УДК 004.056:621.397

В.В. Полиновский, В.Ю. Королев, В.М. Малкина, М.И. Огурцов, В.А. Герасименко

Исследование методов интеллектуального стеганографического сокрытия данных в изображениях до и после их изменения

Введение. Современные компьютерные технологии обработки данных позволили широко использовать криптографические методы защиты информации. Однако для ряда прикладных задач информационной безопасности применения криптографических методов недостаточно, поскольку они не позволяют скрыть сам факт наличия или передачи информации с ограниченным доступом. В таких случаях актуальными становятся стеганографические методы.

Постановка проблемы. Компьютерная стеганография (КС) активно развивается уже более 25 лет. Как известно, стеганографические средства [1] пытаются скрыть сам факт передачи данных. Чаще всего в качестве носителя для сокрытия дополнительной секретной информации используются мультимедийные файлы (контейнеры), КС использует в своих методах их психовизуальную избыточность – часть информации файла-контейнера может быть изменена без существенного влияния на качество контейнера. В то же время современная КС использует методы криптографии для шифрования информации перед ее встраиванием в контейнер, что с точки зрения статистики эквивалентно внесению в контейнер стохастического возмущения.

Упрощение использования методов сокрытия информации и возможность передачи информации по открытым цифровым каналам передачи данных сделали доступными стеганографическое программное обеспечение рядовому пользователю персонального компьютера с доступом к глобальным компьютерным сетям. Сегодня существует много различных стеганографических приложений, в том числе и на бесплатной основе. Понятно, что средства стеганографии могут использоваться как законопослушными гражданами, так и уголовными или шпионскими структурами, поэтому активно развиваются соответствующие методы противодействия – компьютерный стегоанализ (СА), который предназначен для

обнаружения факта сокрытия информации внутри контейнера или выявления факта скрытой передачи данных.

Компьютерный стегоанализ. Стегонализ является пассивной атакой на стеганографические системы, то есть такой, которая не изменяет содержание сообщения. Сегодня СА выделяется как самостоятельное научное направление, целью которого является выявление в носителе (контейнере) факта наличия скрытых данных и оценка объема этих данных. СА широко использует аппарат математической статистики, линейной алгебры, комбинаторики, теории планирования эксперимента, статистического анализа, цифровой обработки и распознавания сигналов и изображений, а также другие разделы математики. Численные эксперименты по внедрению и выявлению скрытых данных являются основным способом получения достоверных сведений о качестве работы алгоритмов стеганографии и стегоанализа. Исследование устойчивости методов сокрытия данных в СА позволяет проверить надежность стеганографических алгоритмов, а также внести свой вклад в информационную безопасность государства.

Анализ последних исследований и публикаций. За последние 25 лет создано много методов сокрытия информации в различных типах и форматах [1-4], а также методов обнаружения встроенных данных. Популярным на сегодня методом стеганографического сокрытия является метод замены наименее значимых бит (НЗБ-стеганография). Идея метода состоит в замене от одного до четырех младших бит в байтах цветов пикселей исходного изображения битами сообщения, которые нужно скрыть в этом контейнере [10]. Такие методы надежны и наиболее просты для программирования, поэтому большинство коммерческих и свободных программ сокрытия данных имеют в своем составе приложения НЗБ-стеганографии. Метод применяется в растровых изображениях, представленных в форматах без потерь.

Соответственно, большинство методов стегоанализа разработано для выявления именно НЗБ-стеганографии [1-4]. Одним из наиболее точных современных методов обнаружения данных в изображениях, сохраненных в форматах без потерь, является RS-стегоанализ [2-3].

Однако абсолютное большинство современных цифровых фотографий хранится в формате JPEG, так как в нем лучше реализовано сжатие изображений при минимуме потерь визуального качества. Высокая производительность JPEG-алгоритмов основывается на быстрых преобразованиях, в которых ограничивается интенсивность высокочастотных составляющих изображений. Но как утверждается в работе [1] , непосредственное применение методов НЗБ-стеганографии к изображениям в формате JPEG достаточно просто может быть обнаружено, поскольку существенно искажает соотношение чисел изображения в таком формате. При этом использование файлов цифровых фотографий с расширениями кроме JPEG для передачи или демонстрации любительских фотографий через Интернет на сегодняшний день является подозрительным для стегоаналитика.

При создании методов стегоанализа разработчики исходят из того, что пользователи будут фотографировать объекты или сцены фотокамерами среднего или высокого класса, или будут использовать цифровые фотографии с тематических сайтов в сети Интернет. Однако изображение может быть обработано владельцем фотографии (обработка изображения для демонстрации в Интернет), или самим пользователем для того, чтобы исключить для стегоаналитика возможность получения точного оригинала.

