Адаптивные методы стегоанализа

30 декабря 2015 г.

Коллектив: Дуплищев И.К.

Эффект от использования кластера в достижении целей работы: Возможность обработки больших массивов данных (~40Гб памяти на ядро)

1 Введение

Сегодня мы живём в мире информационных технологий. Информация стала неотъемлемой частью нашей жизни. С появлением современных средств копирования и тиражирования данных остро встаёт проблема сохранения авторских прав и защита от несанкционированного тиражирования. Соответственно возникает потребность в шифровании данных, скрытой их передаче и во внедрении специальных меток в электронные представления данных для однозначной идентификации владельца.

Способы и методы скрытия секретных сообщений известны с давних времён. Вместе с их появлением возникла и наука, изучающая данную сферу человеческой деятельности. Она получила название стеганография. Это слово происходит от греческих слов «steganos», что означает секрет или тайна, и «graphy» – запись. Буквально – «тайнопись». Исторически это направление появилось первым, но затем во многом было вытеснено криптографией. В отличие от криптографии, где неприятель точно может определить, является ли передаваемое сообщение зашифрованным текстом или нет, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания. Таким образом, под словом «стеганография» принято понимать метод передачи сообщения, который скрывает факт передачи сообщения. Отметим, что сегодня стеганография и криптография существуют в тандеме, взаимно дополняя друг друга. Стеганографические методы позволяют уменьшить вероятность выявления факта передачи некоторого сообщения. Криптографические методы – увеличить степень защищённости встроенного сообщения [1]

Сегодня, благодаря научным достижениям в области компьютерной техники и технологий появлению новых способов передачи информации, появились новые стеганографические методы, в основе которых лежат особенности представления информации в оцифрованном виде. К примеру, существуют методы, которые позволяют скрывать сообщения в компьютерных файлах (контейнерах) за счёт учёта естественных неточностей устройств оцифровки и избыточности аналогового видео или аудиосигнала. Таким образом, можно говорить о новом витке развития – эре компьютерной стеганографии.

Наряду с развитием стеганографии идёт бурное развитие стегоанализа. Основной задачей стегоанализа является определение факта наличия скрытого сообщения в предположительном контейнере (речи, видео, изображении). Решить эту задачу возможно путём изучения статистических свойств сигнала. Например, распределение младших битов сигналов имеет, как правило, шумовой характер (ошибки квантования). Они несут наименьшее количество информации о сигнале и могут использоваться для внедрения скрытого сообщения. При этом, возможно, изменится их статистика, что и послужит для аналитика признаком наличия скрытого сообщения. [2]

Целью данной работы является исследование различных методов стегоанализа, основанных на классификации контейнеров (использовались изображения) и определения факта внедрения скрытой информации.

Изначально делается допущение, что известен алгоритм стеганографии и объем скрытой информации для дальнейшего анализа.

Задачи на 3-й семестр магистратуры:

- Исследовать различные варианты преобразования изображений для улучшения качества стегоанализа
- Сформировать базы изображений с преобразованиями
- Произвести тестирование на полученной базе

2 Исследуемые алгоритмы стеганографии

Как известно, любой файл на жёстком диске представляется последовательностью байт, такое представление удобно при рассмотрении методов включения инородных данных внутрь контейнера, так как любая программа, реализующая данную функцию, переходит именно к такому представлению. Помимо этого для скрытия данных могут быть использованы и так называемые служебные заголовки файлов.

В качестве алгоритмов стеганографии использовались:

- LSB (*Least Significant Bits*)
- HUGO (*Highly Undetectable steGO*) [3]
- WOW (*Wavelet Obtained Weights*) [4]
- UNIWARD (*universal wavelet relative distortion*) [5]

2.1 LSB

Суть метода замена наименее значащего бита (Least Significant Bits - LSB) заключается в сокрытии информации путем изменения последних битов изображения, кодирующих цвет на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.

