УДК 004.056

В.Ю. Королев, В.В. Полиновский, В.А. Герасименко

Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей

Предложена концепция стегано-криптографической персонализации информации на основе аппаратно-программной системы аутентификации пользователей и протокола передачи данных с повышенной степенью защиты. Показано, что реализация стеганографических программных средств на базе флеш-накопителей позволяет повысить уровень персонализации информации с ограниченным доступом.

A concept of stegano-cryptographic personalize information based on a hardware-software system, user authentication and data transmission protocol with a high degree of protection is suggested It is shown that the implementation of the steganographic software on the basis of flash-storage can increase the level of information personalization with a restricted access.

Запропоновано концепцію стегано-криптографічної персоналізації інформації на основі апаратно-програмної системи автентифікації користувачів і протоколу передачі даних з підвищеним ступенем захисту. Показано, що реалізація стеганографічних програмних засобів на базі флеш-накопичувачів дозволяє підвищити рівень персоналізації інформації з обмеженим доступом.

Введение. Развитие электронных коммуникаций и Интернет-сервисов происходит в условиях постоянного роста количества некомпенсированных угроз их безопасности. Сообщения о взломе крупных ИТ-систем и краже данных публикуются в электронных СМИ регулярно. Поскольку сегодня несанкционированный доступ к конфиденциальной информации стал одной из составляющих международного криминального бизнеса, защита информации должна быть постоянно выполняемой функцией, интегрированной с бизнес-процессами организации, а соответствующие аппаратно-программные средства требуют совершенствования.

Оценка современного состояния средств стеганографической защиты информации

В течение последних 15–20 лет создано и разрабатывается множество методов и алгоритмов стегано-криптографической защиты информации [1–6], а также соответствующего программного обеспечения (ПО) для персональных компьютеров (ПК). В то же время интерес пользователей к программам стеганографической защиты информации существенно снизился, что связано, в том числе и с определенным прогрессом в области стеганоанализа, построенного на методах дуальной статистики [5, 6].

Анализ рынка продуктов для защиты информации показывает, что за последние четыре года не появилось ни одного нового успешного инновационного коммерческого программного продукта стегано-криптографической защиты. Известные фирмы–производители либо пополняют стеганографические программы дополнительными инструментами компьютерной безопасности, либо осваивают смежные области информационных технологий, отводя стеганографическим средствам незначительную роль.

Большинство стеганографических программных продуктов доступных в Интернете используют метод наименее значимых бит (НЗБ) для сокрытия информации в контейнере. В то же время известно нéсколько методов стеганоанализа, построенных на основе дуальной статистики, которые позволяют не только определить наличие в изображéнии данных, скрытых с помощью НЗБ-алгоритмов, но и дать оценку объему скрытой в контейнере информации [5, 6]. Поэтому простые стеганографические методы не обеспечивают тайну передачи данных, т.е. по степени защиты информации не превосходят криптографические продукты, что и объясняет падение интереса к ним. Решение про-

блемы требует создания новых аппаратно-программных средств стегано-криптографической защиты информации.

Постановка задачи

Наряду с широко распространенными средствами защиты, базирующимися на методах криптографии, известны методы стеганографической защиты информации, основной задачей которых является сокрытие самого факта существования или передачи зашифрованных данных с помощью носителей, не вызывающих подозрений у противника.

Использование стеганографических средств на базе аппаратно-программных устройств персонализации информации, позволяющих скрыть факт работы с такими программами, обеспечивает существенное усиление криптографической защиты данных как для корпоративных ПК, так и для ПК, принадлежащих физическим лицам.

Эксплуатационные особенности средств НЗБ-стеганографии

Опыт коммерциализации и практического использования программ НЗБ-стеганографии с изображениями либо со звуковыми файлами показывает, что эти программы – *индивидуальные средства сокрытия информации*. Действительно, за последние 20 лет существования стеганографических программ не было примера их массового долговременного внедрения в информационную сеть организаций, интеграции с бизнес-процессами либо построения на их основе действующих протоколов скрытой передачи данных. Это можно объяснить следующими причинами.

