УДК 004.056; 004.415.24

Н.В. Кошкина

Обзор и классификация методов стеганоанализа

Определены и проанализированы основные подходы к решению задач стеганоанализа мультимедийных контейнеров. Выполнена классификация стеганоаналитических методов по различным критериям. Описаны примеры визуального, сигнатурного и статистического стеганоанализа. Для статистических методов с обучением выделены возможные варианты построения характеристических векторов и используемые классификаторы.

The main approaches to the solving problems of steganalysis for the multimedia carriers are identified and analyzed. The classification of the existing stegoanalytical methods according to the various criteria is performed. The examples of visual, signature and statistical steganalysis are described. For the statistical methods with learning, the possible ways of building the characteristic vectors as well as the used classifiers are identified.

Визначено та проаналізовано основні підходи до розв'язання задач стеганоаналізу мультимедійних контейнерів. Виконано класифікацію стеганоаналітичних методів за різними критеріями. Описано приклади візуального, сигнатурного та статистичного стеганоаналізу. Для статистичних методів з навчанням виділено можливі варіанти побудови характеристичних векторів та класифікатори, які використовуються.

Введение. Современные стеганографические системы предлагают различные варианты сокрытия тайных сообщений в обычных, не привлекающих особого внимания цифровых объектах – контейнерах. Для мультимедийных контейнеров чаще всего используются методы внедрения сообщений в младшие биты элементов контейнера или его частотных коэффициентов. Кроме того, тайные данные могут быть внедрены в служебные поля и после маркера конца файла. Путем подбора шага квантования во время *mp*3-сжатия они могут быть скрыты в битах парности кадров аудиосигнала. Также существуют программы, использующие для сокрытия перестановку элементов контейнера согласно граф-теоретическому методу, скрывающие данные согласно методу расширения спектра, внедряющие информацию в палитру изображений.

Постановка задачи

Различные интернет-ресурсы открывают доступ к более чем ста программным продуктам для стеганографического внедрения данных в аудио- или видеосигналы, изображения, текстовые или *HTML*-документы, исполняемые модули, динамические библиотеки и другие типичные для цифровых сред контейнеры [1]. Следует, однако, учитывать, что такая форма коммуникации может быть использована для реализации противоправных действий и стать угрозой информационной безопасности государства и различных организаций [2]. Поэтому актуально развитие дисциплины, в рамках которой создаются и исследуются методы противодействия стеганографии, – стеганоанализа. Последний развивается с некоторым запаздыванием относительно стеганографии, о чем в частности свидетельствует количество публикаций, раскрывающих те или иные вопросы этих дисциплин. Количество работ, предлагающих стеганоаналитические методы, в настоящее время стремительно увеличилось. Так же как в стеганографии [3, 4] и других науках, подобный скачок в развитии влечет за собой необходимость систематизации выполненных исследований, осуществления классификации и анализа существующих методов.

Таким образом, цель данной статьи – анализ и классификация существующих стеганоаналитических методов, предназначенных для обнаружения скрытых вложений в аудиосигналах и изображениях.

Классификация стеганосистем

Как правило, стеганоаналитик не изменяет содержимое атакованных им сигналов или изображений, а пытается обнаружить в них скрытые сообщения и иногда их размер и содержание.

Такой стеганоанализ можно рассматривать как осуществление пассивных атак на стеганографические системы [5]. По уровню обеспечения стойкости к пассивным атакам стеганосистемы можно разделить на три класса:

• *Теоретически стойкие* – осуществляют сокрытие информации в тех элементах контейнеров, значения которых не превышают уровня шумов или погрешностей квантования. Невозможность различения пустых и заполненных контейнеров для таких систем должна быть теоретически доказуема.

• *Практически стойкие*. Возможность выявления стеганоконтейнеров, созданных такими системами, не исключена, но на данный момент противник не располагает необходимыми для этого ресурсами, в частности стеганоаналитическими методами и программами.

• *Нестойкие* – стеганосистемы, для которых существуют стеганоаналитические методы, определяющие факт их эксплуатации.

Развитие стеганоанализа и создание новых методов обуславливают переход определенных стеганосистем из класса практически стойких в класс нестойких. Но следует учитывать, что часто исследование стойкости существующих стеганографических систем и соответствующего программного обеспечения к методам стеганоанализа не только позволяет оценить их практическую пригодность, но и указывает пути возможного усовершенствования. А после усовершенствования стеганосистема возвращается в класс практически стойких.

Классификация методов стеганоанализа

Стеганоаналитические методы в целом можно классифицировать по разным критериям. В зависимости от количества информации, доступной аналитику, можно выделить *направленные* и *универсальные* методы анализа. При разработке направленных методов предполагается, что все детали алгоритма сокрытия известны, но неизвестен стеганографический ключ. При разработке универсальных методов использование алгоритма сокрытия возможно только в режиме «черного ящика». В этом случае аналитик старается найти определенные признаки, характерные для пустых контейнеров, которые удовлетворяли бы требованиям репрезентативности и контекстной независимости, и одновременно менялись бы при встраивании в контейнер дополнительной информации. Универсальные методы, как правило, менее точны в сравнении с направленными, однако они значительно более широко применимы.