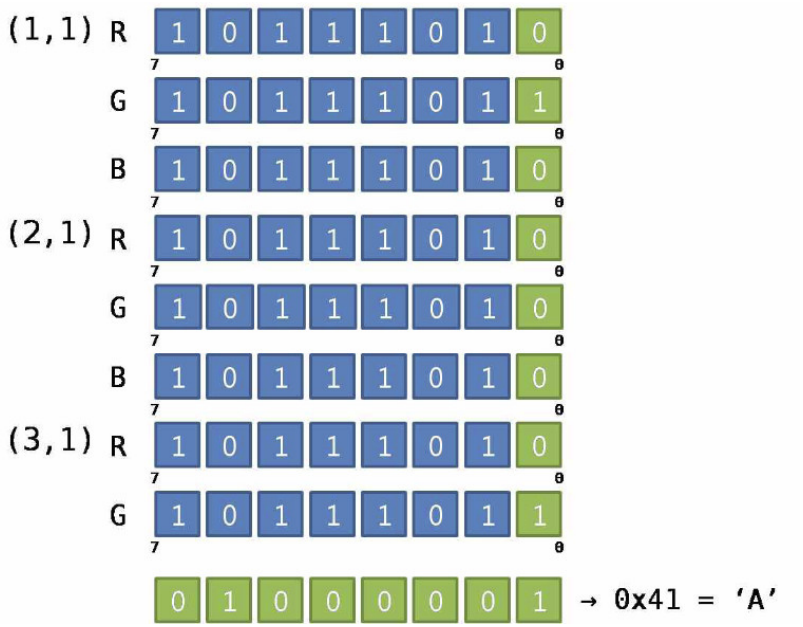

Рис. 1: Пример LSB

2.2 HUGO

HUGO (*Highly Undetectable steGO*) – это стеганографическая система, которая оптимизирована для противодействия обнаружению против конкретного алгоритма стегоанализа SPAM [6]. Как показали результаты исследования авторов статьи [7] , такая стеганографическая система является так же сложной для обнаружения для некоторых других методов стегоанализа. Основная идея HUGO заключается в том [8] , что в процессе вложения, каждый пиксель изменяется с вероятностью обратно пропорциональной его «вкладу» в суммарное искажение изображения, который определяется стоимостью изменения пикселя.

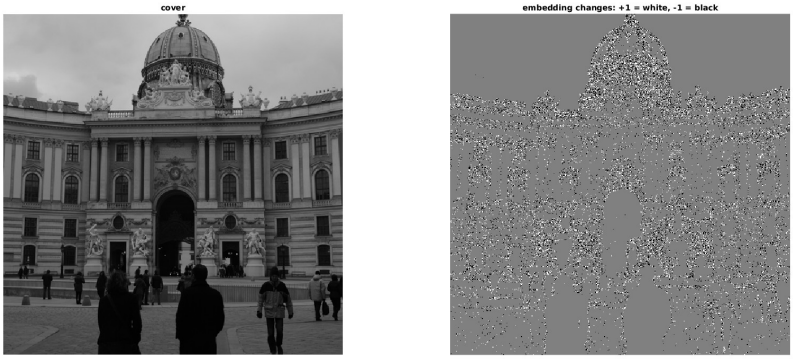

Рис. 2: Пример HUGO

2.3 WOW

WOW (*Wavelet Obtained Weights*) - стеганографическая система, направленная на более эффективное скрытие информации в изображениях. Внедрение информации происходит в специально определенные места. После внедрения происходит небольшое изменение окресности точки изображения для большей скрытности алгоритма.

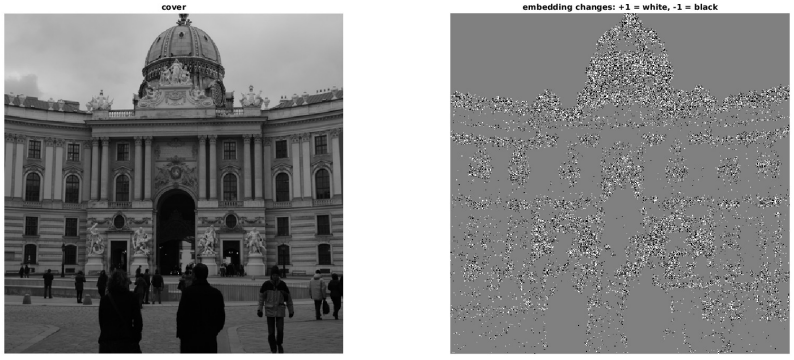

Рис. 3: Пример WOW

2.4 UNIWARD

UNIWARD (*universal wavelet relative distortion*) - стеганографическая система, основанная на наработках HUGO и WOW, использующая наиболее зашумлённые места в изображении для улучшения скрытности алгоритма.

