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

Предложена концепция стеганокриптографической персонализации информации на основе аппаратно-программной системы аутентификации пользователей. Показано, что реализация стеганографических программных средств с предварительной обработкой изображений на основе размытия по Гауссу с индикацией угрозы обнаружения скрытых данных позволяет повысить уровень персонализации информации с ограниченным доступом.

The concept steganographiccryptographic personalization of information based on the hardware-software system of user authentication is presented. The implementation of the steganographic software increases the level of personalization of information with the restricted access.

Запропоновано концепцію стеганокриптографічної персоналізації інформації на основі апаратно-програмної системи автентифікації користувачів і протоколу передачі даних з підвищеним ступенем захисту. Показано, що реалізація стеганографічних програмних засобів з попередньою обробкою зображень на основі розмиття за Гаусом з індикацією погроз виявлення схованих даних дозволяє підвищити рівень персоналізації інформації з обмеженим доступом.

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 факт наличия или передачи информации с ограниченным доступом. В таких случаях актуальными становятся стеганографические методы.

Состояние проблемы

Компьютерная стеганография (КС) активно развивается уже более 25 лет. Как известно, стеганографические средства [1] пытаются скрыть 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 включением в контейнер, что по данным 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

Это есть пассивная атака на стеганографические системы, не изменяющая содержание сообщения. Сегодня СА выделяется как самостоятельное научное направление, цель которого – 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 – основной способ 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 сегодня методом стеганографического сокрытия есть 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. 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, ограничивающих 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 сегодня подозрительны для стегоаналитика.

При создании методов стегоанализа разработчики исходят из того, что пользователи будут фотографировать объекты или сцены фотокамерами среднего или высокого класса, или 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 статьи 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 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 ложноположительно выявленных стеганобит (ЛПВС) [4] – величин естественного шума и артефактов регистрации фотографий, которые некорректно 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 задача авторов статьи – 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. Цель этих действий – выявление универсальных средств, способных снизить риск обнаружения данных, скрытых внутри файлов изображений.

Основная часть

Выполним формализацию направлений статистических исследований *RS*-СА – их можно сгруппировать по основным направлениям.

• 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.

• 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.

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

• Тестирование методов обхода: предварительная фильтрация, подбор изображений, добавление в которые стеганобит не увеличивает существенно процент ПВС при *RS*-СА.

Архитектура программного комплекса анализа изображений

Для исследований характеристик массивов изображений различными методами был разработан универсальный комплекс анализа изображений с модульной архитектурой, позволяющий добавлять новые форматы файлов изображений и алгоритмов их анализа, а также выполнять обработку этих изображений без изменения самого комплекса [6]. Главной задачей 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 узкоспециализированны и выполняют анализ изображений только одного типа и одним алгоритмом, результаты обработки также представляются в своем формате.

Для решения этой задачи реализована модульная архитектура комплекса, предусматривающая реализацию фильтров и анализаторов в отдельных модулях–расширениях комплекса [7], что позволило 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, реализующие 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, включающая интерфейсы фильтра и анализатора, а также несколько классов, реализующих эти интерфейсы. Каждый из этих классов реализован в отдельном проекте *dll*-библиотеки.

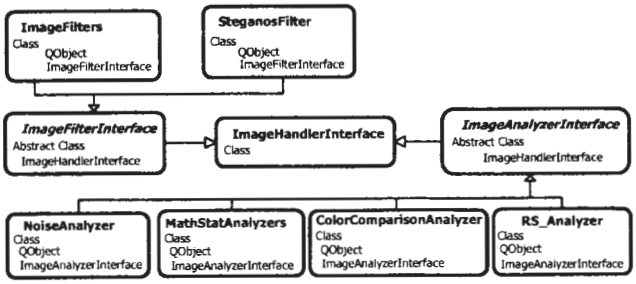

Рис. 1. Диаграмма классов фильтров и анализаторов

Кроме интерфейсов на диаграмме приведены два класса фильтров и четыре 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.

• Выбор файла базы данных для хранения статистики.

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

• Задача последовательности экземпляров фильтров и анализаторов, которыми будут обрабатываться и исследоваться фотографии. Фильтр – это модуль, меняющий 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.

• 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.