По критерию цели атаки можно выделить:

• *Статический стеганоанализ*, цель которого – различение пустых и заполненных контейнеров и определение метода или программы, с помощью которых заполненные контейнеры создавались.

• *Динамический стеганоанализ*. Целью такого анализа может быть определение размера скрытого сообщения и его местоположения в стеганоконтейнере, получение оценки тайного ключа, параметров алгоритма внедрения, а также извлечение скрытого сообщения.

• *Вспомогательный стеганоанализ* подразумевает разработку активных и злоумышленных атак с целью спровоцировать повторную передачу сообщения.

В зависимости от объекта поиска в проверяемых контейнерах стеганоаналитические методы можно разбить на три класса: *визуальные*, *сигнатурные* и *статистические*.

Визуальные и сигнатурные методы

Визуальные методы базируются на способности анализа зрительных образов системой человеческого зрения. При визуальном стеганоанализе изучается графическое представление битовых срезов контейнеров–изображений, где ищутся видимые нарушения межпиксельной и внутрипиксельной корреляции. В отдельных случаях информативен визуальный контроль однотонных фрагментов изображения или анализ артефактов сжатия в увеличенном масштабе [6]. Также полезную для стеганоанализа информацию можно получить с помощью визуального анализа спектрограмм аудиосигналов [7]. В частности, таким образом возможен поиск пиков синхронизации или иных нетипичных артефактов в частотной области.

Сигнатурные методы направлены на поиск «отпечатков пальцев», оставляемых в стеганоконтейнере некоторыми программами сокры-

тия: нетипичных значений в служебных полях и полях данных файлов, несоответствий формату, специфических для определенных стеганографических программ битовых последовательностей.

Сигнатурный стеганоанализ реализован, например, в программе *StegSpy v*2.1, которая идентифицирует стеганоконтейнеры, созданные с помощью программ *Hiderman*, *JPHide and Seek*, *Masker*, *JPegX*, *Invisible Secrets*, а также находит местоположение внедренной информации [8]. Сигнатурные методы могут быть как направленными, так и универсальными. Рассмотрим примеры направленного сигнатурного стеганоанализа.

Весьма специфический след оставляет за собой программа *Hide and Seek*, которая скрывает информацию в файлах формата *gif*. Сокрытие в данной программе осуществляется путем замены младших бит цветовых индексов точек изображения, местоположение битов скрываемой информации определяется генератором случайных чисел. Однозначную идентификацию цветного изображения, представленную *Hide and Seek* стеганоконтейнером, легко осуществить путем анализа значений элементов палитры этого изображения: значения всех цветовых составляющих элементов палитры будут кратны четырем, в частности белому цвету будет соответствовать не значение (255, 255, 255), как в пустом контейнере, а (252, 252, 252). Дополнительным подтверждением наличия скрытого сообщения в случае *Hide and Seek* служит размер изображения. Эта программа в версии 4.1 создает только стеганоконтейнеры размера 320×480 пикселей. Если же исходное изображение было меньшим указанных размеров, оно дополняется черными пикселями, большим – обрезается. Версия 5.0 аналогично подгоняет исходное изображение к одному из следующих размеров: 320×200, 320×400, 320×480, 640×400 или 1024×768 пикселей.

Еще одна стеганографическая программа, вмешательство которой легко выявить сигнатурным анализом, – *JPegX* [9]. Эта программа внедряет секретные данные после маркера конца *jpeg*-файла, а перед скрываемым сообщением обязательно добавляет сигнатуру 5*B* 3*B* 31 53 00, по которой стеганоконтейнер и программа, с помощью которой он создан, однозначно идентифицируются в дальнейшем. Так же находятся изображения со скрытой информацией, созданные программой *Hiderman*. Вмешательство этой программы обнаруживается по наличию сигнатуры 43 44 4*E* при просмотре изображения в шестнадцатеричном редакторе (*CDN* в *ASCII*-коде).

Метод направленного сигнатурного стеганоанализа для выявления *BPCS*-стеганографии описан в работе [10]. *BPCS* (*Bit-Plane Complexity Segmentation*), что можно перевести как «разделение битовых слоев на сегменты по уровню сложности». Это официальное название стеганографического метода, который активно развивается японским профессором Эйджи Кавагучи. Метод *BPCS* внедряет сообщения в сегменты битовых слоев изображения, сложность которых выше заданного порога. Сложность сегмента может быть рассчитана по-разному, в частности в [10] мерой сложности выступает количество переходов цвета вдоль столбцов и строк черно-белого представления квадратного сегмента $m \times m$ битового слоя. Сложность сегментов при этом варьируется от нуля (чисто белый или черный блок) до $m \times (m - 1) \times 2$ (блок в виде шахматной доски). Сегменты со сложностью ниже порога классифицируются как информационные, выше – шумоподобные. Использование для сокрытия шумоподобных сегментов не только младшего, а всех битовых слоев, позволяет существенно увеличить пропускную способность стеганоканала при соблюдении условия визуальной незаметности вмешательства.