Одна из целей данной работы заключается в проведении исследований заданной точности и достоверности получения результатов [5] для RS-анализа массива файлов-контейнеров с целью выявления их закономерностей и путей обработки этих файлов для безопасного сокрытия стеганографических данных внутри этих файлов.

Постановка задачи. Как правило, для статистических исследований методов стегоанализа берут наборы фотографий (около 150-450 файлов) без возможности оценки их предварительной обработки. В нашем цикле работ было показано [1-5], что такой подход приводит к преувеличению возможностей метода стегоанализа. Кроме того, на результаты статистических исследований влияет не только степень зашумления изображения, но и разрешение фотографии. Так для изображений большого формата без встроенных

стеганографических данных характерно меньшее значение ложно положительно выявленных стеганобит (ЛПВС) [4] – величин естественного шума и артефактов регистрации фотографий, которые неверно трактуются методом RS-стегоанализа, как скрытые данные. С другой стороны, метод СА при моделировании работы НЗБ-алгоритма выдает величину положительно выявленных стеганобит (ПВС) с погрешностью в большую или в меньшую сторону в силу стохастической природы формирования изображения и случайных совпадений и несовпадений значений стеганобит с битами цифровой фотографии. Поэтому задачей данной работы является выполнение RS-анализа массива изображений, полученных из камер различных марок и типов, часть которых может быть обработана. После первоначального анализа массив будет подвергнут воздействию различных фильтров, и будет оцениваться влияние внесенных изменений на результаты стегоанализа. Целью этих действий является выявление универсальных средств, способных снизить риск обнаружения данных, скрытых внутри файлов изображений.

Основная часть. Выполним формализацию направлений статистических исследований RS- СА - их можно сгруппировать в следующие основные направления:

1) Количественные исследования – сбор статистики для изображений со встроенными данными и оригиналов (без скрытых данных). По полученным данным (особенностям изображений-аномалий) можно сделать правдоподобные предположения о ложном обнаружении скрытых данных и других слабых мест методов стегоанализа.

2) Определение влияния цифровой фильтрации на RS-СА результаты. Анализ существующих операций над изображениями при подготовке к печати и / или типовых операциях шумоподавления и улучшения визуального качества: усиление яркости, повышение контраста и т. д.

3) Исследование качественно-количественных соотношений изображений (статистики высокого порядка, производные статистические характеристики).

4) Тестирование методов обхода: предварительная фильтрация, подбор изображений, добавление в которые стеганобит не увеличивает существенно процент ПВС при RS-CA.

Архитектура программного комплекса анализа изображений. Для исследований характеристик массивов изображений различными методами был разработан универсальный комплекс анализа изображений с модульной архитектурой, который позволяет добавлять новые форматы файлов изображений и алгоритмов их анализа, а также выполнять обработку этих изображений без изменения самого комплекса [6]. Главной задачей, которая ставилась при разработке комплекса стегоанализа, была потребность проведения исследований не только оригинальных массивов изображений, но и определенным образом модифицированных версий в процессе обработки изображений, например – результатов фильтрации по выбранным оператором-аналитиком алгоритмам. Кроме того, необходимо было выполнять анализ изображений различными алгоритмами, т.е. в общем случае над изображениями необходимо выполнить заданную последовательность операций фильтрации и анализа. Каждая операция имеет возможность настройки, т.е. задания параметров фильтрации и анализа.

Полученные массивы статистик хранятся в базе данных, структура которой позволяет сохранять и получать статистику, обработанную другими модулями анализа данных. Также комплекс имеет достаточно широкие возможности выборки и анализа накопленных данных. По перечисленным характеристикам комплекс стегоаналитических исследований существенно отличается от имеющихся решений, большинство из которых являются узкоспециализированными и выполняют анализ изображений только одного типа и одним алгоритмом, результаты обработки также представляются в своем формате.

Для решения этой задачи была реализована модульная архитектура комплекса, которая предусматривает реализацию фильтров и анализаторов в отдельных модулях-расширениях комплекса [7]. Это позволяет добавлять такие модули без изменения основного комплекса. Фильтр и анализатор в этой архитектуре определяются как программные интерфейсы (набор методов с определенными сигнатурами), используемые основным комплексом при обработке

файлов. Модули-расширения представляют собой обычные dll-библиотеки, содержащие один или несколько классов, которые реализуют эти интерфейсы.