• Широкомасштабное развертывание стеганографических средств в корпоративной среде противоречит сути их применения – секретности использования, так как подобную деятельность сложно долго сохранить в тайне. Действительно, если противнику известно, что для передачи данных применяются стегано-криптографические программы, то эффект от их использования для защиты информации значительно снижается.

• Работа со стеганографическими средствами предполагает, по крайней мере, понимания различий между форматами графических файлов, а также базового уровня знаний в области защиты информации для устранения угрозы потери конфиденциальных данных по причине ошибок, связанных с человеческим фактором.

• Активное использование стеганографических программ требует защищенного хранения большого массива уникальных или малоизвестных фотографий либо наличия у пользователя навыков по выбору из сети Интернет цифровых носителей, соответствующих поставленным задачам. В противном случае теряется скрытность стеганографии.

• НЗБ-стеганография в сравнении с криптографией существенно ограничивает пропускную способность канала связи, так как в целях скрытности передачи данных не рекомендуется заполнять изображения–носители более чем на 10% емкости НЗБ-уровня. Этим объясняется отсутствие коммерческих протоколов скрытой передачи данных на базе НЗБ-стеганографии.

Использование стеганографического ПО при соблюдении мер компьютерной безопасности имеет равнозначную защищенность информации с ограниченным доступом при работе на корпоративных ПК, ноутбуках или при запуске с внешнего накопителя с аппаратно-программным шифрованием потока данных. С другой стороны, флеш-накопители, даже в корпоративной среде, – это персонализированные устройства хранения информации.

Поэтому совмещение флеш-накопителя и сервисного портабельного программного обеспечения (пПО) [7, 8], в том числе стеганографического, представляется естественным с позиции повышения функциональности и эффективности использования устройств хранения данных и ПО, особенно для таких категорий служащих, как мобильные сотрудники, командированные или надомные работники. При этом флеш-накопители с перестраиваемым ключом–аутентификатором имеют ряд преимуществ при решении задач компьютерной безопасности, в частности компьютерной стеганографии.

Уязвимость средств стегано-криптографической защиты информации через атаки на открытые аппаратно-программные платформы

Сценарии использования стеганографических средств, рассматриваемые в литературе [1, 4], предполагают отправку заполненного контейнера по электронной почте или другой способ непосредственной передачи файлов от отправителя к получателю. В то же время подавляющее большинство известных случаев крупных краж данных связано с хакерским взломом корпоративных сетей и серверов баз данных либо злонамеренными действиями инсайдеров, а не с перехватом электронной деловой корреспонденции на стороне отправителя или получателя. Поэтому организация стегано-криптографической защиты информации с ограниченным доступом на компьютеризованном рабочем месте, подключенном к локальной корпоративной сети, или на ноутбуке мобильного сотрудника представляет собой актуальную научно-прикладную проблему, поскольку может являться последним труднопреодолимым рубежом технической защиты высококонфиденциальной коммерческой информации.

Однако использование существующих средств стеганографической защиты данных непосредственно на корпоративном ПК или ноутбуке имеет недостаток с точки зрения безопасности информации, заключающийся в необходимости их инсталляции в операционную систему. Современные специализированные системные программные средства способны восстановить удаленную с жесткого диска информацию [9], если она не удалена сертифицированными программами стирания, а также обнаружить следы использования стеганографических программ [10]. Такие действия позволяют идентифицировать стеганографические программы [11, 12], чтобы извлечь данные из контейнера и приступить к их дешифровке. Таким образом, при использовании в предлагаемых на рынке стеганографических программных средствах стойкость стеганографических и криптографических систем мало чем отличается, т.е. обеспечивается длиной ключа алгоритма шифрования.

Скомпенсировать уязвимость программных стеганографических средств может переход к реализации систем на базе персонализированных накопителей данных [13–15], а также безопасно настроенного портабельного программного обеспечения [7, 8], запускаемого с этих устройств, т.е. переход к специализированным корпоративным аппаратно-программным решениям с аутентификацией пользователя, не оставляющего следов работы в открытых операционных системах.