• После окончания обработки накопленная статистика доступна для выборок и экспорта в виде отчетов трех типов (рис. 2). Статистика по изображениям позволяет получить результаты анализа изображений по каждому файлу отдельно. При этом можно выбрать необходимый набор данных, выводимых для изображений, а также задать условие фильтрации по ним, например: (Ширина > 1000), Высота > 1000) и (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: ([*a*1] > 90) и ([*a*2] > 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, количе-

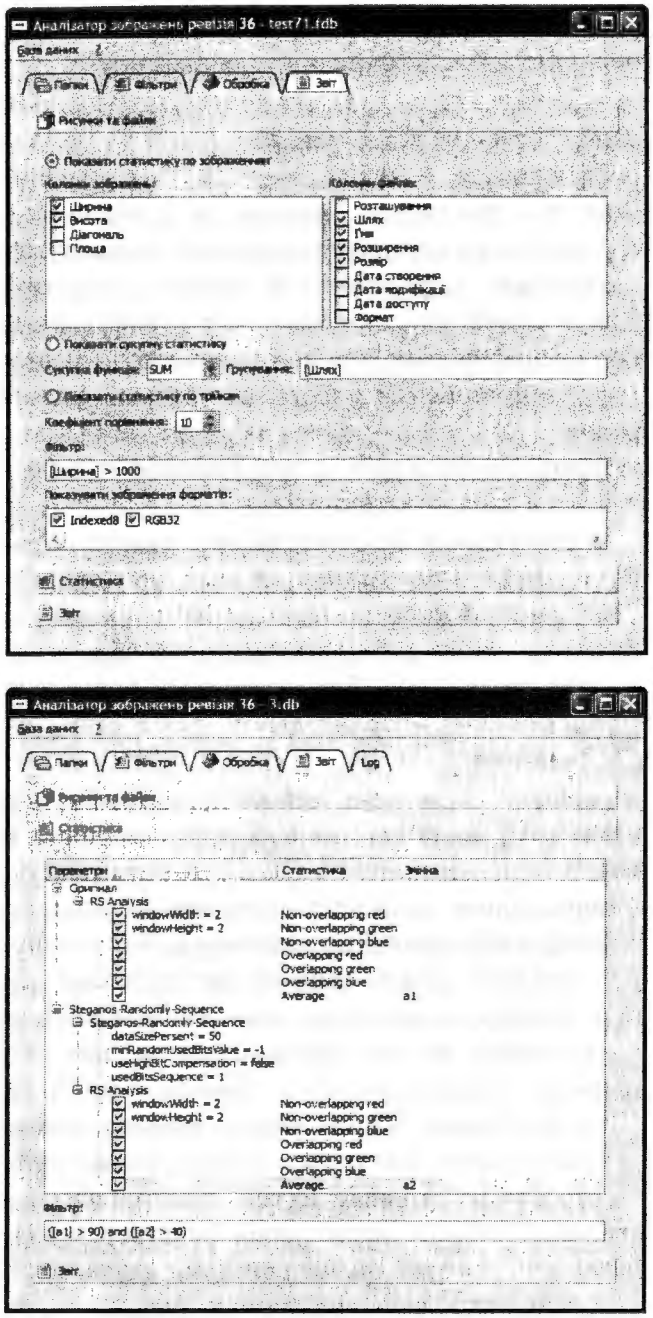

Рис. 2. Параметры получения отчета по статистике

ство 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.

Результаты анализа изображений

Авторами 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 средства стеганографического анализа изображений – *RS*-анализа [3]. Сегодня это наиболее популярный и эффективный способ обнаружения данных, скрытых 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 чрезвычайно эффективен [8] и, хорошо зарекомендовал себя на мировом рынке средств стегоанализа [7], применяется практически везде, где выполняется поиск данных, скрытых с использованием стеганографических методов защиты. *RS*-анализ достаточно сложен 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. Цель выполнения этих исследований – 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 вероятно-

стью пяти 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 считаются изображения с вероятностью более 10 процентов. Если будем иметь метод обработки изображений, позволяющий уменьшать результаты *RS*-анализа, то можем обработать изображение, уменьшив вероятность сокрытия данных внутри этого изображения, скажем, до двух процентов. Теперь можем вставить внутрь изображения столько данных для сокрытия, чтобы вероятность снова возросла до пяти 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 табл. 1. Этот набор с 1960 изображениями не должен в массе своей вызвать подозрений у средств обнаружения данных, скрытых стеганографической.

