МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Сравнение методов стегоанализа в файлах формата PNG

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Ермолаевой Анастасии Сергеевны

Научный руководитель

к. ф.-м. н., доцент _____ А. Н. Гамова

22.01.2024 г.

Заведующий кафедрой

д. ф.-м. н., доцент _____ М. Б. Абросимов

22.01.2024 г.

Саратов 2024

ВВЕДЕНИЕ

Невозможно жить в современном мире, ни разу не столкнувшись с понятием стеганографии. Её применение уже настолько повсеместно, что давно не ассоциируется с секретностью и воспринимается как данность нашего времени.

По сути, это не новый метод и применялся ещё с древних времён, однако с ходом прогресса появилось всё больше направлений его использования, и, как следствие, сменились и приоритеты в этих направлениях. Если раньше целью было сокрытие секретного сообщения, то сейчас он чаще используется в интересах авторского права, когда внедряемая информация может быть известна, а целью применения стеганографии при этом является само внедрение этого сообщения в контейнер. В любом случае идёт работа с информацией об информации, то есть, метаданными, и именно их используют, в том числе, для анализа контейнера на наличие скрытого сообщения, ведь если где-то есть потребность в скрытии информации, то обязательно появится потребность в её раскрытии или хотя бы в знании о её наличии.

Методов стегоанализа существует столь же много, сколько и методов стеганографии. В данной работе мы рассмотрим только те методы, которые могут быть применены к изображениям формата PNG, реализуем некоторые из них.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 63 страницы, из них 38 страниц – основное содержание, включая 26 рисунков и 2 таблицы, список использованных источников из 15 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 «Компьютерная стеганография» даются основные определения и понятия, используемые в стеганографии, описаны основные принципы компьютерной стеганографии, а также приведена общая схема стегосистемы.

В подразделе 1.1 «Классификация методов компьютерной ситеганографии» даётся классификация методов компьютерной стеганографии, дан более подробный обзор на методы, основанные на избыточности аудио- и видеофайлов, в том числе преимущества и недостатки, и приведено описание метода наименее значащих бит.

В подразделе 1.2 «Компьютерная стеганография в PNG-файлах» приводится подробное описание устройства формата PNG, приводится список его преимуществ и недостатков и приведены в пример два метода стеганографии, основанных на особенностях структуры формата PNG: метод горизонтального наполнения данными и метод, основанный на манипуляции с блоком, содержащим информацию о ширине и высоте изображения.

В разделе 2 «Методы стегоанализа» приведена классификация методов стегоанализа, основные принципы, на которых они основаны, приведены некоторые примеры методов, их преимущества и недостатки.

В подразделе 2.1 «Визуальные методы» описаны основные принципы работы визуальных методов стегоанализа, приведено описание метода побитовых срезов, дан пример работы метода на основе среза наименее значащих бит, указаны его основные преимущества и условия, при которых его применение может быть наиболее выгодным.

В подразделе 2.1 «Статистические методы» описываются принципы работы статистических методов, приведены примеры некоторых статистических методов стегоанализа, таких как гистограммный метод, метод хи-квадрат и RS-анализ, дано подробное описание работы метода хи-квадрат и RS-анализа, указаны их преимущества и недостатки.

В подразделе 2.2.1 «Метод хи-квадрат» дано описание алгоритма работы метода хи-квадрат, особенности его работы, преимущества и недостатки.

Данный способ предназначен для обнаружения информации, скрытой методом наименьших значащих бит (LSB).

Для анализа изображения используется гистограмма значений цветов пикселей, в которой рассматриваются пары ближайших значений, различающиеся лишь последним битом.

Последовательность средних арифметических значений пар столбцов будет рассматриваться как теоретически ожидаемое значение, а все чётные, либо все нечётные значения в парах – в качестве эмпирически наблюдаемой выборки.

При реализации критерия хи-квадрат происходит сравнение между значениями теоретически ожидаемой частоты и значениями эмпирически наблюдаемой.

Если получившееся значение хи-квадрат получается больше табличного значения квантиля, то это указывает на случайность рассматриваемых данных, а значения меньше либо равные значению квантиля, наоборот, указывают на закономерность, а значит, и на факт наличия встроенного сообщения.

