УДК 004.056; 004.415.24

ВЫЯВЛЕНИЕ В АУДИОСИГНАЛАХ СКРЫТЫХ СООБЩЕНИЙ, ВНЕДРЕННЫХ С ПОМОЩЬЮ ПРОГРАММЫ S-TOOLS

Наталия Кошкина

С помощью современных стеганографических методов возможны различные варианты организации скрытых каналов коммуникации в процессе обмена типичными, не привлекающими внимания, данными. Но такая форма коммуникации представляет проблему для информационной безопасности государства, а также различных организаций, поскольку может быть использована для осуществления незаконных действий. Доступность, распространение и усовершенствование стеганографических программных продуктов и технологий повлекли за собой существенное возрастание интереса к методам выявления стеганоконтейнеров, в частности, стегано-аудиосигналов. В работе рассмотрен стеганоаналитический метод, базирующийся на явлении «отрицательного резонанса». Исследована его эффективность при обнаружении аудио-стеганоконтейнеров, созданных с помощью программы S-Tools. Выявлены важные зависимости метода: зависимость точности стеганоанализа от количества элементов в обучающей выборке SVM; от способа формирования обучающей выборки; от наполненности стеганоконтейнеров. Также в работе определены отличающие статистики для S-Tools, оценена роль стеганоключа и каждого элемента характеристических векторов сигналов. Выполненные исследования позволили улучшить оценки точности метода и определить его эффективность в разных условиях стеганоанализа.

Ключевые слова: *информационная безопастность, аудиостеганоанализ, S-Tools, статистика, линейное предсказание, метод опорных векторов.*

Введение. Одной из дисциплин, исследующих проблематику информационной безопасности, является компьютерная стеганография. В отличие от криптографии, блокирующей несанкционированный доступ к конфиденциальной информации, стеганография идет принципиально дальше – она скрывает сам факт существования этих данных, внедряя их в типичный, не привлекающий внимания объектноситель. Возможность использования методов компьютерной стеганографии для осуществления незаконной деятельности ставит под угрозу безопасность государства, а также различных организаций. Это в свою очередь влечет за собой необходимость создания методов обнаружения объектов, которые несут в себе дополнительную информацию, скрытую стеганографическими методами, – стеганоконтейнеров. Данное направление исследований получило название стеганоанализ.

Стеганоанализ задействуется в случае необходимости контроля над попытками нелегального использования методов компьютерной стеганографии. Кроме этого исследование стойкости существующих стеганографических методов и программ к методам стеганоанализа позволяет оценить их практическую пригодность и, во многих случаях, открывает пути к усовершенствованию. Большая часть существующих на сегодня публикаций в данной области посвящена стеганоанализу изображений. Но поскольку распространенные стеганографические программные продукты практически в равной степени позволяют скрывать сообщения как в изображениях, так и в аудиосигналах, вопросы аудиостеганоанализа хотя и менее раскрыты исследователями, но не менее актуальны и важны.

В данной работе изложены результаты базирующегося на явлении «отрицательного резонанса» направленного статистического аудиостеганоанализа для программы S-Tools, которая разработана Энди Брауном в 1996 году. В силу удобства своего использования она не утратила актуальности и на текущий момент доступна для скачивания на многих интернет ресурсах. Исследование этого вопроса выполнялось в работе [7], однако в ней просчитана только точность 85.6%, полученная при выявлении стеганоконтейнеров с 60% наполненностью. В реальных условиях стеганоанализа наполненность может варьироваться от 0 (в этом случае проверяемый контейнер не содержит скрытых сообщений) до 100% (проверяемый контейнер содержит скрытое сообщение максимально допустимого размера). Как это повлияет на точность стеганоанализа? Зависит ли точность от способа формирования обучающей выборки для SVM-классификатора? Все ли элементы характеристического вектора одинаково важны для целей стеганоанализа? Повлияет ли на точность изменение типа исследуемых контейнеров? Эти и другие сопутствующие вопросы остались в [7] не раскрытыми, но они важны для корректной интерпретации результатов стеганоанализа на практике. Кроме того, авторы [7] никак не комментируют

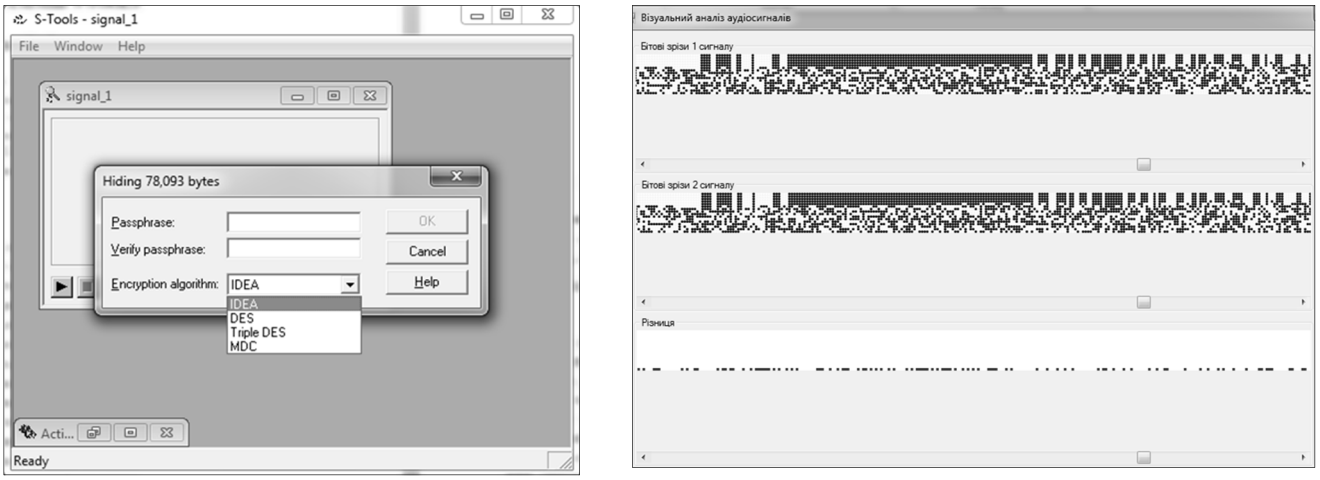
роль стеганоключа, вместе с тем, как будет показано ниже, ее определение открывает пути для усовершенствования метода.