Среди прототипов комплекса можно назвать комплексы MGEBO [1] и Digital Invisible Ink Toolkit [4], а среди аналогов – приложения, разработанные лабораторией проф. Д. Фридрич, Virtual Steganographic Laboratory for Digital Images [7].

На рис. 1 приведена диаграмма классов комплекса, которая включает интерфейсы фильтра и анализатора, а также несколько классов, реализующие эти интерфейсы. Каждый из этих классов реализован в отдельном проекте dll-библиотеки.

Кроме интерфейсов на диаграмме приведены 2 класса фильтров и 4 класса анализаторов:

- ImageFilters – реализует набор стандартных графических фильтров: GaussianBlur, Defocus, Highlight, Sharpen, BigEdge, Emboss, EmbossColor, EdgeDetect, Negative, RemoveChannel, Punch;

- SteganosFilter – реализует фильтры сокрытия данных, основанные на алгоритме НЗБ;

- MathStatAnalyzers – выполняет анализ изображений методами математической статистики, возвращая среднее значение, среднеквадратичное отклонение и медиану для нескольких характеристик в различных цветовых пространствах;

- RS-Analyzer – выполняет RS-анализ и возвращает набор коэффициентов результатов;

- ColorComparisonAnalyzer – выполняет сравнение цветных составляющих пикселей изображения (R, G, B) и возвращает статистику по соотношению между ними;

- NoiseAnalyzer – возвращает шумовые характеристики для разных цветных пространств.

Количество таких классов фильтрации и анализа будет расширяться для поддержки новых методов и алгоритмов. Работа с комплексом разбивается на несколько этапов:

1) Выбор файла базы данных, в котором будет храниться статистика.

2) Добавление папок с изображениями, которые необходимо обработать. Поддерживается рекурсивная обработка поддиректорий и задание списка масок файлов для обработки.

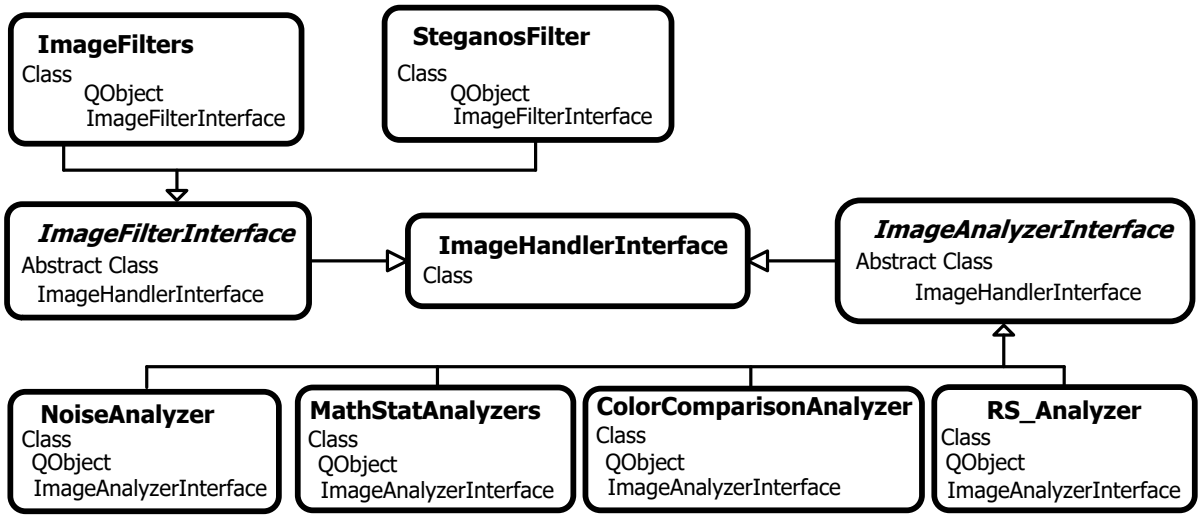

Рис. 1. Диаграмма классов фильтров и анализаторов

3) Задача последовательности экземпляров фильтров и анализаторов, которыми будут обрабатываться и исследоваться фотографии. Фильтр – это модуль, который меняет изображение согласно определенному алгоритму. Анализатор возвращает определенный набор статистик. Для модулей обоих типов может задаваться набор специфических для них параметров (например, коэффициенты работы алгоритмов фильтрации и анализа) – таким образом, создаются экземпляры фильтров и анализаторов, и добавляются в последовательность.

4) Запускается на выполнение задача обработки файлов по данным предыдущих этапов. Реализация обработки выполнена по схеме рабочих потоков, файлы изображений обрабатываются независимо, благодаря чему повышена эффективность параллельной обработки на SMP-системах.

