Рисунок 5. Статистика приближения результата к эталонному значению при распознавании

нерации занимают меньше времени, чем вычисления единственной итерации алгоритма обратного распространения.

В целом, генетические алгоритмы значительно выигрывают у схемы обратного распространения в задаче распознавания профилограмм УДЧ, позволяя получать лучшие векторы весовых коэффициентов за существенно меньшее количество времени.

СПИСОК ЛИТЕРЕТУРЫ

1. Rumelhart, D.E. Learning internal representations by error propagation / D.E. Rumelhart, G.E. Hinton, R.J. Williams // Parallel Distributed Processing.- 1986.- V.1.- p. 318–362.
2. Montana, D.J. Training Feedforward Neural Networks Using Genetic Algorithms / D.J. Montana, L. Davis // Proceedings of the Eleventh International Joint Conference on Artificial Intelligence, Detroit, MI.- 1989.- p. 762–767.
3. Prudencio, R.B.C. Evolutionary Design of Neural Networks: Aplication to River Flow Prediction / R.B.C. Prudencio, T.B. Ludemir // Proceedings of the International Conference on Artificial Inteligence and Aplications.-2001.- p. 56–66.
4. Prudencio, R.B.C. Design of Neural Networks for Time Series Prediction Using Case-Initialized Genetic Algorithms / R.B.C. Prudencio, T.B. Ludemir // Proceedings of the 8th International Conference on Neural Information Processing, ICONIP.- 2001.- p. 990–995.

Д.т.н., дир. ***Липанов А.М.****, к.ф.-м.н., с.н.с.* ***Тюриков А.В.****, аспирант* ***Суворов А.С.****, д.т.н., с.н.с.* ***Шелковников Е.Ю.****, к.т.н., с.н.с. Гуляев П.В. – (3412) 21-89-55, iit@udman.ru - Институт прикладной механики УрО РАН.*

УДК: 004.032.26

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В СЛЕПЫХ МЕТОДАХ ОБНАРУЖЕНИЯ ВСТРОЕННОЙ СТЕГАНОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

А.Ж. Абденов, Л.С. Леонов

В статье рассматривается слепой метод обнаружения встроенной стеганографической информации в цифровых изображениях. В качестве вектора признаков изображения используются статистические моменты в частотной области гистограмм вейвлет-коэффициентов, вычисленных на глубину разложения 3. Классификация обучающей базы данных проводилась с помощью нейронных сетей.

Ключевые слова: стеганография, стегоанализ, нейронные сети, RBF-сети, дискретное преобразование Фурье, вейвлет-преобразование.

Введение.

Стеганография – искусство невидимой коммуникации. Цель стеганографии скрыть сам факт наличия связи. Это достигается путем внедрения скрытых сообщений в различную мультимедийную информацию – цифровые изображения, видео и звуковые файлы. Исходное изображение (в данной работе будем рассматривать только случай цифровых изображений) называют контейнером, а изо-

бражение со встроенной информацией – стего, или стего-изображением. За счет избыточности представления мультимедийной информации (например, человек не может различить цвет с номером 250 и 251) возможно встраивание информации в контейнеры без заметного визуального искажения.

Стегоанализ – искусство обнаружения скрытой в контейнерах информации [1,2]. Стеганографическая система передачи информации считается безопасной, если набор стего изображений имеет точно такие же статистические характеристики, как и набор изображений-контейнеров.

Стегоаналитические методы можно разделить на два класса: методы обнаружения определенного стеганографического алгоритма, когда алгоритм встраивания известен, и слепые методы, при использовании которых алгоритм встраивания неизвестен.

В методах первой группы фактически восстанавливается ход работы стеганографического алгоритма. Из преимуществ такого подхода можно отметить максимальную точность и надежность обнаружения при условии справедливости сделанных априорных предположений об используемом алгоритме. Однако, даже при незначительном отличии метода встраивания от предполагаемого, например использовании блочного разбиения изображения нестандартного размера, вероятность обнаружения встроенного сообщения значительно снизится.