Таким образом, ***целью данной работы*** является детальный анализ стеганоаналитического метода на базе явления «отрицательного резонанса» и оценка точности выявления этим методом S-Tools стегановложений в аудиосигналы при разных условиях стеганоанализа. Для достижения этой цели в работе решались следующие ***задачи***: 1) анализ элементов характеристических векторов аудиосигналов, оценка их значимости для целей стеганоанализа; 2) определение степени наполняемости контейнеров при «контрольном стеганопреобразовании» тестируемых сигналов, обеспечивающей наилучшую точность стеганоанализа; 3) определение оптимальных с точки зрения точности стеганоанализа параметров SVM классификатора; 4) выявление зависимостей точности стеганоанализа от различных условий его выполнения; 5) оценка точности стеганоанализа на разных типах аудиоконтейнеров.

О программе S-Tools 4.0. Интерфейс программы S-Tools 4.0 выполнен в виде многооконного MDI-приложения для операционной системы Microsoft Windows (рис. 1а). Для работы со стеганоконтейнерами используется механизм Drag-and-Drop. С помощью данной программы можно скрыть конфиденциальные сообщения в неупакованных изображениях или аудиосигналах. Используемые S-Tools 4.0 аудиосигналы имеют формат *.wav и разрядность 8 или 16 бит на отсчет. Скрываемое сообщение обязательно шифруется с помощью одного из симметричных шифров – IDEA, DES, TripleDES, MDC (по выбору пользователя), то есть в S-Tools 4.0 реализована криптостеганосистема. Секретным элементом данной криптостеганосистемы является пароль пользователя, который инициирует генерацию крипто и стеганоключей.

Реализованное в программе стеганопреобразование состоит в замене наименьшего значащего бита отсчета-носителя битом секретного сообщения (классический метод НЗБ). При сокрытии сообщений, длина которых меньше максимально возможной для данного контейнера, выполняется распределенное внедрение данных. Последовательность распределения битов сообщения по контейнеру определяется генератором псевдослучайных чисел, начальное значение которого является стеганоключом.

Один из простейших методов стеганоанализа – визуальный анализ битовых срезов контейнера. Этот метод, в частности, позволяет исследовать любой стеганографический программный продукт по стратегии «черного ящика» с целью определения местоположений внедряемых программой данных, а также в некоторых случаях стеганоключа или его достоверной оценки, используемой для дальнейшего стеганоанализа другими методами. Результат визуального анализа битовых срезов для одного из тестовых контейнеров представлен на рис. 1б, где подтверждается, что в S-Tools 4.0 реализован распределенный НЗБ метод.



а) б)

Рис. 1. Интерфейс программы S-Tools 4.0 (а) и битовые срезы оригинального сигнала, полученного из него стеганоконтейнера, и разности между ними для 16-битного тестового сигнала (б)

Формирование характеристического вектора для стеганоанализа. Стеганопреобразование изменяет статистику оригинальных контейнеров. Стеганоанализ в работе [7] построен на том, что для пустого контейнера изменение статистических характеристик в результате его стеганопреобразования более существенно, чем для контейнера, который уже был заполнен с помощью этого

же стеганопреобразования. Если каждому сигналу поставить в соответствие характеристический вектор, содержащий величины изменений его статистики, образовавшиеся после «контрольного стеганопреобразования» (КСП) этого сигнала, то выявление факта наличия скрытых сообщений возможно по значениям этих величин. Данное явление в [7] было названо «отрицательным резонансом». Отметим, что подобная идея в том или ином виде присутствует в современных стеганоаналитических методах. Например, в работе [4] она используется для атаки на программу OutGuess, которая внедряет дополнительную информацию в НЗБ коэффициентов дискретного косинусного преобразования изображений в формате JPEG. Для аудиостеганоанализа подобная идея используется в работе [6], где вычисляется мера искажений с расстоянием Хаусдорфа для сигнала и его обесшумленной версии. Итак, пусть имеется некоторый тестовый набор аудиосигналов. Среди этого набора могут быть как пустые контейнеры, т.е. сигналы без вложенных секретных сообщений, так и заполненные, т.е. сигналы, содержащие стегановложения. Для их различения с помощью явления «отрицательного резонанса» нужно выполнить стеганографическое преобразование всех сигналов данного тестового набора – КСП. В нашем случае во все сигналы с помощью программы S-Tools внедряется некоторое случайное сообщение.

Обозначим через $X=\{x_1,x_2\ldots x_N\}$ тестовый сигнал до КСП, а через $X'=\{x'_1,x'_2\ldots x'_N\}$ – его же после КСП. Характеристический вектор $V=\{\delta_1,\delta_2,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7,\delta_8\}$ каждого проверяемого аудиосигнала будет включать в себя разности значений математического ожидания, дисперсии, асимметрии и эксцесса после и до выполненного стеганопреобразования:

$$\delta_1=m_a-m_b=\frac{1}{N}\sum_{j=1}^{N}x'_j-\frac{1}{N}\sum_{j=1}^{N}x_j=\frac{1}{N}\sum_{j=1}^{N}(x'_j-x_j),$$

$$\delta_2=v_a-v_b=\frac{1}{N-1}\sum_{j=1}^{N}\left(x'_j-m_a\right)^2-\frac{1}{N-1}\sum_{j=1}^{N}\left(x_j-m_b\right)^2=\frac{1}{N-1}\sum_{j-1}^{N}\left(\left(x'_j-m_a\right)^2-\left(x_j-m_b\right)^2\right),$$

$$\delta_3=s_a-s_b=\frac{\frac{1}{N}\sum_{j=1}^{N}\left(x'_j-m_a\right)^3}{\left(\sqrt{\frac{1}{N}\sum_{j=1}^{N}\left(x'_j-m_a\right)^2}\right)^3}-\frac{\frac{1}{N}\sum_{j=1}^{N}\left(x_j-m_b\right)^3}{\left(\sqrt{\frac{1}{N}\sum_{j=1}^{N}\left(x_j-m_b\right)^2}\right)^3},$$

$$\delta_4=k_a-k_b=\frac{\frac{1}{N}\sum_{j=1}^{N}\left(x'_j-m_a\right)^4}{\left(\frac{1}{N}\sum_{j=1}^{N}\left(x'_j-m_a\right)^2\right)^2}-\frac{\frac{1}{N}\sum_{j=1}^{N}\left(x_j-m_b\right)^4}{\left(\frac{1}{N}\sum_{j=1}^{N}\left(x_j-m_b\right)^2\right)^2}.$$