5) После окончания обработки накопленная статистика доступна для выборок и экспорта в виде отчетов трех типов (см. рис. 2). Статистика по изображениям позволяет получить результаты анализа изображений по каждому файлу отдельно. При этом можно выбрать необходимый набор данных, которые будут выводиться для изображений, а также задать условие фильтрации по ним, например: ([Ширина] > 1000) and ([Высота] > 1000) and ([Имя] like 'nature %'). На второй вкладке можно выбрать набор доступных данных статистики, он

отображается в виде дерева, содержащего последовательности экземпляров фильтров и анализаторов с вложенными списками статистики, которую можно включить в отчет (рис. 2).

По данным статистики можно также использовать фильтрацию, задавая нужным колонкам символические имена и используя их в выражениях фильтра, например: ([a1] > 90) and ([a2] > 40). После задания параметров отчета можно просмотреть результат на третьей вкладке. Его можно экспортировать в csv-файл для дальнейшей обработки в табличном процессоре.

Второй вариант статистики – совокупный, позволяет выводить агрегированную выбранной функцией (минимум, максимум, сумма, количество и среднее значение) статистику по заданным данным, сгруппированную по выбранным колонкам. Например, можно получить суммарную статистику отдельно по всем папкам, в которых находятся обработанные изображения.

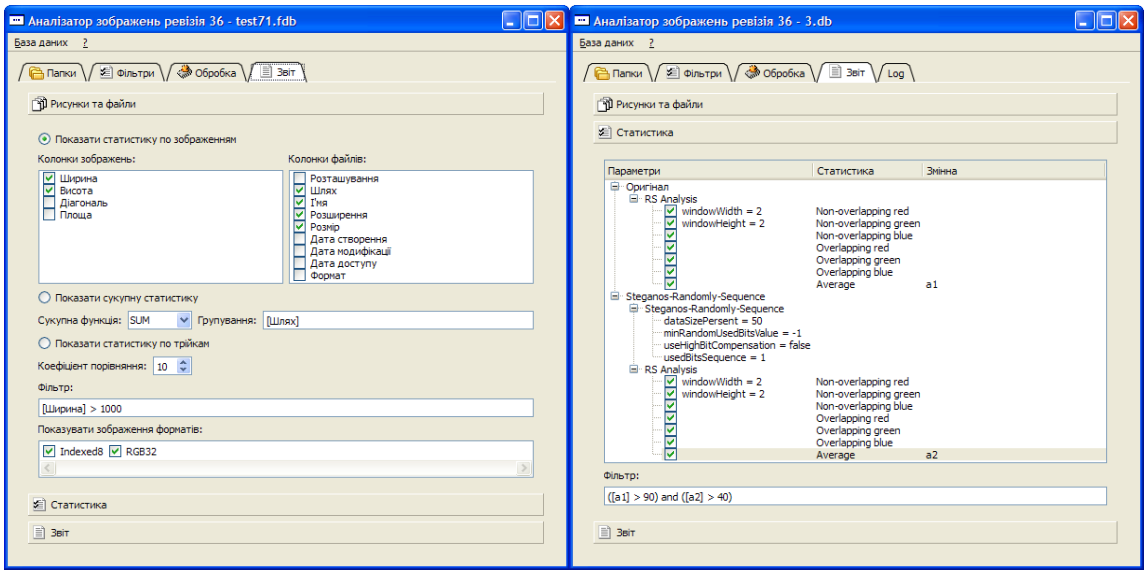

Рис. 2. Параметры получения отчета по статистике

Результаты анализа изображений. Авторами был выполнен ряд исследований влияния различных возможных модификаций, которые могут быть внесены в изображение при его изменении как обычными пользователями для улучшения качества, так и с целью сокрытия внутри изображения каких-то данных специальными широко известными стеганографическими методами. Оценка выполнялась путем применения распространенного на сегодняшний день средства стеганографического анализа изображений – RS-анализа [3]. На сегодняшний день это

наиболее популярный и эффективный способ обнаружения данных, которые были скрыты в изображениях с использованием различных стеганографических методов [6].

Поскольку он не привязан к конкретным алгоритмам сокрытия, он изучает собственно изображение с целью выявления его природных закономерностей и возможных изменений, которые были внесены туда и исказили эти закономерности [2]. Метод RS-анализа является чрезвычайно эффективным [8] и, хорошо зарекомендовав себя на мировом рынке средств стегоанализа [7], применяется практически везде, где выполняется поиск данных, скрытых с использованием стеганографических методов защиты. RS-анализ является достаточно сложным вычислительно, требует значительных компьютерных мощностей для использования, особенно при анализе большого количества изображений. Однако он обладает исключительной точностью обнаружения данных, причем результаты выдаются не в бинарной форме ответа «Да/Нет», а в виде процента вероятности наличия скрытых данных внутри файла-контейнера.