Слепые стегоаналитические методы являются наиболее перспективным направлением. Данный подход основан на оценке вектора признаков изображения. Далее, в зависимости от задачи стегоанализа производится либо многомерная классификация полученного вектора признаков, либо вычисление многомерной функции оценки длины встроенного сообщения. Преимущества данного подхода заключаются в его универсальности.

Постановка задачи.

На основании имеющейся базы данных контейнеров и стего определить наличие встроенного в изображение сообщения.

Методика решения задачи.

Будем рассматривать слепой метод обнаружения встроенной стеганографической информации в цифровых изображениях. Т.е. такой метод потенциально сможет обнаруживать использование любого стеганографического алгоритма сокрытия информации.

При работе любого слепого алгоритма обнаружения встроенной информации можно выделить следующие этапы:

1) построение многомерного пространства признаков изображения;
2) анализ различий исходных изображений и стего в пространстве признаков;
3) классификация базы данных исходных изображений и стего на две группы;
4) отнесение анализируемого изображения к изображению-контейнеру или к стего в соответствии с результатами пп.2-3.

Впервые слепая схема была описана Мемоном и Фаридом [3,4], которая состояла в следующем. Сначала проводили трехуровневое вейвлет-преобразование изображения, затем для детализирующих вейвлет-коэффициентов (горизонтального, вертикального и диагонального поддиапазонов) находили среднее, дисперсию, эксцесс и коэффициент ассиметрии. Также вычисляли вектор ошибок предсказания вейвлет-коэффициентов на основании значений соседних коэффициентов и вычисляли также точечные статистические характеристики. Таким образом получали 72-разрядный характеристический вектор изображения. Затем слепой детектор на основе 72-разрядного характеристического вектора обучали на базе данных контейнеров и стего. И проводили классификацию с помощью линейного дискриминанта Фишера. С дальнейшим развитием стеганографических средств данный метод потерял актуальность, но методология применяется во всех слепых схемах.

Выбор признаков является одним из самых важных этапов построения слепого метода обнаружения стеганографической информации. Пространство пикселей изображения преобразуется в пространство признаков и определение наличия встроенного сообщения идет уже в пространстве признаков.

В данной работе в качестве признаков будем использовать статистические моменты в частотной области гистограмм вейвлет-коэффициентов.

Использование статистических характеристик гистограмм изображений продиктовано легкостью моделирования гистограмм с помощью суммы, как правило, двух случайных нормальных переменных и полнотой представления изображения. Можно увидеть, что в частотной области отличие стего от контейнера легче различить (рисунок 1).

Статистические моменты в частотной области гистограмм определим следующим образом:

$$M_n = \sum_{k=-N/2}^{N/2} |f_k|^n \, p(f_k), \quad (1)$$

где n - порядок момента, N - количество отсчетов коэффициентов дискретного преобразования Фурье (ДПФ) для гистограммы, f_k - к-я частота в ДПФ (k=-N/2,…-1,0,1,..N/2).

$$p(f_k) = \frac{|H(f_k)|}{\sum_{k=-N/2}^{N/2} |H(f_k)|}, \quad (2)$$

где $|H(f_k)|$ - амплитуда ДПФ гистограммы $h(x_k)$,

$$H(f) = \int_{-\infty}^{\infty} h(x) e^{-j2\pi fx} dx, \quad (3)$$

где h(x) - гистограмма изображения, или другими словами, количество пикселей, принимающих значение x.