Зачастую стегановложение рассматривают как добавление к сигналу некоторой шумовой компоненты. Если выделить каким либо образом шум сигнала, то для полученных численных значений шумовой компоненты также можно провести анализ изменений статистики после КСП. Один из возможных вариантов определения шума – выделение его в составе ошибки линейного предсказания сигнала. На малых временных промежутках (≈20 мс) присутствует сильная корреляция между отсчетами аудиосигнала. Это позволяет, зная корреляционную функцию, предсказывать значение очередного отсчета. Аудиосигнал $X(n)$ делится на кадры, в рамках которых предсказанное значение вычисляется как линейная комбинация его предыдущих отсчетов

$$\tilde{X}(n)=\sum_{i=1}^{p}\alpha_i X(n-i).$$

Разность между реальными и предсказанными значениями составляет ошибку предсказания

$$e(n)=X(n)-\sum_{i=1}^{p}\alpha_i X(n-i).$$

В процессе вычисления этой ошибки сигнал делится на короткие кадры с перекрытиями (в данной работе использовались кадры по 11,61 мс с 50% перекрытием между ними, а также порядок модели p=10). Для получения оптимального предсказания минимизируется среднеквадратическая ошибка предсказания, т.е. решается следующая система уравнений:

$$\sum_{k=1}^{p}\alpha_k R\left(|i-k|\right)=R(i),\ 1\le i\le p,$$

где $R(k)=\sum_{m=0}^{N-1-k}X(m)X(m+k).$

В матричной форме эта система выражается как

$$\begin{pmatrix} R(0) & R(1) & R(2) & \dots & R(p-1) \\ R(1) & R(0) & R(1) & \dots & R(p-2) \\ R(2) & R(1) & R(0) & \dots & R(p-3) \\ \dots & \dots & \dots & \dots & \dots \\ R(p-1) & R(p-2) & R(p-3) & \dots & R(0) \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \dots \\ \alpha_p \end{pmatrix} = \begin{pmatrix} R(1) \\ R(2) \\ R(3) \\ \dots \\ R(p) \end{pmatrix}.$$

Существуют эффективные методы для инвертирования таких матриц, в частности α_i и соответственно $e(n)$ можно получить, используя рекурсивную процедуру Левисона-Дурбина [3, 5]. Для определения изменений статистики шумовой компоненты после внедрения секретного сообщения, характеристический вектор необходимо дополнить разностями значений математического ожидания, дисперсии, асимметрии и эксцесса для ошибки линейного предсказания сигнала после и до КСП. Это соответственно будут элементы $\delta_5, \delta_6, \delta_7, \delta_8$ характеристического вектора V, которые вычисляются аналогично первым четырем, но не для самого тестового сигнала, а для ошибки его линейного предсказания $e(n)$.

В итоге из каждого тестового аудиосигнала будет извлечен 8-мерный характеристический вектор V. Исследуем какие из его элементов обеспечивают разделимость пустых и заполненных контейнеров, созданных программой S-Tools (отметим, что для других стеганографических программных продуктов результат может отличатся).

Анализ характеристического вектора, выделение ключевых статистик. Вводя понятие «отрицательного резонанса» авторы [7] изначально опирались на работу [4], в которой в свою очередь вводится понятие «отличительных статистик» (distinguishing statistics). Под отличительными статистиками F в [4] подразумеваются некоторые макроскопические статистические величины, которые предсказуемо изменяются с увеличением длины встроенного секретного сообщения.

Было экспериментально проверено, какие из элементов вектора $V = \{\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8\}$ являются отличительными статистиками в нашем случае. Для этого сначала был рассмотрен процесс стеганоанализа пустых контейнеров, при котором случайным образом были выбраны 10 аудиосигналов (пустых контейнеров) и из каждого из них образованы стеганоконтейнеры с наполненностью 9, 26, 50, 76 и 100%. Полученный при этом характеристический вектор поэлементно отображен на рис. 2 (отметим, что этот же эксперимент выполнялся и для большего числа тестовых сигналов, полученные при этом результаты выглядят аналогично представленным на рис. 2).

Результат данного эксперимента показывает, что наилучшими кандидатами в отличительные статистики F являются элементы и δ_8 характеристического вектора. δ_6 монотонно возрастает с увеличением длины скрытого сообщения, а δ_8 – монотонно убывает. Значения этих элементов для пустого и максимально заполненного контейнеров, т.е. F(0) и F(max δ_6 _message) соответственно, являются экстремумами функции F. Аналогичные результаты были получены в экспериментах, в которых стеганопреобразование с наполняемостью 9, 26, 50, 76 и 100% применялось не к пустым, а к уже заполненным контейнерам (стеганоключи при первом и втором стеганопреобразовании различны).

Таким образом, если использовать 100% наполняемость контейнеров во время КСП, то для каждого тестового контейнера $X(n)$ будет справедливо неравенство

$$\left|\Delta F(X_{orig}(n))\right| > \left|\Delta F(X_{stego}(n))\right|,$$

где $X_{orig}(n)$ – пустой контейнер, $X_{stego}(n)$ – образованный из него стеганоконтейнер.

Действительно если $X(n)$ не содержит скрытого сообщения, то после КСП для отличительных статистик этого сигнала имеем

$$\left|\Delta F(X_{orig}(n))\right| = \left|F(max\_message) - F(0)\right|.$$

Если же $X(n)$ содержит секретное сообщение, то при последующем внедрении сообщения максимально возможной длины, часть сообщения будет внедрена в область, статистика которой соответствует естественной статистике данного сигнала, а другая часть – в область, статистика которой уже была изменена стеганопреобразованием. «Статистическая картина» младших битов тех отсчетов, которые уже являются носителями скрытого сообщения при повторном внедрении тем же методом, по сути, не поменяется и значение отличительных статистик будет близким к $F(max\_message)$.