Но, как оказалось, *BPCS*-стеганоконтейнеры можно выявить, построив гистограмму сложности, представляющую собой относительную частоту возникновения различных сложностей сегментов изображения. Построенная гистограмма есть сигнатурой *BPCS*-метода, поскольку имеет специфическую форму. Для гистограмм стеганоконтейнеров в районе порога внедрения всегда наблюдается характерная впадина, а распределение сложностей после порога близко

к нормальному. Устранения данной сигнатуры возможно путем использования половины шумоподобных данных для регулирования значений сложности, но это вдвое уменьшает пропускную способность.

Примером универсального сигнатурного стеганоанализа есть метод, описанный в работах [11, 12]. Авторы этих публикаций показывают нецелесообразность применения изображений, первоначально сохраненных в формате *jpeg* для сокрытия информации в пространственной области. Квантование, применяемое при сжатии, служит хрупким «отпечатком пальца», который дает возможность обнаружить изменение даже одного пикселя. Нахождение изменений основывается на исследовании совместимости блоков 8×8 пикселей изображения со сжатием *jpeg* с заданной матрицей квантования. С целью соблюдения условия невидимости стеганографические методы предусматривают внесение как можно меньшего количества искажений в контейнер, поэтому после внедрения данных в изображении будет отслеживаться характерная структура, указывающая на то, что в прошлом оно было сохранено в *jpeg* формате. Анализ коэффициентов дискретного косинусного преобразования (ДКП) блоков 8×8 пикселей для достаточно больших изображений позволяет восстановить использованную матрицу квантования. Стеганопреобразование нарушает полное соответствие блока *jpeg* формату в том смысле, что полученный после него блок пикселей не может быть образован путем *jpeg*-декомпрессии никакого блока квантованных ДКП-коэффициентов. Найденные расхождения интерпретируются как сигнатура стеганографии. Подсчет количества несовместимых блоков позволяет оценить размер секретного сообщения. Для идентификации пикселей, несущих скрытую информацию, рассчитывают совместимые блоки, близкие по значениям к блокам с нарушенной *jpeg* совместимостью. Так можно выявить применение любых стеганографических методов, за исключением тех, которые внедряют сообщения в квантованные коэффициенты ДКП-изображений.

Использование для сокрытия данных первых попавшихся контейнеров повышает вероятность успеха визуальных и сигнатурных методов [13]. Не сложно обнаружить стороннее вмешательство в изображения, которые не являются фото или сканированным материалом, а были созданы с помощью компьютерных программ. Дискредитировать стеганосистему могут и изменения младших битовых слоев гладких участков высококачественных изображений. Поэтому в качестве контейнеров целесообразно выбирать достаточно зашумленные сигналы и изображения с большим количеством мелких деталей.

Если пользователи стеганографической системы выбирают только подходящие для сокрытия контейнеры, визуальный или сигнатурный анализ эффективны для выявления факта эксплуатации не более чем 10 процентов существующих стеганографических программ. Например, в работе [14] показана неэффективность сигнатурного анализа при выявлении *S-Tools* стеганоконтейнеров.

Статистические методы

Значительно большую гибкость и широкую область применения имеют статистические методы стеганоанализа. Они, как правило, основываются на анализе различий в статистических характеристиках естественных, т.е. «чистых» контейнеров и тех, которые подвергались стеганопреобразованию – носителей скрытой информации.

Первый статистический метод – *Хи-квадрат атака*, предложенная в 1999 г. [15] для обнаружения НЗБ-стеганографии. В данном методе применяется критерий согласия Пирсона, на основе которого происходит сравнение близости распределения исследуемой последовательности элементов контейнера к распределению, характерному для стеганограмм. *Хи-квадрат атака* дает превосходные результаты в случаях, когда аналитику известно, в каких отсчетах контейнера осуществлялось сокрытие. Если же использованная стеганосистема предполагает зависящие от ключа местоположения внедрения битов, то эффективность данного метода бы-

стро падает со снижением длинны скрываемого сообщения.

