т.е. один детектор способен обнаружить большее количество вирусов.
2. Один (или однотипные) детектор не в состоянии обнаружить все разновидности вирусов, так как невозможно приобрести структуру детектора, которая была бы схожа с большим многообразием вредоносных программ.
3. ИИС способна распознавать чистые файлы и вредоносные программы и обнаруживать неизвестные вирусы. Вероятность возникновения ошибки очень мала, что делает такую систему привлекательной для использования в системах защиты информации. Использование ИИС совместно с уже существующими антивирусными продуктами значительно увеличит уровень защиты компьютерной системы

Исследования проводятся в рамках научно-исследовательского проекта по теме «Методы искусственного интеллекта для защиты информации» по заказу Министерства образования Республики Беларусь.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Почему не срабатывают антивирусы – http://www.i2r.ru, 2003.
2. L de Castro and J Timmis. Artificial Immune Systems: A New Computational Intelligence Approach. Springer, 2002.
3. С.В. Безобразов. Искусственные иммунные системы для защиты информации: сравнительный анализ методов негативной и позитивной селекций детекторов // Инженерный вестник.-2006.- №1(21)/1.-С.76-82.
4. Иммунитет. Энциклопедия «Кругосвет» – http://krugosvet.ru, 2004.
5. С.В. Безобразов. Применение искусственных иммунных систем для обнаружения вирусов // Вестник БрГТУ. Физика, математика, информатика.-2005.- №5(35).-С.66-70.
6. F. Esponda, S. Forrest, and P. Helman. A formal framework for positive and negative detection. IEEE Transactions on Systems, Man, and Cybernetics 34:1 pp. 357-373, 2004.
7. Kohonen T. Sell-organised formation of topologically correct feature maps// Biological Cybernetics. - 1982. - N43.-P.59-69.
8. В.Медведев, В.Потемкин. Нейронные сети. MATLAB 6. М: Диалог-МИФИ. 2002. 496 с.
9. В.А. Головко. Нейронные сети: обучение, организация и применение. Кн. 10: Учеб. пособие для вузов / Общая ред. А. И. Галушкина. - М.: ИПРЖР, 2000. –С.114-129.

Статья поступила в редакцию 21.12.2006

УДК 681.3

Горбашко Л.А.

АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ С ВЕКТОРНЫМ КВАНТОВАНИЕМ

Введение

Задача защиты информации от несанкционированного доступа приобретает все большую актуальность в современном мире. Развитие информационных технологий дало новый толчок для развития компьютерной стеганографии. Стеганография исследует скрытую передачу данных в маскирующем сигнале.

Для скрытой передачи информации выбирается контейнер, которым чаще всего служит графический файл. В него особым образом встраивается сообщение, которое нужно передать тайно. В результате получается комбинированное изображение – стего, которое и передается по каналу связи.

Современные исследования направлены на встраивание информации в частотной области. При этом перед встраиванием данных производят разложение контейнера на любые частотные составляющие (преобразования Фурье, вейвлет-, дискретное косинусное и т.п.).

При встраивании текстового сообщения необходимо обеспечить его извлечение без искажений, для чего применяются дублирование сообщения, избыточное кодирование. Соответственно, объем встраиваемых данных в этом случае невелик и составляет примерно 1% от размера контейнера [1]. При встраивании цифровых данных, имеющих аналоговую природу - изображения, звуковые файлы - можно допустить некоторое искажение оригинала при встраивании, т.к. человеческие органы чувств, воспринимающие информацию, не являются идеальными. Небольшие отклонения цветов изображения либо амплитуды и частоты звука не определяются человеком. Поэтому появляется возможность значительно увеличить объем встраиваемых данных, используя предварительное сжатие сообщения. Методы сжатия могут быть различны от отбрасывания нулевых коэффициентов после частотного разложения сообщения до предварительного квантования и кодирования сообщения.

Таким образом, современной проблемой стеганографии является увеличение объема встроенных данных при сохранении прозрачности и робастности стего. Для этого применяются различные методы, в частности, сжатие данных перед встраиванием. Одним из способом сжатия является применение различных методов квантования.

Применение квантования в стеганографии

Квантование является одним из способов сокращения объема информации. В стеганографии широко используются все виды квантования. Так, линейное и решетчатое квантование используются авторами в работах [1, 2].