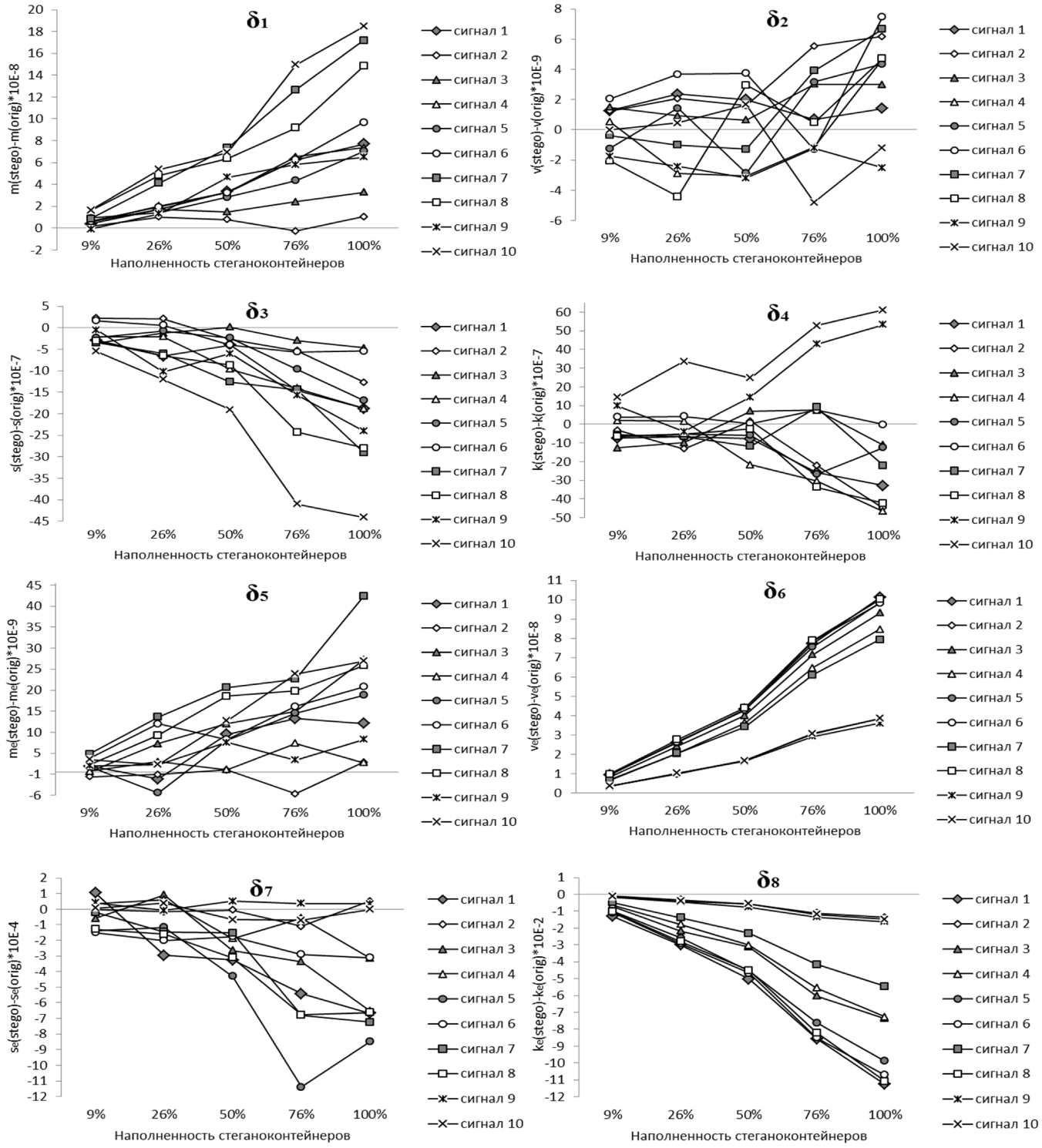


Рис. 2. Изменение статистики оригинальных сигналов в зависимости от наполненности создаваемых из них стеганоконтейнеров

Изменение отличительных статистик после КСП в этом случае выражается как

$$\left|\Delta F(X_{stego}(n))\right| \approx \left|F(max\_message) - F(secret\_message)\right|,$$

где *secret_message* – неизвестное аналитику сообщение, скрытое в проверяемом стеганоконтейнере. Так же можно описать изменение и остальных элементов характеристического вектора сигнала.

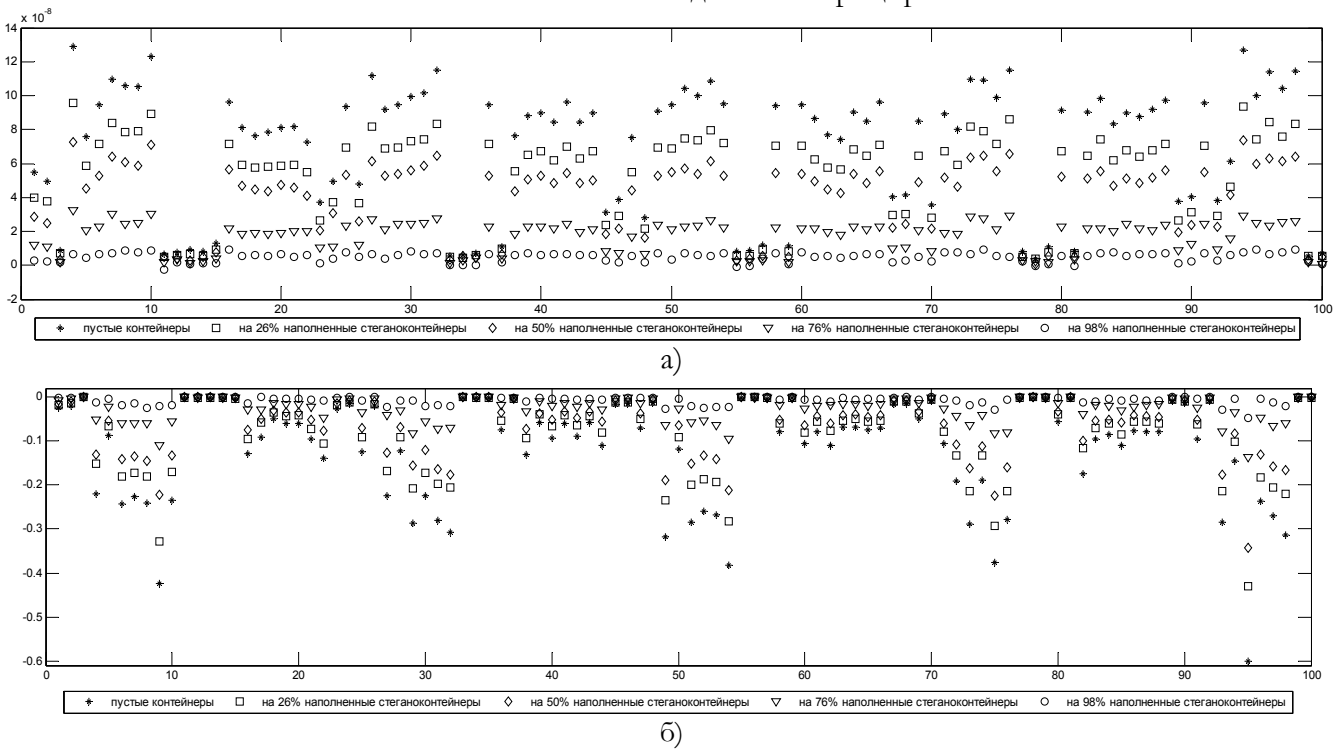
Но только найденные отличительные статистики монотонны и имеют своими экстремумами $F(0)$ и $F(max\_message)$. Следовательно, только для них выполняется

$$\forall secret\_message: \left|F(max\_message) - F(0)\right| > \left|F(max\_message) - F(secret\_message)\right|.$$

Таким образом, значения элементов характеристического вектора δ_6 и δ_8 для заполненных контейнеров всегда будут меньшими, чем для соответствующих им пустых. Но так как в общем случае стеганоаналитик не имеет одного из контейнеров пары «пустой»-«заполненный», то кроме этой закономерности для возможности выявления стеганоконтейнеров важен еще и разброс полученных значений отличительных статистик на всем множестве исследуемых контейнеров.