Рис. 4: Пример UNIWARD

3 Классификация изображений для стегоанализа

Используемые алгоритмы:

- *SVM*
- *Extra Trees*
- *Decision Tree*
- *Random Forest*
- *SGC*
- *Ada Boost*

4 Извлечение метаинформации

Необходимым шагом для обработки изображений для задачи стегоанализа является извлечение неких характеристик, позволяющих зафиксировать факт изменения изображения. Такие методы давно известны и называются «feature extractor». Были рассмотрены 2 вида извлечения информации: SPAM [6] и SRM [9]

Визуальное сравнение характеристик изображений:

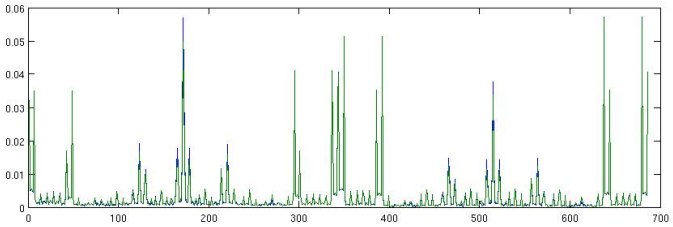

Рис. 5: SPAM

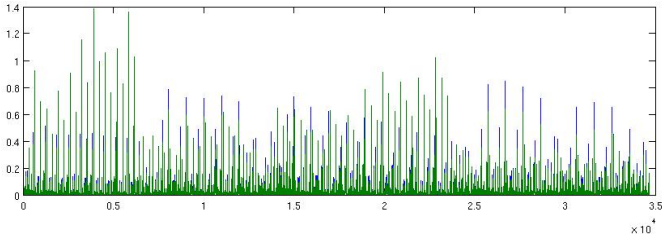

Рис. 6: SRM

Для проведения экспериментов был взят метод SRM, т.к. он содержит в себе намного больше характеристик и проявил лучшую эффективность в стегоанализе.

5 Преобразование изображений

Для улучшения эффективности стегоанализа с использованием классификации было решено преобразовывать изображения. Рассматривались следующие варианты:

- Вырезание частей
- Изменение размера
- Наложение маски

Для исследований был выбран последний вариант как наиболее универсальный. По сути наложение маски - процесс удаления несущественных частей изображения. После такого преобразования увеличивается вероятность попадания в пиксель стегоконтейнера.

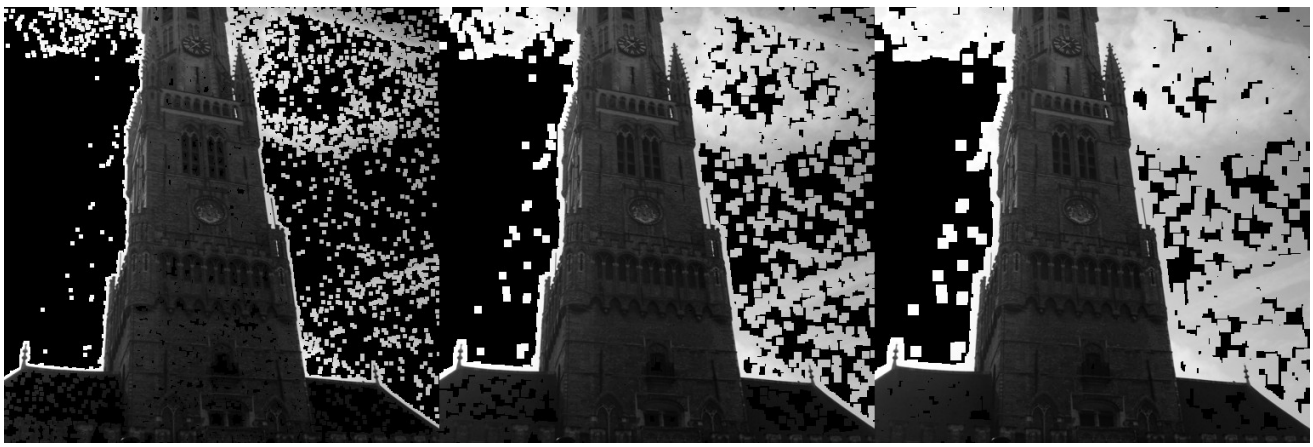

Рис. 7: Наложение маски на изображение с разным размером

Алгоритм преобразования изображения:

1. Используя алгоритмы стеганографии внедрить в изображение информацию
2. Сравнить с оригиналом, получить набор измененных пикселей
3. Сгенерировать маску в зависимости от размеров вырезаемой области

Данная схема является наиболее простой. Более эффективный алгоритм базируется не на измененных байтах изображения, а на матрице вероятностей внедрения для изображения, которая извлекается во время работы стеганографических алгоритмов. Эта схема на текущий момент не реализована.