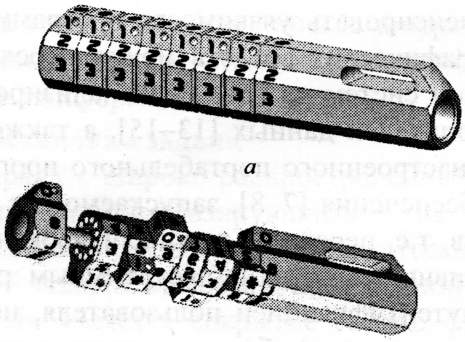
Очевидно, что для нормальной работы таких систем необходимо проводить процедуры идентификации и аутентификации пользователей или же ввода кодовой последовательности как одного из параметров при стеганографическом сокрытии информации.

В то же время, несмотря на наличие достаточно большого количества устройств идентификации и аутентификации пользователей, а также ввода кодовой последовательности, наиболее популярным остается клавиатурный метод введения ключевой информации. При этом многие используют простые пароли для доступа к информационным ресурсам. Следовательно, усиление парольной защиты – актуальная проблема для разработчиков систем доступа к информационным ресурсам.

Универсальный ключ-аутентификатор

Авторами для решения таких задач предлагается использовать разработанный в Центре таймерных вычислительных систем ключ–аутентификатор и универсальный считыватель для него [16] (рис. 1), что позволяет создать более совершенный способ аутентификации и ввода кодовой информации.

Техническим результатом данной разработки является увеличение емкости кодовой информации за счет изменения формы аутентификатора, увеличения количества положений секретных элементов относительно считывателя с одновременным увеличением количества видов секретных элементов, а также повышение удобства пользования аутентификатором за счет внедрения 10–12-значной буквенно-цифровой системы запоминания кода.



а

б

Рис. 1. Новый отечественный ключ-аутентификатор: *а* – нейтральная форма; *б* – рабочая

Кроме того, изменение формы аутентификатора осуществляется поворотом секретного элемента на определенный угол и фиксацией его в этом положении либо заменой, по меньшей мере, одного секретного элемента на другой. При этом аутентификатор может иметь так называемую нейтральную форму, когда все секретные элементы занимают такое положение относительно друг друга и относительно основы, в котором все внешние плоскости элементов и основы совпадают (рис. 1,*а*). В такой нейтральной форме удобнее сохранять аутентификатор, поскольку он не имеет резких выступов или впадин вдоль оси. Это удобство вынуждает пользователя всякий раз после ввода кодовой информации с аутентификатора, имеющего измененную форму, перестраивать его в нейтральную форму, что в свою очередь исключает возможность овладения кодом другим лицом в случае потери, кражи или копирования. Нейтральная форма аутентификатора может использоваться как одна из кодовых комбинаций.

Изменение формы аутентификатора достигается также заменой, по меньшей мере, одного секретного элемента определенного типа на другой. Пользователь может даже собрать свой аутентификатор, нанизав какие угодно секретные элементы в любом порядке, что позволяет создавать разные типы аутентификаторов, не похожие друг на друга, и увеличивает количество возможных кодовых комбинаций. Кроме того, можно дополнительно изменять код путем открывания (закрывания) или частичного закрывания (открывания) каналов для прохождения сигнала, предварительно сделанных в секретных элементах. Базовый ключ содержит 2^{192} комбинаций.