Было проведено исследование оценки качества обнаружения стеганографических данных с использованием метода RS-анализа – анализ большого массива изображений (в количестве 1960 единиц), полученных из сети Интернет и домашних коллекций обычных пользователей для оценки метода RS-стегоанализа на типичных изображениях, циркулирующих по незащищенным каналам связи. Целью выполнения этих исследований, как было указано выше, является выявление возможного внесения изменений, что позволит предотвратить обнаружение последующего скрытного внесения информации внутрь изображения-контейнера.

Например, имеем обработанное каким-либо образом (или вообще необработанное) изображение. RS-анализ показывает, что с вероятностью 5 процентов в нем есть скрытые данные. Изучение результатов применения метода RS-анализа [8] показывает, что это весьма вероятно для обычных изображений и не вызовет подозрений, подозрительными являются изображения с вероятностью более 10 процентов. Если мы будем иметь метод обработки изображений, позволяющий уменьшать результаты RS-анализа, то мы можем обработать изображение, уменьшив вероятность сокрытия данных внутри этого изображения, скажем, до

2х процентов. Теперь мы можем вставить внутрь изображения столько данных для сокрытия, чтобы вероятность снова возросла до 5 процентов. Тогда метод RS-анализа не будет способен обнаружить факт сокрытия данных внутри изображения-контейнера даже в том случае, если оригинал этого изображения будет представлен для анализа стегоаналитикам.

Результаты первоначального анализа и анализа после применения различных типов фильтров и изменений эталонных изображений представлены в таблице 1. Этот набор с 1960 изображений не должен в массе своей вызвать подозрений у средств обнаружения данных, скрытых стеганографической.

Таблица 1. Результаты RS-анализа необработанных и обработанных изображений

Начальное	F5	BigEdge	Defocus	EdgeDetect	Emboss	Emboss Color	Gaussian Blur	Highlight	Negative
1,607254	0,16502	9,26580866	19,38030437	24,9991248	2,886681	9,84601976	0,338797261	2,75646492	1,327624474
Punch	Remove Channel	Sharpen	SharpenEven More	SharpenMore	OutGuess	StegoImage	Steganos Randomly Sequence	Steganos Randomly Exponent	Steganos Sequentally Sequence
1,327628298	0	7,27011573	430,555542	73,8607556	1,764190194	41,66904026	51,21559884	51,2574905	46,67412468
Steganos Sequentally Exponent			Steganos Skip Values		StegHide			VLS LSB	
46,73445024			1,881033139		1,8465696			1,8298698	

Рассмотрим данные, приведенные в этой таблице. В первом столбце представлен средний результат RS-анализа. Он составляет всего 1,6 процента вероятности наличия скрытой информации, подтверждающей эффективность, точность и качество анализа в области ложно-положительных срабатываний. В последующих столбцах представлены результаты, полученные RS-анализом после использования фильтров, предназначенных для обработки изображений. Все фильтры и алгоритмы применялись с набором параметров по умолчанию, чтобы предотвратить искажение результатов исследования за счет изменения параметров работы фильтров.

Третий столбец представляет фильтр BigEdge (Большие границы), предназначен для выделения и подчеркивания границ изображений, а четвертый – фильтр Defocus (Расфокусировка) – для уменьшения резкости изображения. EdgeDetect – фильтр «Определение границ» – изменяет яркость границ объектов, определенных как, подчеркивая их. Фильтр

Emboss (Тиснение) предназначен для создания текстур – рельефных выпуклых тиснений и фасок, для повышения резкости при ретушировании изображений. Emboss Color (Цвет рельефа) позволяет создавать выпуклые фигуры в оттенках серого, подчеркивая границы изображений цветом. Фильтр Gaussian Blur (Размытие по Гауссу) позволяет уменьшать резкость изображений, интеллектуально отыскивая границы объектов (области повышенного контраста между соседними пикселями) и уменьшая ореолы вокруг них. Фильтр Highlight (Подчеркивание) предназначен для подчеркивания деталей в наиболее светлых и темных областях изображения, расширение тонового диапазона изображения. Фильтр Negative (Негатив) инвертирует цвета изображения, фильтр Punch (Выдавливание) применяет эффект «Рыбьего глаза» (fish eye) на изображении, искажая его перспективу. Фильтр Remove Channel (Удалить канал) полностью удаляет выбранные каналы изображения. Группа фильтров Sharpen (Резкость), SharpenMore (более резкости) и SharpenEvenMore (еще больше резкости) повышает резкость всего изображения, повышая резкость границ объектов и малых деталей. Разница лишь в интенсивности эффекта.

