техник нанесения водяных знаков на ПО
- Сделан обзор уже существующих решений
- Произведена декомпозиция ЦВЗ на различные виды и спроектированы конкретные реализации
- Реализована упрощенная версия МАКа под Windows
- Написана первая спецификация и реализован прототип каркасного ЦВЗ

* Дополнительные результаты

- Проведено исследование внутренней структуры секции кода исполняемых файлов
- Получен инструмент сравнения исполняемых файлов друг с другом