Один из первых методов статистического стеганоанализа, учитывающий возможность зависимости местоположений внедрения от секретного ключа, – это *RS*-анализ (*Regular-Singular*), предложенный в работе [16]. Данный метод направлен на выявление скрытых зависимостей между элементами контейнера. В рассмотрение вводятся функции гладкости и переворота, с использованием которых группы пикселей изображения делятся на три класса: регулярные, сингулярные и неиспользуемые. Естественные изображения характеризуются большим количеством регулярных групп в сравнении с сингулярными. При различении пустых и заполненных контейнеров используется переворот с наложенной на группу маской, состоящей из значений –1, ноль и единица. Для естественных изображений количество регулярных групп, полученных с некоторой маской M приблизительно такое же, как и количество регулярных групп, полученных с инверсной маской $-M$. То же самое наблюдение справедливо и для сингулярных групп. Внедрение сообщения в младшие биты контейнера влечет за собой сближение количества регулярных и сингулярных групп, полученных с маской M. С увеличением длины скрываемого сообщения разность между количеством этих групп стремится к нулю. В то же время разность между количеством регулярных и сингулярных групп, полученных с маской $-M$ увеличивается с увеличением длины скрываемого сообщения.

Обобщением *RS*-анализа и его формулировкой в несколько других терминах является метод *SPA* (*Sample Pair Analysis*), предложенный в работе [17].

Наиболее многочисленный класс статистических методов – это методы классификации с обучением. В отличие от *Хи-квадрат атаки*, *RS*-анализа и *SPA* такие методы, как правило, универсальны. Общая схема стеганоанализа для них может быть описана следующим образом:

- Определение характеристических векторов контейнеров.
- Выбор и обучение классификатора, на вход которого подаются характеристические векторы контейнеров обучающей выборки. Последняя формируется из репрезентативного количества пустых и заполненных контейнеров, для каждого из которых известно, какому из двух классов они принадлежат. Контейнеры обучающей выборки должны обладать максимально схожими характеристиками с контейнерами, классификация которых есть целью стеганоанализа.
- Классификация контейнеров, подлежащих проверке.

Характеристический вектор должен быть чувствительным к изменениям, вносимым стеганографическими программами, но при этом независимым от содержимого контейнеров. Элементы характеристических векторов пустых и заполненных контейнеров должны отличаться. Чем большее различие между ними наблюдается, тем лучше такой элемент подходит для целей стеганоанализа. Рассмотрим существующие варианты вычисления характеристических векторов для мультимедийных контейнеров.

Подходы к вычислению характеристических векторов

Авторы работы [18] предлагают строить характеристические векторы на основе оценок качества изображений. Их стеганоанализ базируется на устойчивом различии характеристических векторов, элементы которых – определенные оценки качества пустого и заполненного контейнеров при наличии эталона. Эталонный контейнер получают из проверяемого путем его фильтрации. На этом этапе однородно хорошие результаты для совокупности различных стеганографических методов и программ были получены для двумерного гауссовского фильтра (стеганоанализ в работе [18] выполнялся для модуля *Digimarc* в программе *Photoshop*, метода Коха–Жао [2], технологии *PGS* [19], программ для организации тайной коммуникации *Steganos*, *S-Tools* и *Jsteg*). Результаты, позволяющие различить пустые и заполненные контейнеры, были получены для следующих метрик качества:

• норма Минковского первого и второго порядка, т.е. манхэттенское и евклидово расстояние соответственно (*Minkowsky measures*);

• расстояние Чекановского (*Czekanowski distance*);

• угловая корреляция (*angular correlation*);

• точность изображения (*image fidelity*);

• нормированная взаимная корреляция (*normalized cross-correlation*);

• мера искажения амплитуды спектра Фурье-изображения (*spectral magnitude distortion*);

• медиана искажения фазовых спектров блоков изображения (*median of block spectral phase*);

• медиана взвешенного искажения спектров блоков изображения (*median of weighted block spectral distortion*);

• нормализованная среднеквадратическая ошибка, полученная с учетом модели человеческого зрения (*normalized mean square HVS error*).

В работе [20] рассмотрена проблематика выявления скрытых сообщений в *jpeg*-контейнерах. Расчет характеристических векторов выполняется в частотной области: из файла, хранящего *jpeg*-изображение, извлекаются абсолютные значения квантованных ДКП-коэффициентов блоков 8×8 пикселей. Полученный при этом двумерный массив коэффициентов будет иметь те же размеры, что и исходное изображение. Авторы работы отметили, что абсолютные значения ДКП-коэффициентов будут коррелированы в горизонтальном, вертикальном и диагональном направлениях. Распределение разностей соседних в указанных направлениях значений сконцентрировано в пределах нуля и подобно распределению Лапласа.

Современные стеганографические программы, например *OutGuess*, могут внедрять данные только в половину доступных коэффициентов, а вторую половину использовать для компенсации изменений в гистограмме пространственной или частотной областей. Учитывая это, авторы [20] ищут различия в статистике не первого, а второго порядка для пустых и заполненных контейнеров. Они рассматривают четыре множества разностей коэффициентов ДКП как вероятностные процессы Маркова, для характеристики которых используют матрицы вероятностей перехода с одним шагом. Для уменьшения вычислительной сложности стеганоанализа количество анализируемых элементов уменьшают согласно следующей пороговой обработке: элементы со значениями большими, чем порог T, и меньшими, чем $-T$, преобразуют в T и $-T$ соответственно. Эта процедура приводит к матрице вероятностей перехода размерности $(2T+1)\times(2T+1)$. Результирующий характеристический вектор будет иметь размерность $4\times(2T+1)\times(2T+1)$. В своих экспериментах авторы [20] использовали $T=4$, извлекая из проверяемых изображений 324 элементные характеристические векторы.