Особенности предложенного ключа-идентификатора:

- осуществление двухфакторной (и более) аутентификации пользователя;
- возможность в любое время быстро (за несколько секунд) и самостоятельно, без применения специальных устройств, изменить кодовую комбинацию на ключе;
- использование одного ключа для неограниченного количества объектов со встроенным считывателем;
- ключ может быть перекодирован требуемое число раз;
- потеря устройства ничем не угрожает, поскольку набранный ключ всего лишь носитель кода в момент ввода и при необходимости может быть заменен другим таким же ключом. Пользователю достаточно будет набрать на секретных элементах нового устройства свою кодовую последовательность;
- обеспечивается значительное количество кодовых комбинаций (в степени не менее третьего порядка);
- ключ высоконадежен, поскольку устойчив к воздействию механических факторов, загрязнений, влаги, температуры, статического электричества, электрошокеров;
- ключ устойчив к электромагнитным излучениям (информацию на ключе нельзя стереть, направив на него мощное излучение), а сам не является излучателем, поэтому несанкционированные попытки считывания с помощью дистанционных электромагнитных систем считывания информации не представляют угрозу для безопасности;
- код вводится быстро и скрытно.

Исходя из вышеизложенного, можно утверждать, что интеграция аппаратно-программного комплекса персонализации информационных ресурсов с высокоуровневыми сервисными программами защиты конфиденциальных данных, требующими ввода секретных паролей, – важная научно-практическая проблема.

Интеграция средств персонализации устройств хранения данных со стеганографическим ПО

Флеш-накопители стали массовыми устройствами хранения личной и деловой информации во всем мире, поэтому дополнение таких устройств аппаратно-программными средствами аутентификации пользователей и защиты информации может существенно повысить безопасность корпоративных информационных ресурсов. Аутентификация пользователей выполняется с помощью персонализированного ридера, встроенного во флеш-накопитель, микроконтроллер которого также генерирует криптостойкие кодовые комбинации для программ защиты информации (в том числе для стеганографических приложений) на основе как стохастических, так и псевдослучайных последовательностей (рис. 2) [15].

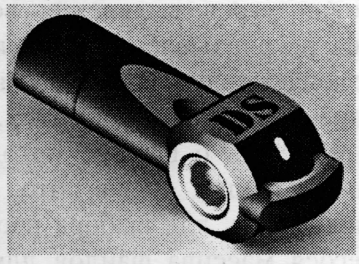


Рис. 2. Модель флеш-накопителя с ридером ключа-аутентификатора

В сравнении с современными системами персонализации информационных ресурсов, защиты информации и идентификации/аутентификации пользователей предлагаемая разработка, а именно персонализированный флеш-накопитель с ридером, реализующим многофакторную аутентификацию, отличается надежностью и не требует вложения значительных средств.

Безопасность операций передачи ключа между компьютером и ридером базируется на протоколе передачи информации с повышенной степенью защиты [13–15] и событийно-условной модели работы пользователя со стеганографическим ПО для персонализированного флеш-накопителя [2].

Таким образом, использование программ стеганографической защиты информации вместе с персонализированным устройством хранения, ключом-аутентификатором и аппаратно-программным шифрованием позволяет повысить уровень защиты конфиденциальной информации как для корпоративного, так и личного использования.

Стеганоанализ изображений методом дуальной статистики

RS-анализ [5] является развитием стеганоанализа на базе методов дуальной статистики [6], в частности – обобщением метода анализа пар значений (*Sample Pairs*) [5, 6] и подобных этому методу. Сегодня *RS*-анализ есть одним из наиболее точных методов обнаружения информации, скрытой в изображениях с помощью НЗБ-стеганографии и представленной в области пространственных координат. Поэтому современная система стегано-криптографической защиты информации должна иметь средства защиты от атак, основывающихся на известной математической модели контейнера [4].

Для большинства естественных изображений НЗБ-уровень считается случайным, поскольку он не содержит какой-либо легко распознаваемой структуры. Поэтому классические характеристики случайных процессов и оценки, применяемые к НЗБ-уровню, не могут надежно отличить естественные шумы от псевдослучайно встроенных стегобитов сообщения, зашифрованного методами криптографии, особенно если его длина составляет менее одного процента емкости контейнера. Однако НЗБ-уровень, даже если и выглядит случайным, связан с другими битовыми уровнями нелинейной зависимостью, на чем и основывается *RS*-стеганоанализ.