В подразделе 2.2.2 «RS-метод» приведено подробное описание работы RS-анализа и указан ряд его преимуществ.

Метод использует функцию регулярности и маску. В качестве функции регулярности часто выбирается сумма абсолютных разностей (сумма перепадов значений) соседних пикселей, а в качестве маски выступает последовательность значений, каждое из которых выбирается из числа трёх: –1, 0 или 1.

Вычислив значения функции регулярности для группы последовательно идущих бит до наложения маски, сравниваем эти значения с теми, что были получены после наложения маски и после наложения инвертированной (умноженной на -1) маски. В зависимости от того, стало значение больше после наложения маски, стало меньше или не изменилось, эта группа пикселей относится к одной из групп: регулярной, сингулярной или непригодной. Подсчитав количество каждой группы и их долю среди всех групп, на основе

получившихся результатов подсчитываем длину сообщения (его занимаемую долю) в проверяемой области.

В подразделе 2.3 «Методы машинного обучения» указывается, какие задачи решают методы машинного обучения, на чём они основаны и их преимущества над другими методами.

В разделе 3 «Практическая часть» реализуется метод сокрытия информации и 2 метода стегоанализа, а также приводится пример работы программы на основе одного изображения.

В подразделе 3.1 «Использованные программные средства» приводится общая информация о программе и краткое описание её работы.

На вход программе подаётся изображение формата PNG. На выходе программа формирует изображения со стеговложением, наглядные изображения найденного стеговложения, а также несколько файлов с результатами работы программы и собранной статистикой по изображению.

В подразделе 3.2 «Реализация сокрытия данных» рассматривается работа программы на примере изображения формата PNG размером 1280x800 пикселей, и текста, который скрывается в наименее значащие биты синего спектра. Область встраивания выбирается четырьмя способами: линейным, блочным, контрастным и пиксельным. На выходе получаем 4 изображения со стеговложением для каждого значения процента заполненности контейнера.

В подразделе 3.3 «Реализация метода хи-квадрат» описывается алгоритм работы метода хи-квадрат, реализованный в программе, и дан пример его работы на основе изображения, полученного в результате реализации сокрытия данных.

На вход подадим изображения, полученные в результате работы первой части программы, реализующей сокрытие.

Программа получает на вход изображение и разбивает его на блоки определённого размера. В данном случае блоки имеют размер 10240 пикселей и 12800 пикселей. Всего используется 17 разбиений с разной размерностью блоков.

Для каждого блока строятся гистограммы для каждого цветового спектра. Если в гистограмме теоретическое значение меньше 5, эти столбцы объединяются с соседними. Далее для этого блока вычисляется хи-квадрат и по его значению делается вывод, содержится в нём сообщение или нет. Программа сравнивает получившееся значение с табличным значением хи-квадрат для 256 степеней свободы с вероятностью попадания 60%, что равно 247,67. Значения хи-квадрат, использующие меньшее количество цветов, т.е. имеющие меньшую степень свободы чем 256, дополним обратно пропорционально их степеням свободы, т.е. чем меньше используемых цветов, тем больше будет прибавка к хи-квадрат, таким образом значение хи-квадрат может увеличиться максимум в 2 раза.

Также установим нижнюю границу для значения хи-квадрат равную 110. Таким образом, если значение хи-квадрат меньше теоретического и больше установленной нижней границы, то отмечаем этот блок как содержащий вложение.

Также формируем общее изображение найденных стеговложений путём затемнения областей с найденным вложением на фиксированное значение. Таким образом, мы можем найти пересечения блоков разных разбиений и создать общее изображение, где чем темнее область, тем вероятнее в ней находятся скрытые данные.

В подразделе 3.4 «Реализация RS-метода» описывается алгоритм работы RS-анализа, реализованный в программе, и дан пример его работы на основе изображения, полученного в результате реализации сокрытия данных.

Проверяться изображение будет с помощью маски M = [1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0].