Теперь рассмотрим эффект от применения стеганографических алгоритмов. Второй столбец представляет алгоритм F5, предназначенный для сокрытия данных в изображении стеганографическим путем. Он не считается надежным на сегодняшний день [9]. Алгоритм OutGuess позволяет стеганографически встраивать данные внутрь изображений png и jpeg. Как и F5, уязвим к стегоанализу. OutGuess сохраняет статистику, основанную на частотности. В результате, статистические тесты, основанные на частоте подсчетов, не в состоянии обнаружить присутствие стеганографического содержимого внутри изображения. Перед встраиванием данных OutGuess способен определить максимальный размер сообщения, которое может быть скрыто так, чтобы поддержать статистику, основанную на частотности [9].

Алгоритм StegoImage – это LSB-фильтр внедрения данных, он имеет 3 уровня внедрения и выявляется RS-анализом [2]. Steganos-Randomly-Sequence, Steganos-Randomly-Exponent, Steganos-Sequentally-Sequence, Steganos-Sequentally-Exponent, Steganos-SkipValues – пять

фильтров внедрения данных. Они разбиты по алгоритмам выбора последовательности записи битов по байтам рисунка, выбора количества бит, применяемых для сокрытия данных. Стандартный вариант внедрения – первый, можно задавать процент внедрения данных. Алгоритм StegHide позволяет внедрение данных в bmp и jpeg-файлы, предыдущий частотный анализ соответствующих цветов позволяет внедрение данных, не меняя цветовых соотношений, что делает стеганографическое внедрение данных устойчивым против статистических тестов первого порядка, улучшенный алгоритм позволяет предотвратить выявление скрытых данных по соотношениям цветов и частот на основе статистических тестов. Фильтр VLS LSB – Virtual Steganographic Laboratory for Digital Images (VSL) Least Significant Bit (LSB) Steganography реализует традиционный LSB-алгоритм сокрытия данных, с легкостью обнаруживается любым из современных средств стегоанализа [1].

Представим полученные результаты в наиболее наглядном виде. В таблице 3 представлены усредненные результаты влияния внесенных изменений в изображение на вероятность наличия скрытых данных внутри файла-контейнера, определенные путем применения RS-анализа до и после этих изменений. Подсчет выполнялся следующим образом:

$$V_{av} = \frac{\sum_{i=1}^{n}(Pb_i - P_i)}{n} \quad (1)$$

где *Vav* – усредненный результат влияния вносимых изменений на весь набор зображений, n – количество изображений в наборе, который подвергался анализу, Pi – начальная вероятность наличия скрытых данных внутри изображения i, Pb_i – вероятность наличия скрытых данных после применения изменения.

Как можно понять из формулы (1), отрицательные результаты (значения ниже нуля) – это хорошо, поскольку означает уменьшение вероятности скрытых данных. Ноль означает, что вероятность не изменилась, а положительные значения – что вероятность возросла и фильтр непригоден для подготовки изображения для стеганографического сокрытия информации.

Как видно из таблицы 2 и рис. 3, результаты RS-анализа изображений, обработанных с использованием различных вариантов методов воздействия (фильтров и др.), можно разделить

на три группы. К первой группе относятся фильтры, которые не привели к изменению результатов. Среди них можно выделить алгоритмы F5, StegHide, OutGuess и VLS LSB – RS-анализ выявляет скрытые ими данные, но их применение без внесения данных не повышает уровня подозрительности изображений. Отдельно следует выделить фильтр Remove Channel, удаляющий выделенные каналы целиком. После его применения (с удалением наименее информативного голубого канала) вероятность скрытых данных согласно RS-анализу всегда уменьшается до нуля, но его применение значительно и неестественно изменяет изображение, поэтому оно станет подозрительным даже без применения инструментов анализа, делает невозможным применение Remove Channel для сокрытия факта наличия стеганографически защищенных данных. Также не влияет на результаты RS-анализа фильтр Negative.

К фильтрам, которые негативно влияют на результаты RS-анализа эталонных изображений можно отнести алгоритм StegoImage, Steganos-Randomly-Sequence, Steganos-Randomly-Exponent, Steganos-Sequentally-Sequence, Steganos-Sequentally-Exponent, Steganos-SkipValues – стеганографические алгоритмы, без проблем выявляются RS-анализом. Также к ним можно отнести обычные фильтры обработки изображений – Sharpen, SharpenMore и SharpenEvenMore, BigEdge, Defocus, EdgeDetect, Emboss, Emboss Color и Highlight. Изменения, вносимые ими, однозначно приводят к повышению вероятности наличия скрытых данных согласно RS-анализу.