Следующий подход использует в целях стеганоанализа бинарные меры сходства, широко применяемые в биологии, географии, социологии, распознавании образов, поисковых системах и др. [21]. Стеганоанализ, предложенный в [21], базируется на изменении корреляции между битовым срезом, в который внедрены дополнительные данные, и соседними с ним не модифицированными битовыми срезами. Так, например, применение НЗБ стеганографии влечет за собой уменьшение сходства между седьмым и восьмым битовыми срезами изображения. Подход применим как в пространственной, так и в частотной области мультимедийных контейнеров. Характеристический вектор, построенный в данном исследовании, включает в себя 14 элементов, вычисленных как следующие бинарные меры подобия: меры Сокала–Снита (*R.R. Sokal*, *P. Sneath*) 1–5; мера Кульчинского (*S. Kulczynski*) 1; мера Очиаи (*A. Ochiai*); мера Ланса–Уильямса (*G.N. Lance*, *W.T. Williams*); различие структур (*pattern difference*); дисперсия несходства (*variance dissimilarity*); минимум разности гистограмм (*minimum histogram difference*); абсолютная разность гистограмм (*absolute histogram difference*); взаимная энтропия (*mutual entropy*); расстояние Кульбака–Лейблера (*S. Kullback*, *R.A. Leibler*). Эти бинарные меры подобия рассчитываются по содержимому пятиэлементных групп, состоящих

из текущего бита битового среза изображения и четырех смежных с ним в горизонтальном и вертикальном направлениях.

Кроме указанных мер сходства, в характеристический вектор входят еще четыре меры, при расчете которых используются биты, смежные не только по горизонтали и вертикали, но и по двум диагоналям. Каждая анализируемая девятиэлементная группа взвешивается с помощью маски, предложенной Ойяла [22]. Таким образом, 15–18 элементами характеристического вектора являются взвешенные по Ойяла: минимум разности гистограмм (*Ojala minimum histogram difference*); абсолютная разность гистограмм (*Ojala absolute histogram difference*); взаимная энтропия (*Ojala mutual entropy*) и расстояние Кульбака–Лейблера (*Ojala Kullback–Leibler distance*) соотвественно.

Существует ряд методов стеганоанализа, опирающихся на изменения в гистограммах изображений, вызванные их стеганопреобразованием. Так, стеганоанализ с построением характеристических векторов на основе гистограмм предложен, например, в работе [23]. Авторы этой работы рассматривали как контейнеры цветные изображения в форматах *bmp* и *jpeg*. Характеристический вектор, предложенный в данном исследовании, содержит 24 элемента. Первые шесть – это математическое ожидание и дисперсия гистограмм каждой из цветовых составляющих контейнера (красной, зеленой и синей). Кроме того, авторы предлагают анализировать статистику в частотной области гистограмм: к последовательностям значений гистограмм цветовых каналов применяется дискретное преобразование Фурье, затем вычисляются математическое ожидание, дисперсия, асимметрия и эксцесс полученных коэффициентов, составляющих следующие 12 значений характеристического вектора. Еще три значения вектора рассчитываются как полная энергия коэффициентов Фурье красного, зеленого и синего каналов. И последние три значения представляют собой математическое ожидание разности гистограмм во временной и частотной области для каждой цветовой составляющей. Численные эксперименты [23] показали, что метод авторов имеет лучшую точность в сравнении с методом, предложенным в [24], где используется 432-элементный характеристический вектор, полученный на основе статистики амплитуд и фаз коэффициентов кратномасштабного разложения контейнера.

Кроме изложенных вариантов, характеристические векторы могут быть также вычислены на основе матрицы смежности изображения [25, 26], статистики вейвлет-коэффициентов [27–29], коэффициентов контурлет-преобразования (*contourlet transform*) [30, 31] и других способов формирования признаков контейнеров, а также путем объединения признаков, полученных в различных областях представления контейнера в единый характеристический вектор [32].

Способы решения задачи классификации

Рассмотрим классификаторы, применяемые в стеганоанализе для различения пустых и заполненных контейнеров.