Как и с методом хи-квадрат, разбиваем изображение на блоки и применяем метод к каждому блоку отдельно. В отличие от метода хи-квадрат RS-анализ не даёт вывод о том, подозрительная область или нет, а вычисляет длину вложенного сообщения по отношению к проверяемой области. Поэтому при формировании наглядного изображения проверенных областей будет

использоваться градация серого в зависимости от длины найденного сообщения, где белый цвет означает, что найденное сообщение составляет 0% от размера блока, а чёрный – 100%.

Также при формировании общего изображения проверенных областей затемнение не будет меняться на фиксированное значение, а будет зависеть от затемнения в блоке по отношению к общему числу разбиений.

В подразделе 3.5 «Сбор статистики» описывается алгоритм работы с получившимися изображениями для дальнейшей оценки работы методов.

Для этого на основе полученных изображений сформируем новое, состоящее из 4 цветов, каждый из которых означает, было ли произведено встраивание в данную область и нашёл ли метод эту область подозрительной. С помощью таких изображений мы можем не только собрать статистику работы методов, но и наглядно увидеть результат их работы.

В подразделе 3.6 «Выводы» приводится таблица с результатами, полученными в ходе оценки работы методов на одном изображении, приводится ряд выявленных закономерностей и описание изменений метода хи-квадрат, направленных на улучшение его работы.

В ходе практической работы была установлена зависимость между некоторыми параметрами работы метода и изображением. Таким образом была получена нижняя граница хи квадрат, введение которой снизило число ложных срабатываний, а также был внесён множитель значения хи-квадрат, основанный на наблюдаемой закономерности изменения значения хи-квадрат в зависимости от количества цветов в проверяемой области.

Также размер блоков для проверки составлял 10240 и 12800 пикселей, т.к. была выявлена закономерность между размером блока и значением хи-квадрат. Для выявления размера блока, дающего наилучший результат, были построены графики средних значений результатов, полученных в результаты анализа 100 изображений.

Данный анализ показал, что для RS-анализа размер блоков играет не столь существенную роль, поэтому для RS-анализа в работе применяются те же блоки, что и для метода хи-квадрат.

В таблице 1 представлены результаты работы метода хи-квадрат и RS-анализа на изображении с вложением 50%.

Таблица 1 – Результаты работы методов при вложении равном 50%

	Метод хи-квадрат	RS-анализ	Метод встраивания данных
Доля изображения с верно найденным стеговложением (доля чёрных пикселей)	0,5	0,5	Линейный
	0,4522734375	0,4966015625	Блочный
	0,4620751953125	0,1951298828125	Контрастный
	0,05501171875	0,4972802734375	Пиксельный
Доля изображения с ложным срабатыванием методат(доля серых пикселей)	0,3592109375	0,01146875	Линейный
	0,327125	0,4365	Блочный
	0,4504169921875	0,0516904296875	Контрастный
	0,05526171875	0,4972666015625	Пиксельный
Доля изображения с пропущенным стеговложением (доля зелёных пикселей)	0	0	Линейный
	0, 0477265625	0,03984375	Блочный
	0,0379248046875	0,3048701171875	Контрастный
	0,44498828125	0,0027197265625	Пиксельный
Доля изображения без стеговложения, которую метод счёл неподозрительной (доля белых пикселей)	0,1407890625	0,48853125	Линейный
	0,172875	0,0635	Блочный
	0,0495830078125	0,4483095703125	Контрастный
	0,44473828125	0,0027333984375	Пиксельный

В разделе 4 «Аналитическая часть» рассматриваемые методы применяются на выборке из 300 изображений, собирается информация об их работе и делается вывод на основе полученных данных.

В подразделе 4.1 «Сбор статистики» дана общая информация о размере выборки, параметрах изображения, параметрах внедряемого текста и доле производимого вложения.

Была взята выборка из 300 изображений размера 1280x800 пикселей, каждое из которых относится к одному из типов: люди, животные, природа,

город, другое. В каждое изображение встраивается один из трёх текстов: проза, сценарий и юридический документ. В отличие от первого текста, сценарий содержит часто повторяющиеся слова, а юридический – термины и большое количество цифр. Будем рассматривать изображения, заполненные на 0%, 10%, 25%, 40%, 50%, 60%, 75%, 90%, 100%. Для каждого из 4 методов выбора места вставки вычислим средние значения результатов, пример которых представлен в таблице 2, представим в виде графиков и проанализируем.