Теперь рассмотрим третью, самую малочисленную группу алгоритмов – положительно влияющие на результаты RS-анализа. К ним относятся только Gaussian Blur и Punch (особенности работы фильтра Remove Channel и его неприменимость описаны выше). При этом изменения, вносимые фильтром Punch, оказываются малозначимыми и положительные изменения проявляются не на всех изображениях, поэтому его применение в качестве средства для подготовки файла-контейнера для дальнейшего сокрытия информации внутри него является бесперспективным. Таким образом, единственным фильтром, позволяющим стабильно уменьшать результаты RS-анализа, является Gaussian Blur. Его применение дает

положительный эффект независимо от типа и размера изображения, процентное значение улучшения зависит от начального значения RS-анализа изображений.

Таблица 2 представляет изменение показателей результатов RS-анализа изображений в соответствии с формулой (1).

Таблица 2. Влияние применения различных изменений изображений на результаты RS-анализа

Начальное	F5	BigEdge	Defocus	EdgeDetect	Emboss	Emboss Color	Gaussian Blur	Highlight	Negative
0	0	7,692641805	18,56056162	24,17938207	2,088309699	8,798974476	-0,813470076	2,3382909	0
Punch	Remove Channel	Sharpen	SharpenEven More	SharpenMore	OutGuess	StegoImage	Steganos Randomly Sequence	Steganos Randomly Exponent	Steganos Sequentally Sequence
0,00000382	-1,6072539	5,461518206	429,861315	71,67588834	-0,04155358	38,64477387	49,49200375	49,4265843	44,87032833
Steganos Sequentally Exponent			Steganos Skip Values		StegHide			VLS LSB	
44,90458045			0,052070325		0,016699833			0	

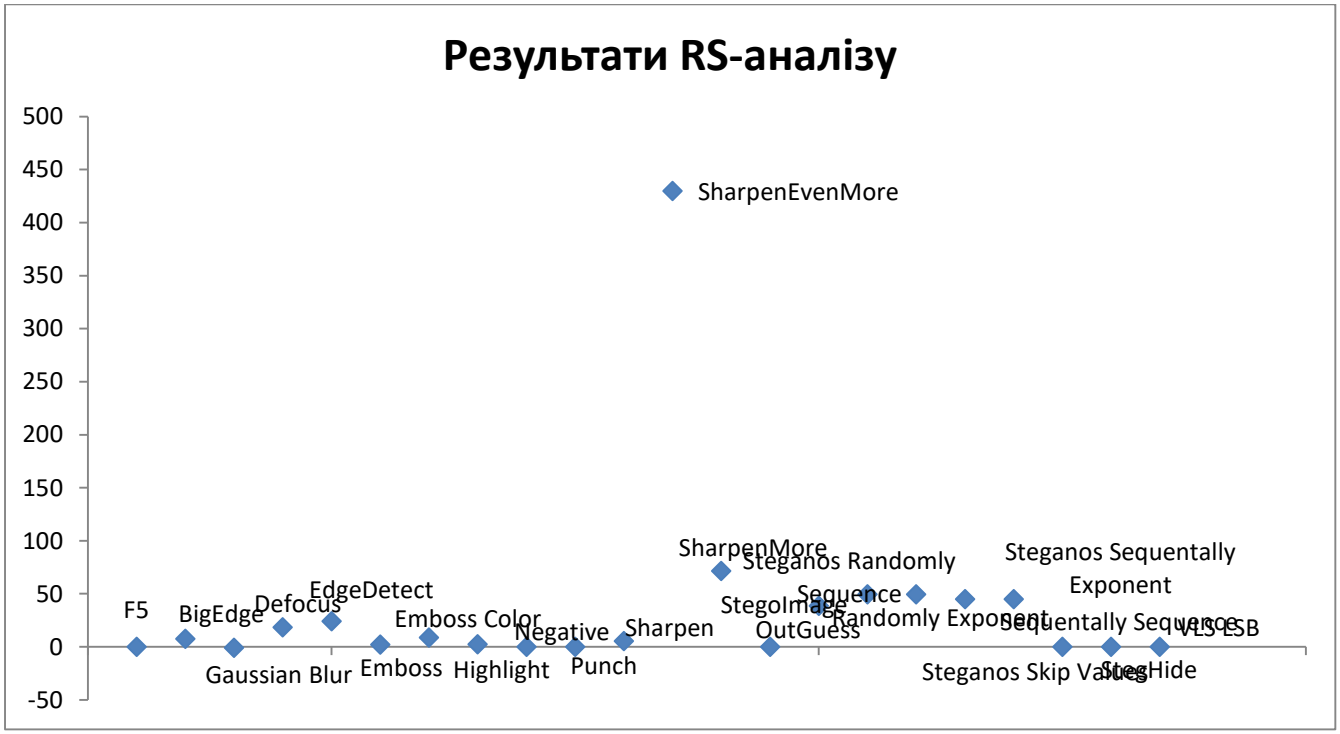

Рис. 3. Влияние применения различных изменений изображений на результаты RS-анализа