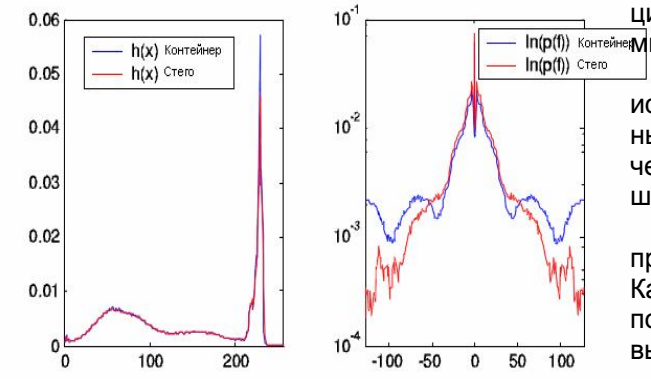

Рисунок 1 – Гистограмма изображения в пространственной области (слева) и в частотной области (справа)

Таким образом, в качестве вектора признаков изображения возьмем 36-разрядный вектор, состоящий из первых трех статистических моментов, вычисленных в частотной области для вейвлет-коэффициентов на трех уровнях разложения (3 уровня разложения x 4 типа вейвлет-коэффициентов (аппроксимационные, детализирующие горизонтальные, вертикальные и диагональные) x 3 статистических момента = 36 признаков).

Слепой метод обнаружения состоит в анализе пространства признаков для анализируемой базы данных изображений. На основе анализа базы данных пространство признаков разделяется на две группы - стего и контейнеры. В данной работе классификацию признаков проведем с помощью нейронных сетей.

Нейронные сети - это модели биологических нейронных сетей мозга, в которых нейроны имитируются относительно простыми, часто однотипными, элементами (искусственными нейронами). Нейронные сети широко используются для решения разнообразных задач. Среди областей применения нейронных сетей - автоматизация процессов распознавания образов, прогнозирование, адаптивное управление, создание экспертных систем, организация ассоциативной памяти, обработка аналоговых и цифровых сигналов, синтез и идентификация электронных цепей и систем.

Нас же интересуют следующие задачи, решаемые с помощью нейронных сетей:

Классификация (обучение с учителем). Примеры задач классификации: распознавание текста, распознавание речи, идентификация личности.

Кластеризация (обучение без учителя). Примером задачи кластеризации может быть задача сжатия информации путем уменьшения размерности данных. Задачи кластеризации решаются, например, самоорганизующимися картами Кохонена.

В данной работе нейронные сети будем использовать для классификации базы данных, использование же кластеризации (обучение без учителя) является темой дальнейших исследований.

Наилучшие результаты были получены при использовании RBF-сетей (см. рисунок 2). Каждый из n компонентов входного вектора подается на вход m базисных функций и их выходы линейно суммируются с весами $\{w_j\}_{j=1}^{m}$.

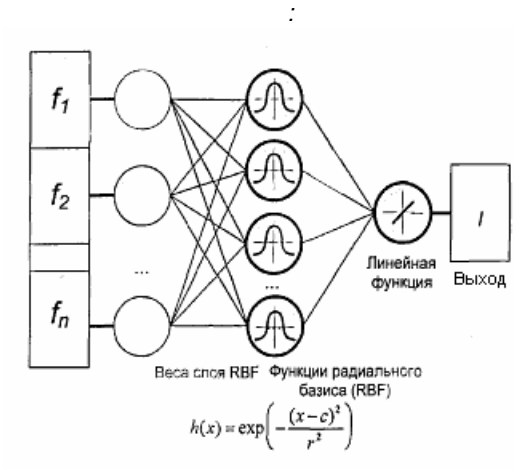

Рисунок 2 – Структура RBF-сети

Выход RBF-сети является линейной комбинацией набора базисных функций:

$$f(\bar{x}) = \sum_{j=1}^{m} w_j h_j(\bar{x}).$$

Если предположить, что параметры функции, смещение **c** и радиус **r** фиксированы, то задача нахождения весов решается методами линейной алгебры. Этот метод называется метод псевдообратных матриц и он минимизирует средний квадрат ошибки. Суть этого методы заключается в следующем.