При исследовании значений δ_6 и δ_8, вычисленных для набора из 1254 речевых аудиосигналов и наборов образованных из них стеганоконтейнеров, было определено, что наименьший разброс значений этих элементов характерен для максимально заполненных контейнеров, а наибольший – для пустых.

Пример данной закономерности для 100 сигналов представлен на рис. 3. Как видно на этом рисунке для всех сигналов δ_6 и δ_8 ведут себя как отличительные статистики, однако часть оригинальных сигналов изначально могут иметь значения отличительных статистик близкие к их «типичным» значениям для стеганоконтейнеров. Если это будет справедливо для всех отличительных статистик, то такой сигнал в дальнейшем будет классифицирован ошибочно.



а)

б)

Рис. 3. Значения δ_6 (а) и δ_8 (б) для пустых и стеганоконтейнеров различной наполненности

Отметим, что в более ранней работе [2], где исследовались стегановложения программы Hide4PGP было показано, что для выявления Hide4PGP стеганоконтейнеров более широкого диапазона наполненностей по сравнению с подходом представленным в [7] и повышения точности выявления относительно коротких сообщений наполняемость тестовых контейнеров во время КСП должна быть меньше, чем предполагаемая наполненность искомых стеганоконтейнеров. Этот факт объясняется отсутствием в стеганосистеме Hide4PGP стеганоключа, определяющего месторасположение битов секретного сообщения. В таком случае изменение отличительных статистик для пустых контейнеров

$$\left|\Delta F(X_{orig}(n))\right| = \left|F(control\_message) - F(0)\right|,$$

где $control\_message$ – сообщение, используемое во время КСП («контрольное сообщение»).

При повторном стеганопреобразовании с более коротким сообщением, чем внедренное в первый раз, все «контрольное сообщение» попадет в область с уже измененной статистикой и после двух внедрений значение отличительных статистик будет близким к $F(sec\,ret\_message)$, а их изменение $\left|\Delta F(X_{stego}(n))\right| \approx 0$.

Так как для программы Hide4PGP, как и в случае S-Tools, 6-й и 8-й элементы характеристического вектора ведут себя как отличительные статистики, как пример вышеизложенного на рис. 4 в качестве $\left|\Delta F(X_{stego}(n))\right|$ изображены графики этих элементов для 10 случайно выбранных заполненных на 50% с помощью Hide4PGP стеганоконтейнеров.

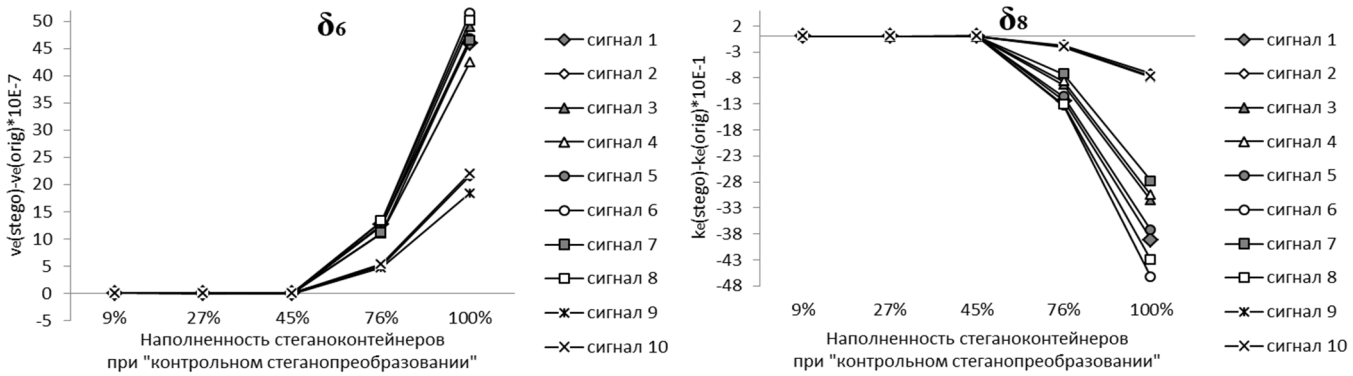


Рис. 4. Значения δ_6 и δ_8 при повторном внедрении в 50% заполненные с помощью Hide4PGP стеганоконтейнеры

На рис. 4 видно, что отличительные статистики практически не изменяются при повторном стеганопреобразовании с наполняемостью контейнеров, меньшей первичных 50%. С дальнейшим же увеличением этой наполняемости увеличивается и $\left|\Delta F(X_{stego}(n))\right|$. Таким образом, отсутствие стеганоключа, регулирующего местоположение секретного сообщения, снижает стойкость стеганосистемы (в частности реализованной в программе Hide4PGP) к данному методу стеганоанализа, позволяя улучшить точность выявления стеганоконтейнеров за счет возможности минимизации $\left|\Delta F(X_{stego}(n))\right|$.

SVM классификация пустых и заполненных контейнеров. Наличие стабильных различий в характеристических векторах пустых и заполненных контейнеров обеспечивает их разделимость на два класса с помощью метода опорных векторов (SVM – support vector machine).

SVM – эффективный бинарный классификатор, разработанный В.Н. Вапником в 90-х годах XX века [9-10]. Для того чтобы использовать SVM с целью выявления стеганоконтейнеров, нужно предварительно обучить классификатор на некоторой выборке, для которой априори известна принадлежность сигнала к одному из классов – «пустой» или «заполненный». Основной проблемой метода является выбор оптимальной гиперплоскости, которая позволяет разделить классы с максимальной точностью. Для этого разделяющая гиперплоскость выбирается таким образом, чтобы расстояние между ближайшими объектами, расположенными по разные стороны от нее, было бы максимальным. Для линейно неразделимых данных вводятся ослабляющие коэффициенты (soft-margin SVM). Так же для линейно неразделимых данных в SVM реализована идея перехода к пространству более высокой размерности, в котором ранее неразделимые данные могут стать линейно разделимыми. Такой подход называют переходом к ядру (kernel trick).