6 Тестирование

Тестирование различных классификаторов производилось с использованием базы изображений BOWS2. Размер выборки был ограничен в 4000 изображений из-за аппаратных ограничений. Первый тест показывает основан на изображениях без наложения маски. Далее можно проследить как улучшается точность при отбрасывании ненужных данных.

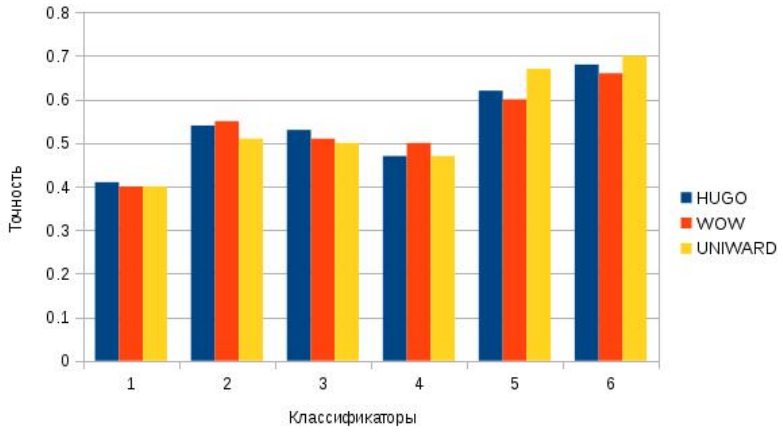

Рис. 8: Тестирование классификаторов на различных стеганографических алгоритмах. Классификаторы: 1- Extra Trees; 2- Decision Tree; 3- Random Forest; 4- SGC; 5-Ada Boost; 6- SVM

Для упрощения восприятия данных далее будет приведены усредненные графики:

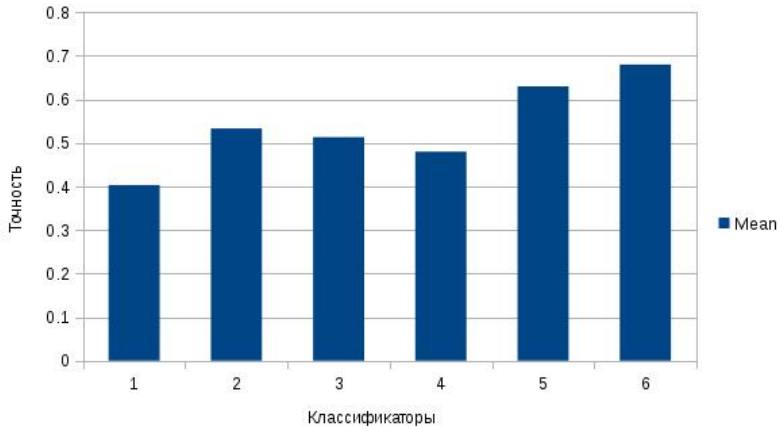

Рис. 9: Тестирование классификаторов на различных стеганографических алгоритмах. Классификаторы: 1- Extra Trees; 2- Decision Tree; 3- Random Forest; 4- SGC; 5-Ada Boost; 6- SVM

Большая часть классификаторов показывает близкий к 0.5 результат, что недопустимо. Следующим этапом будет наложение квадратной маски с длиной стороны 10:

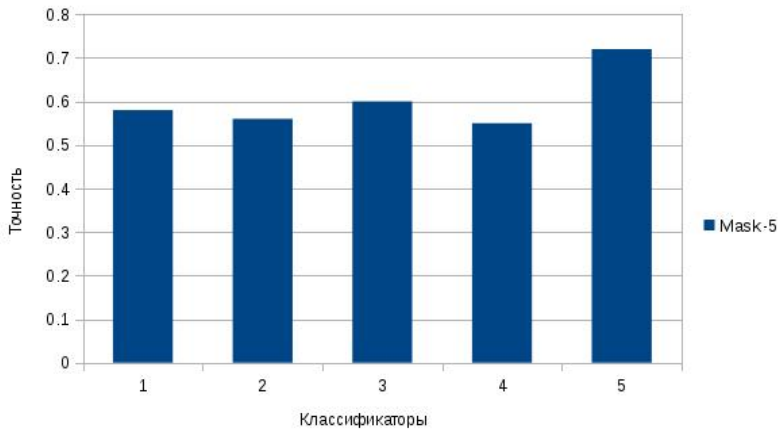

Рис. 10: Тестирование классификаторов на различных стеганографических алгоритмах. Классификаторы: 1- Extra Trees; 2- Decision Tree; 3- Random Forest; 4- SGC; 5- SVM