Находится интерполяционная матрица H:

$$H = \begin{bmatrix} h_1(\overline{x_1}) \ldots h_m(\overline{x_1}) \\ \ldots\ldots\ldots\ldots\ldots \\ h_1(\overline{x_p}) \ldots h_m(\overline{x_p}) \end{bmatrix},$$

где *m* - число нейронов в скрытом слое, *p* – размер обучающей выборки, *n* – число входов сети.

На следующем этапе вычисляется инверсия произведения матрицы *H* на транспортированную матрицу *H*:

$$A^{-1} = (H^T H)^{-1}.$$

Вектор весов:

$$\overline{W} = A^{-1} H^T \overline{y}.$$

Если предположение о фиксированных параметрах функции не выполняются, т.е. помимо весов необходимо настроить параметры активационной функции каждого нейрона (смещение функции и радиус) и задача становится нелинейной. Решать ее приходится с использованием итеративных численных методов оптимизации, в частности, градиентных методов.

Существуют различные алгоритмы обучения RBF-сетей. Наиболее распространен алгоритм, использующий двухшаговую стратегию обучения или смешанное обучение [5]. Он оценивает позицию и ширину ядра с использованием алгоритма кластеризации «без учителя», а затем алгоритм минимизации среднеквадратической ошибки «с учителем» для определения весов связей между скрытыми и выходными слоями. После получения этого начального приближения используют градиентный спуск для уточнения параметров сети. Этот смешанный алгоритм обучения RBF-сети сходится гораздо быстрее, чем алгоритм обратного распространения для обучения многослойных персептронов. Однако RBF-сеть часто содержит слишком большое количество скрытых элементов. Это влечет более медленное функционирование сети.

Для адекватного обучения RBF-сети необходимо подготовить входные данные - провести анализ с помощью метода главных компонент и сжать диапазон по каждому признаку до интервала [0,1].

Среди недостатков RBF-сетей следует выделить неумение экстраполировать свои результаты за область известных данных. В многослойных персептронах такой проблемы нет.

Практические результаты.

Для обучения нейронной сети использовалась база данных, состоящая из 765 изображений, 255 являлось контейнерами, 255 стего с использованием алгоритма F5 [6], 255 стего с использованием алгоритма jsteg [7]. Изображения представлялись разными по содержанию. Это были фотографии пейзажей, животных, макросъемки, городской архитектуры, людей, компьютерная графика, отсканированные фотографии.

Из 600 изображений формировалась обучающая выборка, 165 – контрольная выборка. В результате были получены следующие результаты. Вероятность ошибки в обучающей выборке составила 0%, была построена сеть, состоящая из 400 нейронов. Вероятность ошибки на контрольной выборке – 10%. При использовании двуслойного персептрона были получены ошибки в 10% и 15% соответственно. При использовании для классификации линейного дискриминанта Фишера вероятность ошибок составила 30% и 35%.

Вывод.

В данной работе был предложен новый слепой стегоаналитический метод обнаружения встроенной информации в цифровых изображениях на основе нейронных сетей.

В качестве признаков использовались первые три статистических моментов в частотной области гистограммы вейвлет-коэффициентов, вычисленных до глубины разложения 3. Таким образом, формировался 36-разрядный вектор признаков изображения. С помощью нейронных сетей удалось провести удачную классификацию базы данных изображений с вероятностью ошибок в 0% для обучающей выборки и 10% для контрольной выборке. При использовании же традиционного линейного дискриминанта Фишера вероятность ошибок составили 30% и 35% соответственно.

СПИСОК ЛИТЕРАТУРЫ

1. Fridrich, J. Feature -Based Steganalysis for JPEG images and its Implication for Future Design of Steganographic Schemes [текст]/ J. Fridrich // 6th Information Hiding Workshop. – LNCS. - 2004. - vol.3200. Springer-Verlag,pp. 67-81.