Наиболее популярное ядро, которое в частности активно используют в стеганоанализе, – гауссово (RBF, Radial Basis Functions):

$$K(V_i, V_j) = exp\left(-\frac{\left\|V_i - V_j\right\|}{2\sigma^2}\right), \sigma > 0.$$

Эксперименты показали, что именно оно обеспечивает наибольшую точность стеганоанализа в исследуемой задаче (в сравнении с линейным, квадратичным, полиномиальным ядрами и перцептроном). Выбор оптимального метода для поиска разделяющей гиперплоскости (квадратичное програмирование, последовательная оптимизация, метод наименьших квадратов), а также подбор других параметров SVM, в частности C – верхней границы диапазона поиска множителей Лагранжа в процессе обучения и σ – масштабирующего коэффициента RBF, позволяет добиться улучшения точности классификации в сравнении с точностью, полученной при использовании всех параметров по умолчанию (в наших экспериментах на 2-3%).

В работе [8] показано, что обучающая выборка SVM должна формироваться из пар «пустой» – «стеганоконтейнер», где стеганоконтейнер образован из стоящего с ним в паре пустого контейнера путем его стеганопреобразования. Для выбора оптимальных параметров классификатора не желательным является использование классической кросс-валидации, поскольку она разрывает эти пары. Соотвественно этому в данной работе обучающая выборка формировалась из пар «пустой»-«стеганоконтейнер», а параметры класификатора подбирались по дискретной сетке значений.

Результаты численных экспериментов. В качестве тестовых данных в экспериментах использовался набор из 1254-х 1-минутных фрагментов аудиокниг, оцифрованных с частотой дискретизации 44кГЦ и разрядностью 16 бит. С помощью визуальной среды создания сценариев-скриптов Sikuli из этого набора оригинальных контейнеров было образовано 5 наборов, содержащих S-Tools стегановложения, с наполненностями стеганосигналов в них 9, 26, 50, 76 и 98%. КСП также было организовано на базе Sikuli. Дальнейший стеганоанализ сигналов осуществлялся с помощью программных модулей, созданных в пакете Matlab R2011a.

Сначала была проведена серия тестов на определение оптимального количества сигналов в обучающей выборке. В них увеличивалось количество елементов в обучающей выборке при неизменном количестве елементов контрольной, для которой обученный классификатор определяет метки класса согласно построенному решающему правилу. При чем на вход обученного классификатора по очереди пода-вались две контрольные выборки: 1) выборка из 836-ти пустых контейнеров, не использо-вавшихся при обучении SVM; 2) выборка из 836-ти стеганоконтейнеров фиксированной наполненности, также не использовавшихся при обучении SVM. Результирующая точность подсчитывалась как процент правильно расставленных меток на двух вышеупомянутых контрольных выборках. Результат одного из таких експериментов представлен в таблице 1. В целом установлено, что с увеличением количества елементов точность, как правило, увеличивается (с какого-то момента незначительно), но увеличивается и время расчетов (особенно при использовании метода квадратичного програмирования).

Таблица 1

Зависимость точности стеганоанализа от количества сигналов в обучающей выборке

Количество контейнеров в обучающей выборке	Стеганоконтейнеры наполнены на 98%			Стеганоконтейнеры наполнены на 50%		
	Ложноположительная тревога	Ложноотрицательная тревога	Точность,%	Ложноположительная тревога	Ложноотрицательная тревога	Точность,%
100	101/836	145/836	85.2871	155/836	248/836	75.8971
200	70/836	74/836	91.3876	185/836	207/836	76.5550
300	38/836	32/836	95.8134	182/836	187/836	77.9306
400	43/836	22/836	96.1124	170/836	149/836	80.9211
500	35/836	21/836	96.6507	167/836	140/836	81.6388
600	37/836	19/836	96.6507	167/836	135/836	81.9378
700	38/836	19/836	96.5909	156/836	134/836	82.6555
836	49/836	14/836	96.2321	148/836	111/836	84.5096

Также исследовалось влияние на точность стеганоанализа каждого из элементов характеристического вектора. Результаты этой серии тестов представлены в таблицах 2 и 3. В данном случае использовалась обучающая выборка из 836 контейнеров, половина из которых пустые, а вторая – заполненные. Контрольная выборка, как и в предыдущих тестах, содержала 836 пустых и 836 стеганоконтейнеров фиксированной наполненности. При классификации сигналов по одномерному характеристическому вектору наилучшая точность была получена для $V=\{\delta_6\}$ (один из элементов, выбранных ранее в отличительные статистики), а наихудшая – для $V=\{\delta_2\}$ (по этому элементу сигналы не различимы). Полученная точность для второй отличительной статистики – $V=\{\delta_8\}$ в большинстве случаев хуже, чем для $V=\{\delta_1\}$, $V=\{\delta_3\}$, $V=\{\delta_5\}$. Такой результат является следствием большего разброса значений δ_8 в сравнении с разбросом значений остальных элементов.

При совместном использовании элементов, точность классификации по которым около 60% и выше, результат стеганоанализа улучшается (см. таблицу 3). В целом же наилучшая точность была получена для 7-ми элементного характеристического вектора $V=\{\delta_1,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7,\delta_8\}$.

Таблица 2

Точность стеганоанализа (в %) при классификации по одномерному характеристическому вектору

Наполненность стеганоконтейнеров	$V=\{\delta_1\}$	$V=\{\delta_2\}$	$V=\{\delta_3\}$	$V=\{\delta_4\}$	$V=\{\delta_5\}$	$V=\{\delta_6\}$	$V=\{\delta_7\}$	$V=\{\delta_8\}$
98%	83.9713	52.6914	80.4426	61.2440	76.9139	90.4904	66.7464	79.3660
76%	75.8971	54.0072	73.5048	59.4498	69.4976	87.5598	61.8421	69.7368
50%	61.3636	51.8541	61.9019	55.4426	58.7919	76.9139	55.2632	56.6986
26%	56.5789	49.7608	56.3995	52.0933	53.2297	68.3014	53.9474	53.8876
9%	51.6148	49.6411	50	50	51.7943	57.4163	50.4785	51.0766

Таблица 3

Точность стеганоанализа (в %) для разных вариантов формирования характеристического вектора