В работах [33, 34] для классификации применяется метод k ближайших соседей (*k nearest neighbor*). Это простейший метрический классификатор, основанный на оценивании сходства объектов. Классифицируемый объект относится к тому классу, которому принадлежит большинство из k его соседей, т.е. ближайших к нему объектов обучающей выборки. Метод k ближайших соседей неявно опирается на одно важное предположение, называемое гипотезой компактности: если мера сходства объектов введена удачно, то схожие объекты гораздо чаще лежат в одном классе, чем в разных. В этом случае граница между классами имеет достаточно простую форму, а классы образуют компактно локализованные области в пространстве объектов. Отметим, что для оценки сходства объектов в данном методе обычно используется мера расстояния Евклида.

Следующий возможный вариант – использование наивного байесовского классификатора. Это простой вероятностный классификатор, основанный на теореме Байеса со строгими предположениями о независимости. Теорема Байеса позволяет переставить местами причину и следствие. Зная, с какой вероятностью причина приводит к некоему событию, эта те-

орема позволяет рассчитать вероятность того, что именно эта причина привела к наблюдаемому событию. Наивный байесовский классификатор удобен в случаях, когда размерность характеристического вектора велика и имеется относительно небольшая обучающая выборка. Его применение в целях стеганоанализа описано, например, в работах [35, 36].

В работах [37, 38] для классификации пустых и заполненных контейнеров использован еще один из классических методов интеллектуального анализа данных – деревья решений. Последние представляют собой последовательные иерархические структуры, состоящие из узлов, содержащих правила, т.е. логические конструкции вида *если ... то ...*. Конечными узлами дерева служат *листья*, соответствующие найденным решениям и объединяющие некоторое количество объектов рассматриваемой выборки. Каждому объекту соответствует единственный узел, дающий решение. Чтобы классифицировать новый объект, следует спуститься по дереву до листа и выдать соответствующее значение. Существует значительное число алгоритмов, реализующих деревья решений: *CART*, *C*4.5, *NewId*, *ITrule*, *CHAID*, *CN*2 и др.

В качестве классификатора можно также использовать нейронные сети, основу которых составляют нейроны – элементы, имитирующие работу нейронов головного мозга и характеризуются своим состоянием. У нейронов есть входы (синапсы), соединенные с выходами других нейронов, и есть выход (аксон), сигнал с которого поступает на синапсы других нейронов. Каждый синапс характеризуется величиной синаптической связи, называемой весом. Состояние нейрона определяется как сумма состояний его входов. Значение на выходе нейрона – это функция от его состояния. Данная функция называется *активационной* и может иметь различный вид, чаще всего используется логистическая функция или функция *S*-образного вида (сигмоид). На нейроны самого нижнего слоя подаются значения входных параметров (в данном случае это значения элементов характеристического вектора). Эти значения воспринимаются сетью как сигналы, передаваемые в следующий слой, ослабляясь или усиливаясь в зависимости от весов связей. В результате на выходе нейрона верхнего слоя вырабатывается некоторое значение, рассматриваемое как ответ – отклик всей сети на входные параметры. Для того чтобы сеть работала, нужно выполнить ее обучение, состоящее в подборе весов межнейронных связей, обеспечивающих наибольшую близость получаемых ответов к известным правильным. Самый распространенный тип нейросетей – многослойный перцептрон, который состоит из таких слоев: входной (сенсорный), один или несколько скрытых и выходной. Задача классификации при наличии двух классов (пустые и заполненные контейнеры) может быть решена на сети с одним нейроном в выходном слое, который может принимать одно из двух значений – ноль или единица, в зависимости от того, какому классу принадлежит образец. Нейронные сети применены для классификации контейнеров, например [39, 40].

В работах [41, 42] инструментом классификации выступает дискриминантный анализ, основная идея которого заключается в том, чтобы определить, отличаются ли совокупности объектов по среднему какого-либо их признака (или линейной комбинации признаков), а затем использовать этот признак, чтобы предсказать для новых членов их принадлежность к тому или иному классу. Это достигается применением статистического правила максимизации межклассовой дисперсии относительно внутриклассовой. В рамках линейного дискриминантного анализа осуществляется нахождение линейных комбинаций признаков, наилучшим образом разделяющих два или более классов объектов или событий. В отличие от других вариантов классификации дискриминантный анализ в стеганоаналитических методах может быть применен еще и с целью уменьшения размерности характеристического вектора путем исключения из него наименее информативных элементов.

Отметим, что чаще всего для классификации контейнеров в стеганоаналитических исследованиях применяется метод опорных век-

торов. (*SVM – support vector machine*) – бинарный классификатор, относящийся к граничным методам классификации [43–45]. Он позволяет получить функцию классификации с минимальной оценкой ошибки классификации, а также использовать линейный классификатор для работы с линейно неразделимыми данными. Основная проблема метода – выбор оптимальной гиперплоскости, позволяющей разделить классы с максимальной точностью. Для этого разделяющая гиперплоскость выбирается так, чтобы расстояние между ближайшими объектами, расположенными по разные стороны от нее, было 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*). Для решения задач стеганоанализа наиболее активно используется гауссово ядро (*RBF*, *Radial Basis Functions*), но в отдельных случаях наилучшая точность обеспечивается линейным или полиномиальным ядрами.