Рассмотрим данные, приведенные в табл. 1. 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 ложноположительных 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), предназначенный для выделения и подчеркивания границ изображений, а четвертый – фильтр *Defocus* (Расфокусировка) – для уменьшения резкости изображения. *EdgeDetect* – фильтр (Определение границ) – изменяет яркость границ объектов, 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* (Больше 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*, предназначен-

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*	*Sharpen More*	*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	

ный для сокрытия данных в изображении стеганографическим путем. Он не считается надежным [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 три 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 табл. 2 предложены 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:

$$V_{av} = \frac{\sum_{i=1}^{n} [(Pb)]_i - P_i}{n}, \qquad (1)$$

где V_{av} – усредненный результат влияния вносимых изменений на весь набор изображений, n – количество изображений в наборе, подвергавшемуся анализу, P_i – 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 означают 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 табл. 2 и рис. 3, результаты *RS*-анализа изображений, обработанных с использованием различных вариантов методов воздействия (фильтров и др.), можно разделить

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	

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, негативно влияющим 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 влияющих на результаты *RS*-анализа. К ним относятся только *Gaussian Blur* и *Punch* (особенности работы фильтра *Remove Channel* и его неприменимость описаны ранее). При этом изменения, вносимые фильтром *Punch*, оказываются малозначимыми. А положительные изменения проявляются не на всех изображениях, поэтому его применение в качестве средства для подготовки файла–контейнера для дальнейшего сокрытия информации внутри его – бесперспективно. Таким образом, единственный фильтр, позволяющий стабильно уменьшать результаты *RS*-анализа, – *Gaussian Blur*. Его применение дает положительный эффект независимо от типа и размера изображения, процентное значение улучшения зависит от начального значения *RS*-анализа изображений.

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

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 нуля настолько мало, что этим различием можно пренебречь – оно не позволит применить их для улучшения защиты данных от стегоанализа.

Заключение. Разработанный модульный проблемно-ориентированный комплекс стегоаналитических исследований позволяет оператору гибко изменять направления сбора статистики и экспортировать полученные данные.

Благодаря такому комплексу получены новые результаты в области сокрытия данных стеганографическими методами в изображениях: обнаружены ограничения метода *RS*-CA для многих классов изображений, доступных в сети Интернет, поскольку есть большая вероятность ложноположительных срабатываний; предложены способы обхода метода *RS*-CA; обнаружен максимально допустимый объем безопасного внесения данных, который составляет два процента, а удовлетворительный уровень не должен превышать

пяти. Объемы встраивания пяти–десяти процентов – подозрительны, а более 10 – маловероятны для необработанных цифровых фотографий.

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

Выбор оптимальных параметров этого фильтра в зависимости от параметров изображения и количества информации, которое необходимо скрыть внутри контейнера, – перспективно для дальнейших исследований.

1. *Королёв В.Ю., Полиновский В.В., Герасименко В.А.* Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей // УСиМ. – 2011. – № 1. – С. 79–87.
2. *Корольов В.Ю., Поліновський В.В., Герасименко В.А. RS*-стегоаналіз. Принципи роботи, недоліки та концепція метода його обходу // Вісн. Вінницького політех. ін-ту. – 2010. – № 6. – С. 66–71.
3. *Корольов В.Ю., Поліновський В.В., Герасименко В.А.* Визначення можливостей *RS*-стегоаналізу для дослідження статистичних властивостей зображень // Вісн. Хмельн. нац. ун-ту. – 2010. – № 4. – С. 102–110.
4. *Корольов В.Ю., Поліновський В.В., Герасименко В.А.* Стеганографічна персоналізація інформації на базі ПК // Вісті Акад. інж. наук України. – 2009. – № 2 (39). – С. 18–24.
5. *Планування* досліджень методів стеганографії і стегоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко та ін. // Вісн. Хмельн. нац. ун-ту. – 2011. – № 4. – С. 187–195.
6. *Інформаційна* технологія для дослідження методів стеганографії і стегоаналізу / В.В. Поліновський, В.Ю. Корольов, В.А. Герасименко та ін. // Міжвуз. зб. «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». – 2011. – **5**. – С. 236–242.
7. *Комплекс* статистичних досліджень для стегоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко та ін. // Математичне та комп'ютерне моделювання. – Зб. наук. пр.: Сер. Технічні науки. – 2011. – **5**. – С. 134–149.
8. *Корольов В.Ю., Поліновський В.В., Герасименко В.А.* Дослідження стійкості НЗБ-стеганографії до *RS*-аналізу // Матеріали IV міжнар. конф. «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП – 2009)». Ч. 1. – 2009. – С. 53.
9. *Niels Provos* Defending Against Statistical Steganalysis // 10th USENIX Security Symp. Aug. 13–17, 2001, DC, Washington.