Линейное квантование заключается в замене каждого отсчета сигнала на число, кратное шагу квантования. В результате уменьшается множество возможных значений сигнала. При встраивании сообщения в квантованный контейнер по аддитивному алгоритму отсчеты сигнала изменяются на произвольную величину, равную значениям отсчетов сообщения.

При линейном квантовании сообщения его можно закодировать при помощи алгоритма Кодирование длин серий (RLE – Run Length Encoding).Сжатие сообщения в данном алгоритме происходит за счет того, что в квантованном изображении встречаются последовательности одинаковых чисел. Тогда их можно заменить на пары <количество повторений, значение> [3]. После такого предварительного сжатия сообщения получим увеличение объема внедренных данных при встраивании.

Если предварительно использовать линейное квантование контейнера, то ограничение набора возможных значений отсчетов контейнера дает возможность извлечь сообщение без знания контейнера. Достаточно проквантовать стего с тем же шагом и вычислить разность между принятым стего и квантованным стего- это и будет встроенное сообщение. Реализация

***Горбашко Лариса Ашотовна**, ст. преподаватель кафедры интеллектуальных информационных технологий БрГТУ, lagorbashko@bstu.by.*
Беларусь, Брестский государственный технический университет, 224017, Беларусь, г. Брест, ул. Московская, 267.

данного алгоритма для встраивания текстовых сообщений описана в [1].

Решетчатое квантование похоже на линейное, разница лишь в том, что шаг квантования представляет собой не фиксированную величину, а таблицу значений, т.н. матрицу квантования. Каждый отсчет должен быть кратен числу, находящемуся на соответствующей позиции матрицы квантования. Такая матрица квантования заложена, например, в стандарте сжатия JPEG [3].

При векторном квантовании весь набор отсчетов сигнала разбивается на векторы, векторы объединяются в группы (кластеры). Каждый кластер представлен одним вектором, т.е. каждый n-мерный вектор X изображения заменяется на n-мерный вектор Y, представляющий данный кластер. Набор векторов Y называется *кодовой книгой (codebook)*. После построения кодовой книги проводят квантование изображения, заменяя каждый вектор изображения на индекс ближайшего по евклидову расстоянию вектора.

При восстановлении изображения каждый индекс заменяется на вектор из кодовой книги с соответствующим номером. Поскольку вектор не точно соответствует исходному, при квантовании неизбежно возникают искажения.

Кодовая книга может быть построена заранее и применяться для всех изображений – это *фиксированная* кодовая книга. Параметрами для построения фиксированной кодовой книги служат размерность вектора и евклидово расстояние. В любом случае такая книга имеет достаточно большой размер, т.к. представляет из себя перебор всех возможных значений векторов. Удобство ее использования состоит в том, что не требуется ее передача по каналу связи.

Кодовая книга может строиться специально для каждого изображения – это *адаптивная* кодовая книга. В этом случае, безусловно, уменьшится ее размер, т.к. в книгу включаются только те значения векторов, которые присутствуют в данном конкретном изображении. Недостаток, соответственно, состоит в необходимости передачи ее по каналу связи, что повышает вероятность успешной атаки на стего.

Построение оптимальной кодовой книги является достаточно сложной задачей[4]. Кодовая книга должна быть известна получателю сообщения.

В стеганографии векторное квантование применяют для кодирования встраиваемого сообщения, таким образом, достигается увеличение объема встроенных данных.

Скрытие изображений с использованием векторного квантования

Для внедрения изображения- сообщения в изображение-контейнер был разработан алгоритм:

1. Дискретные отсчеты контейнера подвергаем двумерному вейвлет- преобразованию Хаара.
2. Строим кодовую книгу.
3. Производим векторное квантование (кодирование) сообщения.
4. Индексы векторов встраиваем в вейвлет-коэффициенты аппроксимации контейнера по аддитивному алгоритму [5], коэффициенты детализации остаются неизменными.
5. Производим обратное вейвлет- преобразование и получаем стего.

Извлечение сообщения происходит при известном контейнере. Кроме того, должна быть известна кодовая книга. Ее можно передавать по другому каналу связи либо использовать фиксированную кодовую книгу. Однако следует учесть, что использование фиксированной кодовой книги повышает степень защиты информации, т.к. нет необходимости передавать ее по каналу связи, а извлечение сообщения без кодовой книги не представляется возможным. Последовательность действий при извлечении сообщения обратна последовательности встраивания.