Заключение. Анализ позволяет сделать выводы о том, что наиболее перспективным есть дальнейшее развитие статистических методов, поскольку они более чувствительны, чем визуальное или звуковое восприятие и более гибки в сравнении с сигнатурным стеганоанализом. Несомненное преимущество статистических методов с обучением – это их универсальная природа и потенциальная возможность обнаруживать усовершенствованные и новые методы сокрытия данных путем переобучения классификатора на соответствующих стеганоконтейнерах, а также реконфигурирования характеристических векторов.

1. *Steganography* software. – http://www.jjtc.com/Steganography/tools.html
2. *Конахович Г.Ф.*, *Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
3. *Кошкина Н.В.* Методы синхронизации цифровых водяных знаков // Кибернетика и системный анализ. – 2008. – № 1. – С. 180–188.
4. *Кошкина Н.В.* Обзор спектральных методов внедрения цифровых водяных знаков в аудиосигналы // Проблемы управления и информатики. – 2010. – № 5. – С. 132–144.
5. *Кошкина Н.В.*, *Задирака В.К.* Спектральные методы решения задач компьютерной стеганографии // Там же. – 2011. – № 4. – С. 132–151.
6. *Кошкина Н.В.* Стеганоанализ изображений в формате *jpeg* на базе атаки контрольным внедрением // УСиМ. – 2014. – № 4. – С. 3–17.
7. *Кошкина Н.В.* Определение инварианта к сжатию с потерями для аудиосигналов // Там же. – 2010. – № 3. – С. 86–93.
8. *Швідченко І.В.* Аналіз програмного забезпечення зі стеганоаналізу // Искусственный интеллект. – 2012. – № 3. – С. 487–495.
9. *Hawi T.A.*, *Qutayari M.A.*, *Barada H.* Steganalysis attacks on stego images using stego-signatures and statistical image properties // TENCON'2004, Region 10 Conf. – 2004. – **2**. – P. 104–107.
10. *An attack* to BPCS-steganography using complexity histogram and countermeasure / M. Niimi, T. Ei, H. Noda et al. // Proc. – Int. Conf. on Image Processing, ICIP. – 2004. – **5**. – P. 733–736.
11. *Fridrich J.*, *Goljan M.* Practical steganalysis of digital images-state of the art // Proc. SPIE Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents. – 2002. – **4675**. – P. 1–13.
12. *Fridrich J.*, *Goljan M.*, *Du R.* Steganalysis based on JPEG compatibility // SPIE Multimedia Syst. and Appl. IV. – 2001. – P. 275–280.
13. *Задірака В.К.*, *Кошкіна Н.В.*, *Олексюк О.С.* Аналіз стійкості стеганографічних систем в моделі пасивного противника // Искусственный интеллект. – 2004. – № 3. – С. 801–805.
14. *Солодуха Р.А.*, *Машуков Д.В.* Опыт сигнатурного анализа стеганографической программы *S-Tools* // Вестн. Воронеж. ин-та МВД России. – 2013. – № 2. – С. 253–259.
15. *Westfeld A.*, *Pfitzmann A.* Attacks on steganographic systems // Information Hiding: 3rd Int. Workshop. – 1999. – P. 61–76.
16. *Fridrich J.*, *Goljan M.*, *Du R.* Reliable detection of LSB steganography in grayscale and color images // Proc. of the ACM Workshop on Multimedia and Security. – 2001. – P. 27–30.
17. *Dumitrescu S.*, *Wu X.*, *Wang Z.* Detection of LSB steganography via sample pair analysis // Information Hiding, 5th Int. Workshop. – 2003. – **2578**. – P. 355–372.
18. *Avcibas I.*, *Memon N.D.*, *Sankur B.* Steganalysis using image quality metrics // IEEE Transactions on Image Proc. – 2003. – **12**, № 2. – P. 221–229.