Недостатки *RS*-анализа

Разработчики *RS*-анализа предполагают в своих работах [5, 6], что противник будет использовать современные цифровые фотографии, характеризующиеся низким уровнем шумов, технических артефактов регистрации и сжатия, а также изображения без сложной предпечатной подготовки и последовательности дизайнерских операций над ними. *RS*-анализ может легко обнаружить факт сокрытия сообщений, встроенных в этот класс изображений, и достаточно точно оценить его длину (с точностью до одного бита на пиксель [5]), которая рассчитывается на основании анализа отличий НЗБ-плоскости и сдвинутой НЗБ-плоскости стеганообраза.

Экспериментально авторами установлено, что для изображений, обработанных методами предпечатной подготовки (например, для публикации в сети Интернет), для изображений с большим количеством малых объектов или содержащих мелкие текстуры, либо шумовые паттерны, а также для оцифрованных образов из разных источников и носителей старше 10–15 лет, для снимков с массовых цифровых фотоаппаратов («мыльницы» или камерофоны) *RS*-анализ не гарантирует верное обнаружение стегобитов и демонстрирует ложноположительное обнаружение существенного количества скрытой информации. Из 3230 изображений, взятых для проведения эксперимента, 686 изображений (т.е. 21%) содержали ложноположительно выявленные стеганобиты на уровне выше двух процентов, из них 481 – на уровне от двух до пяти процентов (15% от общего количества), 156 изображений (на уровне 5–10%) – около 5% фотографий и 49 изображений (1,5% ложноположительно обнаруженных стегобитов).

Очевидно, что для *RS*-анализа критическое значение имеет выбор порогового уровня стохастического возмущения в наименее значимых битах для принятия решения о наличии стегобитов. Этот пороговый уровень неодинаков для различных классов изображений и многообразия объектов регистрации, сцен и фона, поэтому для многих изображений, доступных в Интернет, *RS*-анализ демонстрирует ложное определение встроенных сообщений большого размера. Решить эту проблему можно *выбором порогового значения* на основании статистических исследований крупных выборок изображений.

Такой вывод подтверждают результаты численных экспериментов на больших выборках файлов: для первой выборки объемом 43598 файлов усредненный процент ложных стегобитов составил около 1–2%, а для второй размером 6080 файлов – около восьми. Выборки представляли собой наборы фотографий для дизайнеров. Причем файлы первой группы имели разрешение более девяти мегапикселей, файлы второй группы – порядка одного–трех мегапикселей. Различие величин ложно обнаруженных стегобитов для двух выборок подтверждает сообщение разработчиков метода *RS*-стеганоанализа о зависимости порога разрешения метода от размера изображения.

Приведенные величины ложноположительно обнаруженных стегобитов можно использовать для грубого отсеивания подозрительных файлов. Очевидно также, что дополнение стеганографического ПО процедурами индикации оценки скрытности на основе алгоритмов стеганоанализа позволяет пользователю контролировать скрытность данных и снижает уязвимость от атак, основывающихся на известной математической модели контейнера [4].

Методы обхода *RS*-анализа

Известные стеганографические программные продукты не предоставляют пользователю средств оценки защищенности скрытых данных. В то же время простое добавление панели в рабочую среду программы с цветовой индикацией уровня угроз выявления встроенной информации, рассчитываемой алгоритмом *RS*-анализа, позволяет пользователю осознанно принимать решение об объеме данных, внедряемых в контейнер, и о выборе метода обхода *RS*-анализа. Очевидно также, что *RS*-анализ можно использовать для выбора изображений из имеющегося массива файлов для стеганографического сокрытия информации.

Метод предварительного сглаживания контейнера. На основании приведенного описания можно предложить очевидный метод обхода *RS*-анализа. Для этого нужно уменьшить количество сингулярных групп контейнера [5], а затем встроить в обработанное изображение сообщение, размер которого не вызовет подозрения у стеганоаналитика. Сингулярные группы пикселей для незаполненного контейнера обусловлены шумом, артефактами регистрации, резкими переходами яркости, контурами и т.п. Поэтому сглаживание изображения с помощью фильтрации – низкочастотной, медианной и так далее уменьшает количество сингулярных групп и, следовательно, снижает первоначальный процент ложноположительно обнаруженных стегобитов до нуля.