Характеристика двух методов квантования

Предложенный алгоритм был реализован в двух вариантах.

Первый вариант (назовем его VQ- векторный квантователь) представляет собой обычное векторное квантование [6]. Рассчитаем объем кодовой книги в случае ее фиксированных значений. Число возможных размещений из n различимых вариантов по m с повторениями: $A_n^m = n^m$.

Длина вектора составляет 8 значений, m=8. Количество возможных значений каждого байта зависит от евклидова расстояния E при квантовании. При использовании E=128 цвет каждой точки может отличаться друг от друга на 16 единиц, т.е. количество различимых элементов n=256/16 =16. Тогда количество размещений $A_n^m = 16^8 = 2^{32}$

При размере вектора 8 байт размер фиксированной кодовой книги составит $2^{32}\times8=2^5\times2^{30}$=32 Гб.

Безусловно, хранение такой кодовой книги при современном уровне развития периферийных устройств ПК не представляется целесообразным. Кроме того, даже при возможности хранения такого объема информации кодирование изображения при встраивании занимает недопустимо много времени.

Поэтому в данном варианте создается адаптивная кодовая книга, которую необходимо передавать по каналу связи. Реализация показала, что размер такой кодовой книги зависит от характера изображения и составляет при E=128 порядка 50 векторов, или 50×8=400 байт.

Второй вариант (назовем его LVQ)заключается в использовании нейронной сети [7]. Обучающийся векторный квантователь LVQ (learning vector quantizer) реализуется с помощью сети Кохонена. В этом случае требуется заранее обучить сеть на любой выборке векторов с длиной 8 путем изменения весовых коэффициентов нейронов, затем сохранить конфигурацию нейронной сети. Получим фиксированную кодовую книгу, которую можно использовать для квантования любого изображения, поэтому нет необходимости передавать ее по каналу связи. Размер полученного файла составляет 795 Кбайт.

Анализ производительности методов

Сравним производительность методов скрытия сообщения с использованием векторного квантования в двух вариантах. Для этого выработаем критерии сравнения методов. Т.к. во втором варианте используется фиксированная кодовая книга, то она может быть создана один раз за некоторый период времени, поэтому время создания кодовой книги (или, соответственно, обучения нейронной сети) не будем рассматривать при анализе. Тем не менее, заметим, что время для первого варианта незначительно и сравнимо с временем квантования, но достаточно велико для второго варианта и составляет 1-4 часа.

В качестве критерия используем *время квантования* сообщения при известной кодовой книге, *время обратного квантования* (восстановления изображения на приемной стороне по извлеченным индексам).

Одна из серьезных проблем обработки изображений заключается в том, что до сих пор не найден адекватный критерий оценки потерь качества изображения. А теряется оно постоянно – при переводе в другую систему цветов, при квантовании, сжатии, действии помех при передаче по каналу связи. Можно применить *критерий среднеквадратичного отклонения* значений пикселов от оригинала (или root mean square RMS):

$$d(x,y) = \sqrt{\frac{\sum_{i=1,j=1}^{n,n} \left(x_{ij} - y_{ij}\right)^2}{n^2}}.$$

По нему изображение будет сильно испорчено при понижении яркости на 5%, но человеческий глаз этого не заметит. В то же время изображения «со снегом» – изменение цвета отдельных точек, полос, «муаром» - будут признаны хорошими. Можно оценить изменение качества изображения по максимальному отклонению: $d(x,y) = \max_{ij} \left| x_{ij} - y_{ij} \right|$.

Эта мера чувствительна к биению отдельных пикселов. Т.е. существенно изменить значение только одного пиксела, что практически будет незаметно для глаза, изображение по этому критерию испорчено.

Мера, которую сейчас используют на практике – пиковое отношение сигнал/ шум (peak signal-to-noise ratio, PSNR) [3]:

$$d(x,y) = 10 lg \frac{255^2 \cdot n^2}{\sum_{i=1,j=1}^{n,n} \left(x_{ij} - y_{ij} \right)^2}.$$

Данная мера аналогична среднеквадратичному отклонению, но пользоваться ей удобней из-за логарифмического масштаба шкалы.

Качество изображения оценим по пиковому отношению сигнал/ шум *PSNR*.

Поскольку первый вариант больше зависим от исходных данных, вычислим сначала по экспериментальным данным его усредненные характеристики (таблица 1). Единицы измерения можно не учитывать, т.к. нам необходимы относительные величины.