19. *Kutter M.*, *Jordan F.* JK-PGS (Pretty Good Signature). – http://ltswww.epfl.ch/~kutter/watermarking/JK_PGS.html
20. *Shi Y.*, *Chen C.*, *Chen W.* A Markov process based approach to effective attacking JPEG steganography // Proc. of the 8th Int. Workshop. – 2006. – P. 249–264.
21. *Image* steganalysis with binary similarity measures / I. Avcibas, M. Kharrazi, N. Memon et al. // EURASIP J. on Appl. Signal Processing. – 2005. – P. 2749–2757.
22. *Ojala T.*, *Pietikainen M.*, *Harwood D.* A comparative study of texture measures with classification based on feature distributions // Patt. Recog. – 1996. – **29**, № 1. – P. 51–59.
23. *Detecting* original image using histogram, DFT and SVM / T.H. Manjula Devi, H.S. Manjunatha Reddy, K.B. Raja et al. // Int. j. of recent trends in engin. – 2009. – **1**, № 1. – P. 367–371.
24. *Lyu S.*, *Farid H.* Steganalysis using higher-order image statistics // IEEE Transaction on Information Forensics and Security. – 2006. – **1**. – P. 111–119.
25. *JPEG* steganalysis with high-dimensional features and bayesian ensemble classifier / F. Li, X. Zhang, B. Chen et al. // IEEE signal processing letters. – 2013. – **20**, № 3. – P. 233–236.
26. *Sun Z.*, *Hui M.*, *Guan C.* Steganalysis based on co-occurrence matrix of differential image // Intelligent information hiding and multimedia signal processing. – 2008. – P. 1097–1100.
27. *Lyu S.*, *Farid H.* Steganalysis using color wavelet statistics and one-class vector support machines // Proc. of SPIE, Security, Steganography, Watermarking of Multimedia Contents. – 2004. – **5306**. – P. 35–45.
28. *Zhan S.H.*, *Zhang H.B.* Blind steganalysis using wavelet statistics and ANOVA // Machine Learning and Cybernetics, Int. Conf. – 2007. – **5**. – P. 2515–2519.
29. *Image* universal steganalysis based on wavelet packet transform / X. Luo, F. Liu, J. Chen et al. // Multimedia Signal Processing, IEEE 10th Workshop on Digital. – 2008. – P. 780–784.
30. *Sheikhan M.*, *Moin M.*, *Pezhmanpour M.* Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform // 10th Int. Conf. on Intelligent Syst. Design and Appl. (ISDA). – 2010. – P. 368–372.
31. *Natarajan V.*, *Anitha R.* Blind image steganalysis based on contourlet transform // Int. J. on Cryptography and Information Security (IJCIS). – 2012. – **2**, № 3. – P. 77–87.
32. *Yan Y.*, *Li L.*, *Zhang Q.* Universal steganalysis method based on multi-domain features // J. of Information & Comp. Sci. – 2013. – P. 2177–2185.
33. *Yamini B.*, *Sabitha R.* Blind steganalytic attack as pattern recognition using k-nearest neighbour classification technique // Fifth Int. Conf. on advanced comp. – 2013. – P. 677–682.
34. *Dautrich J.* Multi-class steganalysis // Machine learning course research project distinguishing images embedded using reversible steganographic schemes. – 2009. – P. 1–6.
35. *Kaipa B.*, *Robila S.A.* Statistical steganalyis of images using open source software // Appl. and technol. conf. (LISAT). – 2010. – P. 1–5.
36. An algorithm of echo steganalysis based on bayes classifier / W. Zeng, H. Ai, R. Hu et al. // Proc. of the 2008 IEEE Int. Conf. on Information and Automation, Zhangjiajie. – 2008. – P. 1667–1670.
37. *Geetha S.*, *Ishwarya N.*, *Kamaraj N.* Audio steganalysis with Hausdorff distance higher order statistics using a rule based decision tree paradigm // Expert syst. with appl. j. – 2010. – **37**, № 12. – P. 7469–7482.
38. *Benton R.*, *Chu H.* Soft computing approach to steganalysis of LSB embedding in digital images // 3rd Int. Conf. on Inf. Technol.: Research and Education. – 2005. – P. 105–109.
39. *Nissar A.*, *Mir A.H.* Texture based steganalysis of grayscale images using neural network // Signal processing research. – 2013. – **2**, № 1. – P. 17–24.
40. *Ghanbari S.*, *Keshtegary M.*, *Ghanbari N.* New steganalysis method using glcm and neural network // Int. j. of comp. appl. – 2012. – **42**, № 7. – P. 45–50.
41. *Rajput G.*, *Agrawal R.K.*, *Aggarwal N.* Performance evaluation of exponential discriminant analysis with feature selection for steganalysis // Defence science j. – 2012. – **62**, № 1. – P. 19–24.
42. *Universal* image steganalysis based on wavelet packet decomposition and empirical transition matrix in wavelet domain / X. Yang, Y. Lei, X. Pan et al. // Int. forum on comp. sci.-technol. and appl. (IFCSTA). – 2009. – **2**. – P. 179–182.
43. *Ru X.*, *Zhuang Y.*, *Wu F.* Audio steganalysis based on «negative resonance phenomenon» caused by steganographic tools // J. of Zhejiang University SCIENCE A. – 2006. – **7**, № 4. – P. 577–583.
44. *Johnson M.*, *Lyu S.*, *Farid H.* Steganalysis of Recorded Speech // Proc. SPIE. – 2005. – **5681**. – P. 664–672.
45. *Lyu S.*, *Farid H.* Steganalysis using color wavelet statistics and one-class support vector machines // Proc. of the SPIE. – 2004. – **5306**. – P. 35–45.

Поступила 10.02.2015
+38 044 526-4569 (Киев)
E-mail: *nata.koshkina@gmail.com*