2. Fridrich, J., Goljan M. Practical Steganalysis – State of the Art [текст]/J. Fridrich, M. Goljan // Proc. SPIE Photonics West . - Vol. 4675. - Electronic Imaging 2002, Security and Watermarking of Multimedia Contents. - San Jose, California. – 2002. - pp.1-13.
3. Farid, H., Siwei, L. Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines [текст]/H. Farid, L. Siwei // Information Hiding. 5-th International Workshop. Lecture Notes in Computer Science. - Vol. 2578. Springer-Verlag, - Berlin Hei-delberg New York. - (2002. –pp. 340–354.
4. Avcibas, I., Memon N., Sankur B. Steganalysis using Image Quality Metrics [текст]/I. Avcibas, N. Memon, B. Sankur // SPIE Security and Watermarking of Multimedia Contents II, Electronic Imaging. - San Jose,CA. – 2001.
5. Хайкин, С. Нейронные сети: полный курс [Текст]/ С. Хайкин. – М.: Издательский дом «Вильямс», 2006. – 1106 с.
6. Jsteg [электронный ресурс]: Режим доступа: http://jsteg.org/jstegtest.zip.
7. F5 [электронный ресурс]: Режим доступа: http://wwwrn.inf.tudresden.de/~westfeld/attacks.html.

Д.т.н. профессор ***Абденов А.Ж****. тел. (383)346-08-53, abdenov@ngs.ru, Новосибирский государственный технический университет; аспирант* ***Леонов Л.С.****, тел. (383)346-08-53, adanos@ngs.ru, Новосибирский государственный технический университет*

УДК: 004.651.5

ПРИМЕНЕНИЕ КАЛМАНОВСКОЙ ФИЛЬТРАЦИИ К ОПРЕДЕЛЕНИЮ ДОСТОВЕРНОСТИ ЭЛЕМЕНТОВ ИНТЕГРИРОВАННОЙ БАЗЫ ДАННЫХ

Р.Н. Заркумова

В статье рассматривается понятие интегрированной базы данных как взаимосвязанной совокупности базы данных, базы знаний и базы моделей, используемых для решения задач оценки уровня безопасности информации. Для оценки качественной стороны достоверности элементов или фрагментов интегрированной база данных использован подход калмановской фильтрации.

Ключевые слова: база данных, база знаний, база моделей, достоверность информации, фильтр Калмана

Введение.

Известно [1], что интегрированная база данных (**ИБД**) представляет собой взаимосвязанную совокупность собственно базы данных (**БД**), базы знаний (**БЗ**) и базы моделей (**БМ**). При решении задачи оценки уровня безопасности информации эксперт (или экспертная группа), опираясь на ИБД, должен разработать специфический алгоритм извлечения базы знаний и новых данных, для защиты информации интересующих пользователей и владельца информационных ресурсов.

Нетрудно видеть, что указанный алгоритм в отличие от известного алгоритма вычислительного эксперимента с имитационным моделированием Р. Шеннона [2] имеет признаки, характерные для самоорганизующихся систем, и позволяет эксперту использовать данные, знания, объективные и субъективные модели для решения поставленной проблемы в условиях неопределенности БД, неполноты БЗ и БМ. При этом из всех аспектов, связанных с созданием ИБД, решающее значение приобретает проблема достоверности входящей в нее информации.

Определим достоверность как «уровень разумной уверенности в истинности некоторого высказывания, который удовлетворяет некоторым правилам непротиворечивости и в соответствии с этими правилами формально может быть выражен числом» [3].

Известные подходы к решению проблемы оценки достоверности связаны с применением теоремы Байеса (в широком смысле) [4], теории фильтрации Калмана [5], теории нечетких множеств [6], на основе которых разработаны и применяются в экспертных системах практические способы объединения свидетельств, регистрирующих количественные, качественные и логико-семантические связи между фрагментами базы данных.

Используя идею подхода калмановской фильтрации [5], можно поставить вопрос о качественной стороне достоверности или элементов, или фрагментов, или блоков ИБД в более общем плане, чем это делалось раньше, рассматривая любой ее фрагмент как гипотезу, а фрагменты (элементы), с ко-