Таблица 1

Критерий сравнения	**Опыт 1**	**Опыт 2**	**Опыт 3**	**Средние значения**
Размер контейнера	256x256			-
Размер сообщения	64x64			-
Евклидово расстояние	64	128	192	-
PSNR	50,3483	73,0174	68,0488	63,8048
Время квантования	3,104	2,444	2,253	2,60033
Время обратного квантования	0,05	0,05	0,05	0,05

Таблица 2

	Опыт 1		**Опыт 2**	
Критерий сравнения	**VQ**	**LVQ**	**VQ**	**LVQ**
Размер контейнера	256x256		256x256	
Размер сообщения	64x64		192x192	
PSNR	63,8	18-46	12,0	23,0
Время квантования	2,6	2,6	55,1	24,9
Время обратного квантования	0,05	69,91	3,27	731,50

Теперь проведем сравнение методов первого и второго вариантов (таблица 2) по выбранным критериям - времени квантования, времени обратного квантования, пиковому отношению сигнал/ шум.

Из табл.2 видно, что метод LVQ имеет значительно большее время обратного квантования, т.е. на приемной стороне необходимо затратить значительное время на извлечение изображения. Однако на приемной стороне выигрыш в скорости квантования примерно в 2 раза дает метод LVQ при увеличении объема встроенного сообщения. При малых объемах сообщения скорости квантования примерно одинаковы. Качество восстановленного изображения при малых объемах сообщения оставляет желать лучшего, однако при больших объемах сообщения метод LVQ превосходит метод VQ по качеству изображения в 2 раза.

Таким образом, при больших объемах встраиваемых данных несомненными преимуществами обладает метод с использованием нейронной сети LVQ.

Выводы

На основании проведенных исследований можно выработать рекомендации при использовании методов векторного квантования в стеганографии:

- При небольших объемах внедряемых данных лучшие результаты дает метод VQ с использованием адаптивной кодовой книги, например, при внедрении цифровых водяных знаков. Для подтверждения авторских прав необходимо иметь кодовую книгу. Кодовая книга этого метода небольшая, вполне может храниться вместе с логотипом внедренного изображения. Если уровень секретности тайного канала связи позволяет передавать кодовую книгу и у получателя не располагает временем для извлечения сообщения, то метод VQ может быть использован и для организации тайного канала связи.
- При значительных объемах внедряемых данных целесообразно применить метод `LVQ с фиксированной кодовой книгой, например, для организации тайного канала связи. Кодовая книга создается заранее и хранится на приемной и передающей сторонах без передачи по каналу связи, что повышает уровень секретности; уменьшается также время встраивания. При этом надо учесть, что время извлечения сообщения на приемной стороне все же возрастает в сотни раз, т.е. получатель должен иметь временной ресурс, получая взамен более высокое качество изображения.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Larisa Gorbashko. A Text Data Hiding and Recovering without Host Image. – Proceeding of PRIP'2005, Minsk, 2005.
2. Mukherjee D., Chae J.J., Mitra S.K. A source and Channel Coding Approach to Data Hiding with Application to Hiding Speech in Video. Proceeding of IEEE ICIP'98, Chicago, Oct. 1998, Vol.1, pp.348-352.
3. Ватолин Д. И др. Методы сжатия данных.-М.: Диалог-МИФИ, 2003.
4. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. – М.: Триумф, 2003.
5. Грибунин В.А. Цифровая стеганография. – М.: Эксмо, 2002.
6. Горбашко Л.А. Метод скрытия изображений с применением векторного квантования.
7. Larisa Gorbashko, Vladimir Golovko. A Steganographic Method Using Learning Vector Quantization. –Proceedings of ICNNAI'2006, Brest, 2006.

Статья поступила в редакцию 21.12.2006

УДК 004.8.032.26

Кочурко П.А.

РАСПОЗНАВАНИЕ КЛАССОВ СЕТЕВЫХ АТАК: ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ РАЗЛИЧНЫХ АРХИТЕКТУР

1. Введение

Среди задач системы защиты информации, реализующей механизмы обнаружения атак [1, стр. 96], выделяют в том числе качественное распознавание известных и, зачастую,

***Кочурко Павел Анатольевич**, аспирант кафедры интеллектуальных информационных технологий БрГТУ.*
Беларусь, Брестский государственный технический университет, 224017, Беларусь, г. Брест, ул. Московская, 267.