Поступила 07.07.2014

Тел. для справок: +38 044 526-5585, 564-0472, 067 421-9651 (Киев, Мелитополь)

E-mail: *V.Polinovskyi@tau-systems.org.ua, office@tsaa.org.ua, dshv937@meta.ua, romantic84@gmail.com, gerasymenko_v@mail.ru*

Окончание статьи А.П. Костенко и др.

Специалист–маркетолог или менеджер–маркетолог должен владеть знаниями по кибернетическому маркетингу как важной составляющей современного образования по управлению маркетингом. Таким образом, нужно обеспечить развитие у специалиста-менеджера по маркетингу системного мышления, осознание необходимости применения кибернетических принципов к задачам управления и принятия решений, к исследованию сложных маркетинговых процессов и решения слабоструктурированных проблем.

Разработка и использование комплекса моделей профессиональных знаний руководителей предприятий создаст возможность сократить время для принятия рационального маркетингового решения. Использование в маркетинговых процессах моделей профессиональных знаний руководителей по маркетингу предусматривает одновременное создание динамичной модели получения знаний специалистов–маркетологов, что содействует организации системы накопительных моделей маркетинговых ситуаций.

Заключение. Предложенная концепция сближения маркетинговой системы предприятия и системы маркетинговой информации нуждается в значительных усилиях ученых различных специальностей, в том числе специалистов в области экономической кибернетики и математического моделирования сложных слабоструктурированных рыночных задач.

Рассмотренная концептуальная модель кибернетического маркетинга, который в отличие от существующих информационных технологий, основанных на регрессионно-корреляционных моделях, методах линейного программирования и жестких алгоритмах принятия решения, использует формализованные кибернетические принципы, и в дальнейшем позволит использовать категорно-функторные модели, теорию нечетких множеств и нечеткой логики для автоматизации решения задач маркетинга как непосредственно на предприятии, так и на рынке, что повысит его конкурентоспособность до уровня европейских стандартов.

УДК 004.056:621.397
Исследование методов интеллектуального стеганографического сокрытия данных в изображениях до и после их изменения / Полиновский В.В., Королев В.Ю., Малкина В.М., Огурцов М.И., Герасименко В.А. // УСиМ. – 2014. – № 4. – С. 84–92.

Предложена концепция стеганокриптографической персонализации информации на основе аппаратно-программной системы аутентификации пользователей. Показано, что реализация стеганографических программных средств с предварительной обработкой изображений на основе размытия по Гауссу с индикацией угрозы обнаружения скрытых данных позволяет повысить уровень персонализации информации с ограниченным доступом. Ил.: 3. Табл.: 2. Библиогр.: 9 назв.

UDC 004.056:621.397
Study of Steganography Mining Techiques of Data Hiding in Images Before and After the Changes / Polinovskiy V.V., Korolyov V.Yu., Malkina V.M., Ogurcov M.I., Gerasimenko V.A. // USiM. – 2014. – N 4. – P. 84–92.

The concept steganographiccryptographic personalization of information based on the hardware-software system of user authentication is presented. The implementation of the steganographic software increases the level of personalization of information with the restricted access. Figs: 3. Tables: 2. Refs: 9 titles.