Результаты влияния применения различных изменений изображений на результаты RS-анализа также представлены в графической форме на рис. 3.

Результаты после применения StegHide, Steganos Skip Values и OutGuess отличаются от 0 настолько мало, что этим различием можно пренебречь – оно не позволит применить их для улучшения защиты данных от стегоанализа.

Выводы

1. Предложена комплексная система статистических исследований для методов стегоанализа.

2. Разработан модульный проблемно-ориентированный комплекс стегоаналитических исследований, позволяющий оператору гибко изменять направления сбора статистики и экспортировать полученные данные.

3. Благодаря созданному комплексу получены новые результаты в области сокрытия данных стеганографическими методами в изображениях: обнаружены ограничения метода RS-стегоанализа для многих классов изображений, доступных в сети Интернет, поскольку есть достаточно большая вероятность ложноположительных срабатываний; предложены способы обхода метода RS-стегоанализа; обнаружен максимально допустимый объем безопасного встраивания данных: он составляет 2%, а удовлетворительный уровень не должен превышать 5%. Объемы встраивания 5-10% являются подозрительными, а более 10% – маловероятными для необработанных цифровых фотографий.

4. Единственным средством предварительной обработки изображений среди протестированных, которое позволяет уменьшить вероятность обнаружения данных, что в дальнейшем будут стеганографически скрыты внутри этих изображений, оказался фильтр Gaussian Blur.

5. Выбор оптимальных параметров этого фильтра в зависимости от параметров изображения и количества информации, которое необходимо скрыть внутри контейнера, является перспективным направлением дальнейших исследований.

Литература

1. Королёв В.Ю., Полиновский В.В., Герасименко В.А. Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей // Управляющие системы и машины. — № 1 (231). — 2011. — С. 79—87.

2. Корольов В.Ю., Поліновський В.В., Герасименко В.А. RS-стегоаналіз. Принципи роботи, недоліки та концепція метода його обходу // Вісник Вінницького політехнічного інституту. — 2010. — № 6. — С. 66—71.

3. Корольов В.Ю., Поліновський В.В., Герасименко В.А. Визначення можливостей RS-стегоаналізу для дослідження статистичних властивостей зображень // Вісник Хмельницького національного університету. — 2010. — № 4.— С. 102—110.

4. Корольов В.Ю., Поліновський В.В., Герасименко В.А. Стеганографічна персоналізація інформації на базі ПК // Вісті Академії інженерних наук України. - 2009. - №2(39). — С.18—24.

5. Корольов В.Ю., Поліновський В.В., Герасименко В.А., Горінштейн М.Л. Планування досліджень методів стеганографії і стегоаналізу // Вісник Хмельницького національного університету. — 2011. — № 4.— С. 187– 195.

6. В.В. Поліновський, В.Ю. Корольов, В.А. Герасименко, М.Л. Горинштейн Інформаційна технологія для дослідження методів стеганографії і стегоаналізу // Міжвузівський збірник "Комп'ютерно-інтегровані технології: освіта, наука, виробництво" (м. Луцьк). - 2011. - Випуск №5. - С. 236-242.

7. Корольов В.Ю., Поліновський В.В., Герасименко В.А., Горінштейн М.Л. Комплекс статистичних досліджень для стегоаналізу // Математичне та комп’ютерне моделювання (Кам’янець-Подільський національний університет імені Івана Огієнка). — Збірник наукових праць: Серія Технічні науки. — 2011. — Випуск 5. — С.134 – 149.

8. Корольов В.Ю., Поліновський В.В., Герасименко В.А. Дослідження стійкості НЗБ-стеганографії до RS-аналізу // Матеріали IV Міжнародної конференції “Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП - 2009)”, [Частина 1]. — Вінниця: ВНТУ Мін. Освіти і науки України. — 2009. — С. 53.

9. Defending Against Statistical Steganalysis Niels Provos, 10th USENIX Security Symposium. Washington, DC, August 2001.