Для проверки предлагаемого метода взяты изображения, полученные из разных источни-

ков (фотографии, выполненные с помощью разных цифровых камер и мобильных телефонов), при этом главное условие эксперимента состояло в получении изображения не из сетей общего доступа, а непосредственно из цифровых отображающих систем. Выборка из 1700 изображений обработана существующими фильтрами (усиление цвета, уменьшение/увеличение резкости, размытие и т.п.) и осуществлен стеганоанализ, результаты которого приведены в табл. 1.

Таблица 1. Количество изображений в группах, разбитых по величинам ложноположительно выявленных стегобит *RS*-стеганоанализа после выполнения фильтрации

Название фильтра и классификация операции		Количество изображений, %			
		2% – max	2–5 %	5–10 %	10% – max
Оригинал		19	13	4,6	1,7
Огрубляющие фильтры	Малтиплай	26	19,2	4,6	2
	Оверлей	25	20	4	1
	Хайпас	20	13	7	2
Маскирующие фильтры	Медианный	0,06	0,06	–	–
	Гауссов	0,35	0,35	–	–

В ходе эксперимента обнаружено также, что изображения достаточно легко разделить на три принципиально разные группы:

- обработка которых *существенно* влияет на *RS*-коэффициент;
- обработка которых *мало* влияет на *RS*-коэффициент;
- изображения, при обработке которых одни фильтры влияют на *RS*-коэффициент, а другие – нет.

Исследования метода *RS*-стеганоанализа продолжаются в направлении расширения номенклатуры фильтров и комбинаций их применения.

Алгоритм кодирования пар байтов. Рассмотрим новый стеганографический алгоритм кодирования пар байтов (КПБ). Пусть байты значением Z соответствуют нулевому стегобиту, а байты значением $Z + 1$ – единичному стегобиту (рис. 3). Тогда двоичную последовательность стегобит секретного сообщения можно отобразить на множество пар байтов, не имеющих общих элементов. Причем значения байтов будут соответствовать нулевым и единичным стегобитам, а их индексы относительно начала массива – чередованию стегобитов (рис. 6). В обобщенном виде алгоритма между парами байтов можно установить смещение D.

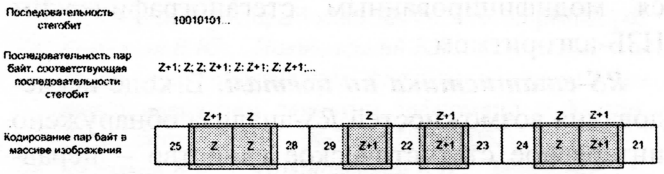


Рис. 3. Иллюстрация работы алгоритма ПКБ для простейшего случая $D = 1$

Для простейшего случая $D = 1$, однако D можно установить как произвольное целое число $1 < D < 255$, а также изменять его по алгоритму. Таким образом, $Z + D \to 0_2$, $Z + 1 + D \to 1_2$, где $Z = 0, 1, \ldots, 255$; $D = 1, 2, \ldots, 254$.

В работе [6] показано, что сдвиги $0 \leftrightarrow 1$, $2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$; $-1 \leftrightarrow 0$, $1 \leftrightarrow 2$, $3 \leftrightarrow 4, \ldots$ $\ldots, 255 \leftrightarrow 256$ соответствуют внесению в НЗБ контейнера скрытого сообщения, а сдвиги $0 \leftrightarrow 2$, $3 \leftrightarrow 4, \ldots, 253 \leftrightarrow 255$ трактуются методом как естественный шум. Меняя параметры Z и D, можно добиться 50%-го заполнения контейнера без явных признаков внесения стегобит для *RS*-стеганоанализа.