По техническим причинам Ada boost не попал в сравнения преобразованных изображений. Точность была повышена на всех запусках. Далее маска с длиной стороны 6:

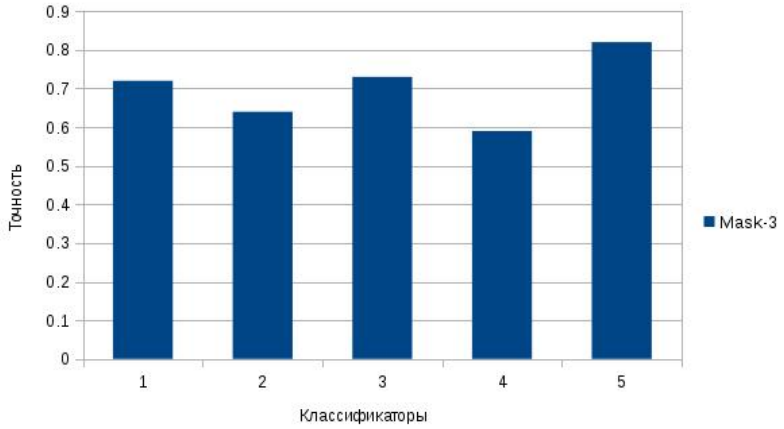

Рис. 11: Тестирование классификаторов на различных стеганографических алгоритмах. Классификаторы: 1- Extra Trees; 2- Decision Tree; 3- Random Forest; 4- SGC; 5- SVM

Общее сравнение точности:

	Оригинал	Маска-10	Маска-6
Extra Trees	0.4	0.58	0.72
Decision Tree	0.53	0.56	0.64
Random Forest	0.51	0.6	0.73
SGC	0.48	0.55	0.59
SVM	0.68	0.72	0.82

7 Заключение

В процессе работы был найден наиболее эффективный вариант преобразования изображений для повышения точности работы классификаторов для стегоанализа. Уменьшение областей с ненужной для анализа информации заметно улучшает работу алгоритма.

Классификатор SVM оказался наиболее эффективным решением.

В следующем семестре запланировано:

- Реализация более эффективной маски для изображений
- Анализ вектора характеристик изображения (SRM) для повышения эффективности стегоанализа
- Тестирование с максимальным количеством изображений (20000)

Список литературы

[1] В. С. Барсуков , А. П. Романцов. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века.

[2] В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. Цифровая стеганография. – Солон - Пресс, 2002. – 272 с.

[3] T. Filler, J. Fridrich, Gibbs Construction in Steganography, IEEE Transactions on Information Forensics and Security, December 2010

[4] V. Holub, J. Fridrich, Designing Steganographic Distortion Using Directional Filters, IEEE Workshop on Information Forensic and Security, Tenerife, Canary Islands, December 2–5, 2012

[5] V. Holub, J. Fridrich, T. Denemark, Universal Distortion Function for Steganography in an Arbitrary Domain, EURASIP Journal on Information Security, (Section:SI: Revised Selected Papers of ACM IH and MMS 2013), 2014

[6] T. Pevny, Steganalysis by subtractive pixel adjacency matrix / T. Pevny, P. Bas, J. Fridrich // IEEE Transactions on Information Forensics and Security, June 2010. – 5(2). – P. 215 – 224.

[7] T. Pevny, Using high - dimensional image models to perform highly undetectable steganography // T. Pevny, T. Filler, P. Bas // Information Hiding, 12th International Workshop. – 2010. – LNCS 6387. – P. 161 – 177.

[8] M. Barni, Watermarking systems engineering: enabling digital assets security and other applications / M. Barni, F. Bartolin i // Signal processing and communications. – CRC Press, 2004. – 500 p.

[9] J. Fridrich and J. Kodovsky, Rich models for steganalysis of digital images, IEEE Transactions on Information Forensics and Security.