Наполненность стеганоконтейнеров	$V=\{\delta_6,\delta_8\}$	$V=\{\delta_1,\delta_3\}$	$V=\{\delta_1,\delta_3\delta_6,\delta_8\}$	$V=\{\delta_1,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7,\delta_8\}$	$V=\{\delta_1,\delta_3,\delta_5,\delta_6,\delta_7,\delta_8\}$	$V=\{\delta_1,\delta_2,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7,\delta_8\}$
98%	92.2249	85.2273	93.6603	96.8900	94.6172	96.2321
76%	87.9187	77.3325	89.8923	93.4211	90.9689	92.2847
50%	77.1531	62.3804	85.8254	88.3971	86.9617	84.5096
26%	69.4976	57.1172	77.9306	79.0670	78.8876	74.6411
9%	56.1603	51.6148	55.9809	57.7751	57.7751	57.7153

Так как стеганоаналитик, как правило, не обладает информацией о длине скрытых сообщений, он может выбрать один из двух вариантов анализа:

1) использовать один классификатор, обученный на сигналах разной наполненности;

2) последовательно проверить некоторый контейнер на наборе бинарных классификаторов, обученных каждый на пустых контейнерах и стеганоконтейнерах одинаковой или близкой наполненности, так чтобы в совокупности набор охватывал все возможные варианты наполненности контейнеров.

Второй подход требует больше времени на анализ, но в целом позволяет более точно определять наличие скрытых сообщений. Так, точность при $V=\{\delta_1,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7,\delta_8\}$ и совпадающей наполненности стеганоконтейнеров обучающей и контрольной выборок приведена в колонках «Совпадение наполненности» таблицы 4 (обучающая выборка состоит из 400 пустых и 400 стеганоконтейнеров, контрольная – из 836 пустых и 836 заполненных).

В колонках «Общая обучающая выборка» этой таблицы приведена точность стеганоанализа при использовании $V=\{\delta_1,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7,\delta_8\}$ и обучающей выборки, состоящей из 400 пустых контейнеров и по 80 контейнеров 100, 76, 50, 26 и 9% наполненности. Как можно было предположить уже после примеров, приведенных на рис. 2 и 3, стеганоконтейнеры с большей наполненностью выявляются с большей точностью. Эта зависимость верна при разных параметрах стеганоанализа и для разных множеств тестовых сигналов.

Эксперименты, подобные вышеприведенным, также были выполнены для 8-битных речевых и 16-битных музыкальных записей.

При сокрытии сообщений в 8-битных сигналах, вносимый НЗБ-стеганопреобразованием шум значительно превышает шум, вносимый им в 16-битные сигналы. Поэтому и выявить скрытую информацию в 8-битных сигналах удается с большей точностью. Так, среднее значение SNR для оригинальных и 100% заполненных 16-битных речевых сигналов тестового набора равно 75.9018 дБ, а для 8-битных – 28.5992 дБ. И, например, точность выявления 8-битных контейнеров в режиме «Совпадение наполненности» при их наполненности на 50% равна 99.6013%, на 25% – 97.6874%, на 9% – 84.2105%.

Музыкальные записи имеют более разнообразное спектральное наполнение по сравнению с речевыми и, как правило, больше высоких амплитуд. Так для использованного в экспериментах набора 1-минутных музыкальных фрагментов после стеганопреобразования всех контейнеров данного набора с их 100% наполняемостью среднее значение соотношения сигнал-шум – mean(SNR)=79.8356 дБ. Точность выявления скрытых сообщений в музыке хуже, чем в речевых сигналах и больше элементов характеристического вектора, по которым сигналы не различимы (не

различимы по $\delta_2, \delta_4, \delta_7$; а наилучшая различимость по δ_6). По вектору $V = \{\delta_1, \delta_3, \delta_5, \delta_6, \delta_8\}$ в режиме «Совпадение наполненности» на 98% наполненные стеганосигналы с музыкой выявляются данным методом с точностью 94.2584%, 76% – с точностью 81.3397%, а 50% – с точностью 62.0415%.

Таблица 4

Зависимость точности стеганоанализа от наполненности стеганоконтейнеров

Наполненность стеганоконтейнеров	«Совпадение наполненности»			«Общая обучающая выборка»		
	Ложноположительная тревога	Ложноотрицательная тревога	Точность,%	Ложноположительная тревога	Ложноотрицательная тревога	Точность,%
98%	44/836	8/836	96.8900	170/836	4/836	89.5933
76%	85/836	26/836	93.3612	170/836	36/836	87.6794
50%	130/836	73/836	87.8589	170/836	87/836	84.6292
26%	203/836	158/836	78.4091	170/836	226/836	76.3158
9%	366/836	344/836	57.5359	170/836	551/836	56.8780

Заключение. В данной работе выполнено более детальное и полное исследование метода стеганоанализа на базе явления «отрицательного резонанса» и его точности, нежели в работе [7]. Предложенный подход может быть применен для оценки точности выявления стегановложений не только S-Tools и Hide4PGP, но и других стеганографических программ. Кроме того он может быть дополнен кросс-тестами, в которых программное обеспечение при КСП не то, с помощью которого создавались выявляемые стеганосигналы. А также исследованием проблематики определения вероятной длины скрытых сообщений.

Метод эффективен при выявлении НЗБ-стегановложений не только в аудиосигналах, но и в изображениях. Соответствующие результаты исследования будут представлены в последующих публикациях. Также планируется выполнить сравнительный анализ точности данного метода аудиостеганоанализа с существующими аналогами, в частности методом на базе матрицы смежности аудиосигналов [1] и методом с измерением искажений, базирующемся на расстоянии Хаусдорфа [6]. Кроме того в перспективе будет рассмотрен один из возможных путей дальнейшего повышения точности стеганоанализа – дополнение характеристического вектора другими элементами, выражающими особенности пустых и заполненных контейнеров.

ЛИТЕРАТУРА

[1]. Кошкіна Н.В. Стеганоаналіз МІК-стеганографії на базі матриці суміжності та методу опорних векторів / Н.В. Кошкина // Искусственный интеллект. – 2012. – № 4. – С. 567-577.

[2]. Кошкина Н.В. Выявление Hide4PGP вложений в аудиосигналах / Н.В. Кошкина //Проблемы управления и информатики. – 2013. – №3.– С. 151-156.

[3]. Cedrick Collomb Linear prediction and Levinson-Durbin algorithm [Электронный ресурс]. – Режим доступа: http://www.emptyloop.com/technotes/A%20tutorial%20on%20linear%20prediction%20and%20Levinson-Durbin.pdf

[4]. Fridrich J., Goljan M., Hogea D., Soukal D. Quantitative steganalysis of digital images: estimating the secret message length // ACM Multimedia systems journal, Special issue on multimedia security, 2003, № 9(3), P.288–302.