Таким образом, базой для построения концепции разработки более эффективного метода стеганографического сокрытия информации является внесение изменений, не подпадающих под указанные ранее сдвиги. Очевидно, что такое сокрытие информации будет трактоваться *RS*-анализом как шум.

Для проверки этого предположения проведены численные эксперименты с различными значениями поворота, которые подтвердили уже названные допущения. Если принять за 100% емкости контейнера полное его заполнение по методу НЗБ-стеганографии, когда в каждом байте содержится один стегобит, то при заполнении контейнера от одного до 100% получим практически такую же оценку по методу *RS*-анализа [5]. Однако при заполнении по алгоритму КПБ *RS*-анализ выдает значения, которые с точностью до одного–двух процентов равны первоначальному значению для незаполненного контейнера. Отметим, что такое встраивание сообщений не выявляет и метод *Sample Pairs*. Таким образом, *RS*-анализ в своем запатенто-

ванном виде не распознает внесение стегобитов, выполненное в соответствии с рассматриваемым алгоритмом, который, по сути, является модифицированным стеганографическим НЗБ-алгоритмом.

RS-статистика по цветам. В ходе исследования возможностей *RS*-анализа обнаружено интересное статистическое свойство – неравномерность значения ложноположительно выявленных стегобитов в разных каналах цветности незаполненного контейнера. Численные эксперименты проведены на двух выборках из 43598 и 6080 файлов разного происхождения. Обозначим символами *R,G,B* значение (в процентах) обнаруженных стегобитов в красном, зеленом и голубом каналах цветности соответственно. В результате экспериментов были получены следующие соотношения (см. табл. 2). Видно, что соотношения между цветами $R > B > G$, $B > R > G$, $B > G > R$, соответствующие ложноположительно выявленным стегобитам, встречаются чаще других комбинаций. Подсчет относительного количества неравенств для обеих выборок, где какой-либо из цветов имеет максимум по ложноположительно выявленным стегобитам, дает следующий результат (см. табл. 2), а подсчет относительного количества неравенств для обеих выборок, где какой-либо из цветов имеет максимум по ложноположительно выявленным стегобитам, дает следующий результат (см. табл. 3).

Таблица 2. Статистика обнаружения стегобитов для различных цветовых соотношений в соответствии со значением *RS*-анализа

Неравенство	№ 1, %	№ 2, %
$R > G > B$	13,46	16,12
$R > B > G$	18,26	18,95
$G > R > B$	8,29	11,23
$G > B > R$	9,43	10,95
$B > R > G$	21,99	19,05
$B > G > R$	19,43	16,97
$R = G > B$	1,03	0,86
$B > R = G$	2,36	1,33
$G = B > R$	1,11	0,97
$R > G = B$	1,72	0,92
$B = R > G$	1,28	1,25
$G > B = R$	1,35	0,97
$R = G = B$	0,28	0,43

Таким образом, для голубого и красного цветов имеет место превышение относительного количества ложноположительно обнаруженных стегобитов на 10–20% в сравнении с зеленым каналом цветности.

Таблица 3. Максимумы цветов в частотах неравенств

Название канала цветности	Значение максимума, %	
	Выборка 1	Выборка 2
Голубой (*B*)	43,78	37,35
Красный (*R*)	33,44	35,99
Зеленый (*G*)	19,07	23,15

Таким образом, для голубого и красного цветов имеет место превышение относительного количества ложноположительно обнаруженных стегобитов на 10–20% в сравнении с зеленым каналом цветности.

Полученные статистические данные можно использовать для управления параметрами алгоритма НЗБ-стеганографии при встраивании данных в каналы изображения после сглаживания, а также для более точного определения порога обнаружения стегобитов в контейнере и для проверки больших массивов файлов на предмет сокрытия в них информации стеганографическими методами.

Заключение. Повсеместное использование флеш-накопителей для хранения как личных файлов, так и документированной деловой информации обусловлено компактными размерами и большим объемом их памяти, а также простотой эксплуатации при доступной массовому пользователю цене. При этом проблему персонализации хранимых на флеш-накопителях данных можно решить путем интеграции аппаратно-программных средств защиты информации, аутентификации пользователей флеш-накопителей, ввода ключей шифрования, а также стегано-криптографических методов.