В подразделе 4.2 «Анализ и выводы» приводится результат анализа выборки в виде графиков и на их основе делается вывод о работе реализованных методов стегоанализа.

В результате были получены следующие графики отдельно для метода хи-квадрат и RS-анализа, представленные на рисунках 1-2, где есть следующие обозначения:

1) L – линейный метод выбора места вставки;
2) P – пиксельный метод;
3) C – контрастный метод;
4) S – блочный метод;
5) A – среднее арифметическое значение всех методов.

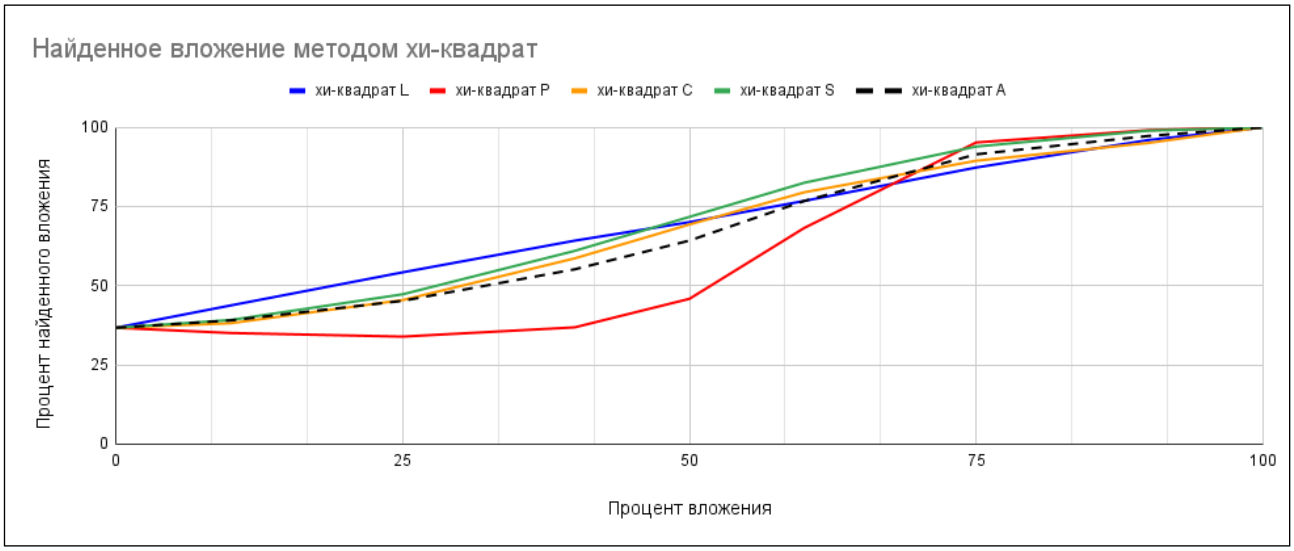

Рисунок 1 – Результаты работы метода хи-квадрат при разных методах вставки

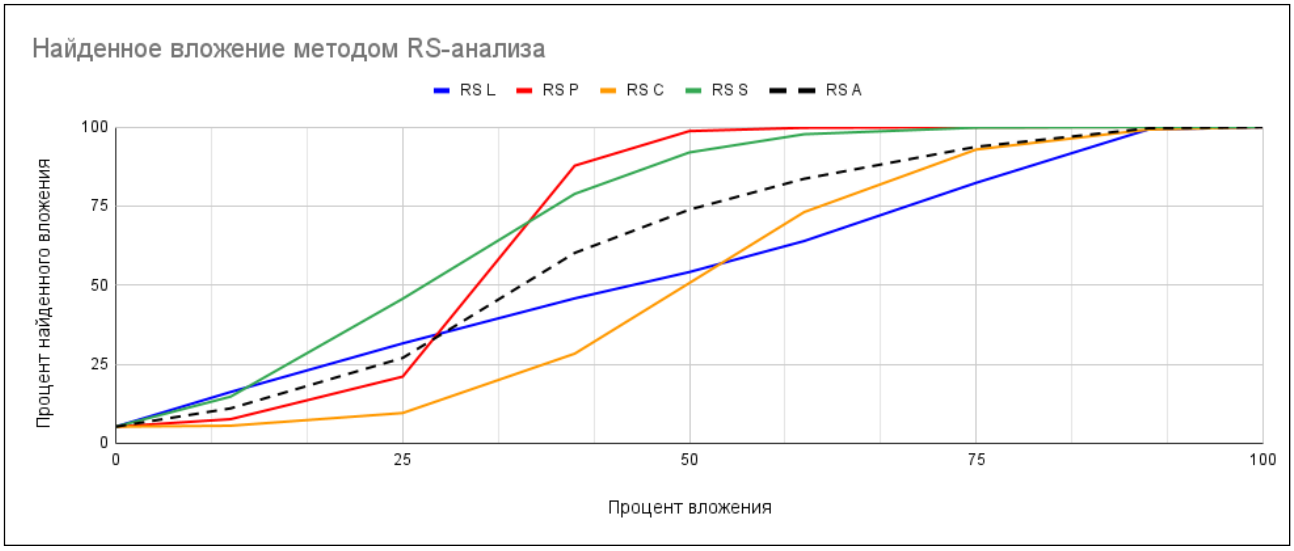

Рисунок 2 – Результаты работы RS-анализа при разных методах вставки

Из этих и других полученных графиков был сделан вывод, что оба метода анализа хорошо справились с линейным методом, выдав наибольший процент верно найденного вложения и наименьшее количество ложных срабатываний.

Хуже всего оба метода анализа справились с пиксельным методом вставки: метод хи-квадрат показал наименьшее значение верно найденного вложения, а RS-анализ при большом проценте верно найденного вложения также дал наибольшее количество ложных срабатываний. Однако, относительно пиксельного метода вставки, это может дать информацию о чувствительности метода анализа к изменениям статистики, при котором RS-анализ начал раньше реагировать на внесение изменений, чем метод хи-квадрат.

Также анализ показал, что метод хи-квадрат имеет большое количество ложных срабатываний, независимо от метода вставки. В пустом контейнере метод хи-квадрат выделяет до 36,7% пикселей изображения как подозрительные. У RS-анализа же этот показатель равняется 5,25%, что значительно меньше при том же уровне верного нахождения вложения в среднем.

Также были сравнены результаты в зависимости от типа изображения.