[5]. Garg M. Linear prediction algorithms. Institute of Technology, Bombay, India, 2003 [Электронный ресурс]. – Режим доступа: http://www.mohrahit.in/find/predict.pdf

[6]. Liu Y., Chiang K., Corbett C., Archibald R., Mukherjee B., Ghosal D. A novel audio steganalysis based on higher-order statistics of a distortion measure with Hausdorff distance // Lecture Notes in Computer Science, 2008, № 5222, P. 487 -501.

[7]. Ru X., Zhuang Y., Wu F. Audio steganalysis based on "negative resonance phenomenon" caused by steganographic tools // Journal of Zhejiang University Science A, 2006, № 7(4), P. 577–583.

[8]. Schwamberger V. Franz M. O. Simple algorithmic modifications for improving blind steganalysis performance // Proceedings of the 12th ACM Multimedia & Security Workshop MMSec, Rome, 2010, P. 225-230.

[9]. Vapnik V.N. Statistical learning theory, New York: Wiley, 1998, 732 p.

[10]. Vapnik V.N. The nature of statistical learning theory, New York: Springer-Verlag, 2000, 332 p.

REFERENCES

[1]. Koshkina N.V. Steganalysis of QIM-steganography based on co-occurrence matrix and support vector machine, Artificial intelligence, 2012, № 4, P. 567-577.

[2]. Koshkina N.V. Detection of hidden messages embedded in audio signals by Hide4PGP, Journal of automation and information sciences, 2013, № 45, P. 75-81. (English version)
[3]. Cedrick Collomb Linear prediction and Levinson-Durbin algorithm [Electronic resource]. – Mode of access: http://www.emptyloop.com/technotes/A%20tutorial%20on%20linear%20prediction%20and%20Levinson-Durbin.pdf
[4]. Fridrich J., Goljan M., Hogea D., Soukal D. Quantitative steganalysis of digital images: estimating the secret message length, ACM Multimedia systems journal, Special issue on multimedia security, 2003, № 9(3), P.288–302.
[5]. Garg M. Linear prediction algorithms. Institute of Technology, Bombay, India, 2003 [Electronic resource]. – Mode of access: http://www.mohrahit.in/find/predict.pdf
[6]. Liu Y., Chiang K., Corbett C., Archibald R., Mukherjee B., Ghosal D. A novel audio steganalysis based on higher-order statistics of a distortion measure with Hausdorff distance, Lecture Notes in Computer Science, 2008, № 5222, P. 487 -501.
[7]. Ru X., Zhuang Y., Wu F. Audio steganalysis based on "negative resonance phenomenon" caused by steganographic tools, Journal of Zhejiang University Science A, 2006, № 7(4), P. 577-583.
[8]. Schwamberger V. Franz M. O. Simple algorithmic modifications for improving blind steganalysis performance, Proceedings of the 12th ACM Multimedia & Security Workshop MMSec, Rome, 2010, P. 225-230.
[9]. Vapnik V.N. Statistical learning theory, New York: Wiley, 1998, 732 p.
[10]. Vapnik V.N. The nature of statistical learning theory, New York: Springer-Verlag, 2000, 332 p.

ВИЯВЛЕННЯ В АУДІОСИГНАЛАХ ПРИХОВАНИХ ПОВІДОМЛЕНЬ, ВКРАПЛЕНИХ ЗА ДОПОМОГОЮ ПРОГРАМИ S-TOOLS

За допомогою сучасних стеганографічних методів можливі різні варіанти організації прихованих каналів комунікації під час обміну типовою інформацією, що не привертає уваги. Але така форма комунікації є проблемою для інформаційної безпеки держави та різних організацій, оскільки може бути використаною для звершення протиправних дій. Доступність, поширення та вдосконалення стеганографічних програмних продуктів і технологій спричинили суттєве зростання інтересу до методів виявлення стеганоконтейнерів, зокрема стеганоаудіосигналів. В роботі досліджено ефективність методу стеганоаналізу аудіосигналів, який базується на явищі «від'ємного резонансу» для виявлення стеганоконтейнерів, що створені програмою S-Tools. Визначені важливі залежності методу: залежність точності стеганоаналізу від кількості елементів в навчальній вибірці SVM; від способу формування навчальної вибірки; від наповненості стегано-контейнерів. Також у роботі визначені відрізняючі статистики для S-Tools, оцінено роль стеганоключа та кожного елементу характеристичних векторів сигналів. Виконані дослідження дозволили покращити оцінки точності методу та визначити його ефективність в різних умовах стеганоаналізу.

Ключові слова: інформаційна безпека, аудіостеганоаналіз, S-Tools, статистика, лінійне передбачення, метод опорних векторів.

DETECTION OF HIDDEN MESSAGES THAT ARE EMBEDDED IN THE AUDIO SIGNALS USING S-TOOLS

There are a lot of variants of the covert communication channels formation during transmitting an usual, non-suspicious data that are possible with using current steganography methods. But these forms of communications are the problem for the state security, as well as for various organizations because they could be used for an illegal activities. Accessibility, spreading and improvement of steganography software and technologies led to a significant increase of interest to the steganographic detection methods in a cover media, in particular, in an audio signals. In this paper was investigated the effectiveness of the audio steganalysis method that based on the "negative resonance" phenomenon for detecting the stego signals, formed by program S-Tools. The important relations of this method were found: the dependence of steganalysis accuracy on the amount of elements in the SVM training set; on the method of training set forming; on steganographic capacity of the stego signals. Also in this paper were found distinguishing statistics for the S-Tools and the roles of the stegokey and of each elements of the signals characteristic vectors have been evaluated. This research allows the improvement of the estimates of accuracy of the method and allows to find their effectiveness in the different steganalysis conditions.

Keywords: information security, audio steganalysis, S-Tools, statistics, linear prediction, support vector machine.

Кошкіна Наталія Василівна, кандидат фізико-математичних наук, старший науковий співробітник, Інститут кібернетики імені В.М. Глушкова НАН України.
E-mail: K_n_v@ukr.net
Кошкина Наталия Васильевна, кандидат физико-математических наук, старший научный сотрудник, Институт кибернетики имени В.М. Глушкова НАН Украины.
Koshkina Nataliia, Candidate of Physics and Mathematics (PhD), Senior Researcher, V.M. Glushkov Institute of Cybernetics of NAS of Ukraine.