Кроме того, дополнение стеганографических средств процедурой оценки (например, с помощью *RS*-стеганоанализа) уровня угроз обнаружения данных, встроенных в носитель, помогает пользователю контролировать степень скрытности конфиденциальной информации.

1. *Задирака В.К.* Комп'ютерна стеганографія // Стан та перспективи розвитку інформатики в Україні: монографія / Сергієнко І.В., Коваленко І.М., Андон П.І. – К.: Наук. думка, 2010. – С. 736–747.

2. *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.
3. *Корольов В.Ю., Поліновський В.В., Герасименко В.А.* Визначення можливостей *RS*-стеганоаналізу для дослідження статистичних властивостей зображень // Вісн. Хмельн. нац. ун-ту. – 2010. – № 4. – С. 102–110.
4. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
5. *Pat. US* 6,831,991. Reliable Detection of LSB Steganography in Color and Grayscale Images / J. Fridrich, M. Goljan. – Publ. 02.08.01. – http://patft1.uspto.gov/netacgi/nph-Parser?patentnumber=6831991
6. *Fridrich J., Goljan M., Du R.* Lossless Data Embedding – New Paradigm in Digital Watermarking // Special Issue on Emerging Applications of Multimedia Data Hiding. – 2002. – **2002**, N 2. – P. 185–196.
7. *Королев В.Ю., Полиновский В.В.* Синтез портабельных информационных сервисов для флеш-накопителей // УСиМ. – 2008. – № 6. – С. 28–33.
8. *Корольов В.Ю., Поліновський В.В., Герасименко В.А.* Тенденції розвитку портабельних програмних систем // Вісн. Хмельн. нац. ун-ту. – 2009. – № 1. – С. 233–241.
9. *Кэрриэ Б.* Криминалистический анализ файловых систем. – СПб.: Питер, 2007. – 480 с.
10. *StegAlyzerAS*: Steganography Analyzer Artifact Scanner. – http://www.sarc-wv.com/products/stegalyzeras.aspx
11. *США* раскрыли российскую шпионскую хайтек-сеть. – http://soft.compulenta.ru/543134/
12. *Стенограмма* заседания суда города Нью-Йорка, США по делу российских агентов (англ. яз.). http://www.justice.gov/opa/documents/062810complaint2.pdf
13. *Корольов В.Ю., Поліновський В.В.* Концепція побудови персоналізованих флеш-накопичувачів даних з апаратним захистом інформації // Матем. маш. і сист. – 2009. – № 4. – С. 96–105.
14. *Корольов В.Ю., Поліновський В.В., Малікова О.В.* Побудова системи захисту інформації на базі персоналізованого *USB*-флеш з використанням ключа-ідентифікатора // Вісн. Хмельн. нац. ун-ту. – 2008. – № 3. – С. 175–181.
15. *Корольов В.Ю., Поліновський В.В.* Криптогенератор з використанням перетворення шумів слабострумних електронних кіл // Вісн. Черкас. держ. ун-ту. Сер. техн. науки. Інформ. технол., обчисл. техн. і автом. – 2009. – № 2. – С. 14–18.
16. *Пат. UA* 89745 Україна, МПК (2009) *E* 05B 19/00 Спосіб автентифікації і введення кодової інформації та автентифікатор зі зчитувачем кодової інформації для його здійснення / В.В. Поліновський, О.М. Ходзінський, Т.М. Нишпорка та ін. // Заявл. 06.08.2009; Опубл. 25.02.2010, Бюл. № 4.

Поступила 07.09.2010
Тел. для справок: (044) 526-3427, 526-6743 (Киев)
© В.Ю. Королев, В.В. Полиновский, В.А. Герасименко, 2011

Внимание !

Оформление подписки для желающих опубликовать статьи в нашем журнале обязательно.

В розничную продажу журнал не поступает.

Подписной индекс 71008