Данные результаты показали, что картинки с изображением природы для RS-анализа имеют рекордно высокий показатель ложных срабатываний – до 18,7% в пустом контейнере – в то время как метод хи-квадрат имеет один из самых низких значений этого показателя на данном типе изображений. Для

метода хи-квадрат же самый высокий показатель ложных срабатываний – 51,3% в пустом контейнере – показал тип картинок с изображением города и зданий. Для RS-анализа этот тип изображений имеет второе место по количеству ложных срабатываний.

Лучше всего оба метода справились с изображением животных.

Значимых отличий в поведении методов замечено не было, на основе чего было сделано предположение, что контейнер влияет на результат анализа, но место вставки влияет на результат гораздо сильнее.

Сравнение результатов в зависимости от типа скрытого текста не дало сколько-либо значимых результатов, из чего был сделан вывод, что при внедрении достаточно большого теста на любом языке особенности текста перестают иметь значимость в сравнении с особенностями языка.

ЗАКЛЮЧЕНИЕ

В ходе работы были рассмотрен метод сокрытия информации в наименее значащих битах, реализовано сокрытие с использованием метода LSB.

Так же были рассмотрены методы, применяемые для выявления наличия сообщения в изображении, и из них были реализованы 2 метода: метод на основе критерия хи-квадрат и RS-метод и получены выводы для каждого из них.

Также были выявлены закономерности в работе хи-квадрат, изменения на основе которых улучшили работу метода.

Был проведён анализ результатов на основе выборки из 300 изображений и выявлены закономерности и особенности каждого из методов, а также произведено их сравнение.

Оба метода показали свою эффективность в вопросе нахождения скрытых вложений, однако RS-анализ выгодно выделяется за счёт меньшего количества ложных срабатываний, а также за счёт меньшего количества условий и требуемых улучшений для стабильной работы.