Наши авторы

Белоцерковская Ольга Юрьевна – ассистент, Кременчугский ун-т экономики, информационных технологий и управления (Кременчуг)

Белошапкин Виктор Клавдиевич – к.ф.-м.н., МНУЦИТиС НАН и МОН Украины (Киев)

Богаенко Всеволод Александрович – к.т.н., ИК им. Глушкова НАН Украины (Киев)

Бодянский Евгений Владимирович – д.т.н., Харьковский национальный университет радиоэлектроники.(ХНУРЕ) (Харьков)

Винокурова Елена Анатольевна – д.т.н., ХНУРЕ (Харьков)

Герасимеико Вячеслав Анатольевич – м.н.с., ИК им. Глушкова НАН Украины (Киев)

Глибовец Андрей Николаевич – к.ф.-м.н., НаУн-т «Києво-Могилянська академія» (НаУКМА) (Киев)

Дехтярук Николай Трофимович – к.т.н., Междунар. ун-т «Украина» (Киев)

Забара Станислав Сергеевич – д.т.н., ун-т «Украина» (Киев)

Королев Вячеслав Юрьевич – к.т.н., ИК им. Глушкова НАН Украины (Киев)

Костенко Александр Петрович – к.т.н., Кременчугский ун-т экономики, информационных технологий и управления (Кременчуг)

Костенко Тамара Ивановна – ассистент, Кременчугский ун-т экономики, информационных технологий и управления (Кременчуг)

Кошкина Наталия Васильевна – к.ф.-м.н., ИК им. Глушкова НАН Украины (Киев)

Кузьмеико Борис Владимирович – д.т.н., Ин-т угольных энерготехнологий НАН Украины (Киев)

Лисецкий Юрий Михайлович – к.т.н., Дочернее предприятие «ЭС ЭНД ТИ УКРАИНА» (Киев)

Малкина Вера Михайловна – д.т.н., Таврический гос. агротехнологический ун-т (Мелитополь)

Марченко Ольга Алексеевна – к.ф.-м.н., ИК им. Глушкова НАН Украины (Киев)

Нагорная Алла Николаевна – к.ф.-м.н., Украинский гос. ун-т финансов и междунар. торговли (Киев)

Огурцов Максим Игоревич – м.н.с., ИК им. Глушкова НАН Украины (Киев)

Пелешко Дмитрий Дмитриевич – д.т.н., Нац. ун-т «Львівська політехніка» (Львов)

Полиновский Вячеслав Васильевич – к.т.н., ун-т «Украина» (Киев)

Ревунова Елена Георгиевна – к.т.н., МНУЦИТиС НАН и МОН Украины (Киев)

Сальников Николай Николаевич – к.т.н., Ин-т космических исследований НАН и ГКА Украины (Киев)

Самойленко Татьяна Анатольевна – к.ф.-м.н., ИК им. Глушкова НАН Украины (Киев)

Сирик Сергей Валентинович – аспирант, НТУУ «КПИ» (Киев)

Ходаковский Николай Иванович – к.т.н., ИК им. Глушкова НАН Украины (Киев)

Цололо Сергей Алексеевич – к.т.н., ГВУЗ «Донецкий нац. техн. ун-т» (Донецк)

Зміст

Contents

Научные консультанты А.В. Палагин, Е.А. Савченко

Научные редакторы С.П. Чарчиян, Н.И. Савенко

Компьютерная группа С.К. Горбунов, Н.С. Сташкова

Журнал входит в Перечень периодических изданий,
рекомендованных ВАК Украины для опубликования результатов диссертаций
на соискание степени доктора физико-математических, технических и экономических наук

Принято к печати ученым советом МНУЦИТиС

Свидетельство о регистрации КВ № 17215 – 5985 ПР от 27.10.2010

Подп. в печать 18.08.2014. Формат 84 × 108/16. Бум. офсетная. Усл. печ. листов 4,0. Уч.-изд. листов 5,58. Печать офсетная. Тираж 150 экз. Зак. № 3980.

Отпечатано в типографии Изд. дома «Академпериодика», 01004, Киев-4, ул. Терещенковская, 4.
Свидетельство субъекта издательской деятельности ДК № 544 от 27.07.2011.

Оригинал-макет журнала изготовлен в редакции с помощью настольной издательской системы.

ISSN 0130- 5395

Национальная академия наук Украины | Международный научно-учебный центр информационных технологий и систем | Институт кибернетики им. В.М. Глушкова | Фонд Глушкова

УСиМ

УПРАВЛЯЮЩИЕ СИСТЕМЫ И МАШИНЫ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Международный научный журнал

№ 4 июль — август 2014

Основные темы выпуска:

Стеганоанализ изображений в формате *jpeg*

●

Метод решения дискретных некорректных задач

●

Решение задачи распределенного индексирования

ISSN 0130-5395

Control Systems and Computers