УДК 621.395

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕВЫХ И СТАТИСТИЧЕСКИХ АЛГОРИТМОВ ОБНАРУЖЕНИЯ СТЕГОАТАК В ИНТЕРЕСАХ СОЗДАНИЯ ЭФФЕКТИВНОЙ СТЕГОАНАЛИТИЧЕСКОЙ СИСТЕМЫ

М. А. Дрюченко, А. А. Сирота

Воронежский государственный университет

Поступила в редакцию 1.03.2009 г.

Аннотация. Рассматриваются возможности использования нейросетевых алгоритмов обнаружения «разладки» и известных статистических алгоритмов анализа данных в интересах выявления стеганографически-скрытых сообщений в звуковых файлах.

Ключевые слова: нейросетевые алгоритмы, методы стегоанализа, форматы звуковых файлов.

Abstract. The possibility of integration of neural network algorithms for change point detection method with a well-known statistical methods of steganalys is examined. Audio files format are used as stego carriers. All methods are implemented in a program.

Keywords: neural network algorithms, methods of steganalys, audio files format.

ВВЕДЕНИЕ

В настоящее время решение проблемы защиты конфиденциальной информации осуществляется средствами криптографии и стеганографии. Стеганография это разновидность засекречивания информации путем скрытного встраивания защищаемых данных в структуру других, называемых стего-контейнерами (СК) и передаваемых по открытым каналам передачи информации [1]. СК может быть любой файл или поток данных, структура и размер которого позволяют спрятать необходимую информацию. Существует ряд стеганографических алгоритмов, специально разработанных, для работы с аудио-контейнерами и учитывающих как особенности звуковых сигналов, так и особенности восприятия звука человеком. Среди них наиболее распространены алгоритмы скрытия, тем или иным способом модифицирующие наименее значимые биты (НЗБ) звуковых файлов-контейнеров как в пространственной области, так и в области преобразования (LSB — least significant bit methods).

Проблемой выявления скрытой информации занимается стегоанализ (СА) [1]. Одно из перспективных направлений СА заключается в создании алгоритмов, позволяющих анализировать информацию без привязки к конкретным программам скрытия и реализованным в них алгоритмам. Для этих целей могут в частности использоваться искусственные нейронные сети (ИНС) [2,3]. Цель данной работы — разработка комбинированного алгоритма обнаружения стеганографического скрытия данных в звуковых файлах, основанного на использовании аппарата ИНС, статистических методов и алгоритмов обнаружения «разладки» [4], а также сравнение полученного алгоритма с известными статистическими алгоритмами стегоанализа.

1. ЗАДАЧИ СТЕГОАНАЛИЗА

Важной задачей стегоанализа является определение существенных свойств СК, выявление их определенных признаков, которые удовлетворяли бы требованиям репрезентативности и контекстной независимости, и одновременно менялись бы при встраивании в контейнер дополнительной информации. Среди статистических характеристик звуковых СК, которые могут меняться в процессе стеганографического скрытия данных, выделяют следующие [5]: неоднородность последовательностей отсчетов, зависимость между битами в отсчетах, зависимость между отсчетами. Эти свойства в различной степени наблюдаются в большинстве звуковых файлов и могут

© Дрюченко М. А., Сирота А. А., 2009

быть использованы для построения стегоаналитических критериев.

Способность к противодействию стегоанализу определяет стойкость [1] стеганографических систем. Противодействие СА может основываться на формировании математических моделей СК и скрываемого сообщения и поиске на их основе «разрешенных» для модификации областей контейнера. На рис. 1 приведен случай встраивания информации в область изображения, статистические характеристики которой S_2 наиболее близки статистическим характеристикам скрываемого сигнала S_1. Аналогичным образом скрытие может производиться в звуковые и видео-файлы. Кроме этого, могут использоваться алгоритмы, восстанавливающие или сохраняющие характер распределения модифицированных бит и их зависимостей с битами в нетронутых областях СК. В подобных случаях выявление скрытой информации сильно затрудняется.

Для обнаружения изменения свойств СК можно использовать искусственные нейронные сети. Аппарат ИНС позволяет достаточно эффективно восстанавливать характер эталонного сигнала, использованного для обучения сети, и одновременно позволяет отследить даже незначительные изменения различных статистических характеристик и корреляционных зависимостей в СК при появлении в нем аномальных изменений. Далее предлагается использовать данный факт в интересах решения задачи СА.

2. ИСПОЛЬЗОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ ‘РАЗЛАДКИ’ ДЛЯ ВЫЯВЛЕНИЯ СКРЫТЫХ СООБЩЕНИЙ

Под началом области стеганографического скрытия в терминах обнаружения разладки будем понимать скачкообразное изменение

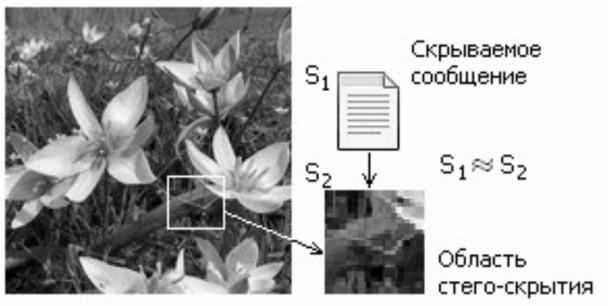

Рис. 1. Схема встраивания информации в выбранную область стего-контейнера, статистические характеристики которой S_2 наиболее близки к статистическим характеристикам сообщения S_1

свойств анализируемой битовой последовательности (СК). Пусть $\{x_k\}$ - отсчеты звукового СК — последовательность независимых случайных величин с плотностью вероятности $P_\theta(x)$, где θ - некий вектор параметров. Можно предположить, что в результате стеганографического встраивания данных, параметр θ изменит свое значение, начиная с некоторого неизвестного момента времени t_0, что в свою очередь приведет к возникновению эффекта «разладки». Иными словами до момента t_0 выполняется $\theta = \theta_0$, а после $\theta = \theta_1$, $\theta_0 \neq \theta_1$. Таким образом, задача поиска разладки, а значит и задача отыскания начала области стеганографического скрытия состоит в определении изменений параметра θ и определении момента времени t_0 [3]. Традиционными показателями эффективности алгоритмов обнаружения разладки обычно являются величина среднего времени запаздывания при обнаружении разладки $\bar{\tau} = M\left(\tau / \tilde{t}_0 \geq t_0\right)$, $\tau = \tilde{t}_0 - t_0$ и уровень ложных тревог $\beta = M\left(\Lambda / \tilde{t}_0 < t_0\right)$, где $\tilde{t}_0$ — оценка момента возникновения разладки; Λ — интенсивность ложных тревог, возникающих до момента наступления разладки [4].

Пусть H_0 — гипотеза, принимаемая в том случае, если сигнал не содержит скрытой информации. В этом случае плотность распределения последовательности анализируемых отсчетов СК $x_1, x_2, \ldots x_N$ обозначим $\omega(x / \theta_0)$. Пусть H_1 — гипотеза, верная в случае скрытного встраивания данных в СК. В этом случае полагаем, что плотность распределения $x_1, x_2, \ldots x_N$ — $\omega(x / \theta_1)$. Пусть также выполняется $H_0 : \theta = \theta_0$, $t < t_0$; $H_1 : \theta = \theta_1$, $t \geq t_0$. Для обнаружения момента разладки, как правило, используются последовательные критерии, фиксирующие изменчивость свойств статистических оценок временных рядов на основе некоторых характеристик. Одним из наиболее эффективных критериев является алгоритм кумулятивных сумм (АКС) [4]. Его основная идея заключается в накоплении суммы значений логарифма отношения правдоподобия для условных плотностей распределения наблюдений в отсутствии и наличии разладки:

$$S_t = (S_{t-1} + \Delta S_t)^+,$$
$$\Delta S_t = \ln\left(\frac{\omega(x_t^{(n)} / \theta_1)}{\omega(x_t^{(n)} / \theta_0)}\right), \qquad (1)$$

где $[x]^+ = \max[0, x]$. Если значения θ_0 и θ_1 до и после изменения свойств процесса известны

неточно, но известно направление скачка в пространстве параметров, может быть использовано асимптотическое разложение Ле Кама [2] для логарифма функции правдоподобия. При этом АКС может быть записан в виде:

$$t_\alpha = \inf\{t : g_t \geq h\},$$
$$g_t = \left[g_{t-1} + \sum_{j=1}^{n} \sum_{q=1}^{r} \frac{\partial \ln \omega(x_j^{(t)} / \theta_0)}{\partial \theta_{0q}} c_q \right]^+, \qquad (2)$$

$g_0 = 0$, $\tilde{t}_0 = t_\alpha - n_\alpha + 1$, h — порог принятия решения о возникновении разладки; t_α — момент подачи сообщения о разладке; n_α — количество шагов, выполненных от момента последнего обнуления кумулятивной суммы g_t до момента принятия решения [6]. Как только значение суммы $g_t > h$, то подается сигнал о разладке. Порог h разумнее всего определять растущим со временем t в виде

$$h(t) = C + \ln(t) + 2 \cdot \ln(\ln(t)), \quad t = 1, 2, \ldots N \qquad (3)$$

Константа C в (3) отвечает за вероятность ложной тревоги. Если уровень $h(t) = C$ выбрать постоянным, то при удаленном моменте возникновения разладки вероятность ложной тревоги будет очень высока.

3. НЕЙРОСЕТЕВОЙ АЛГОРИТМ ВЫЯВЛЕНИЯ СТЕНОГРАФИЧЕСКОГО СКРЫТИЯ ДАННЫХ

Схема работы нейросетевого алгоритма выявления стеганографического скрытия включает реализацию двух этапов: обучение нейронной сети (НС) на «чистых» звуковых образцах; тестирование НС и поиск разладок. С помощью НС в стационарном режиме формируется авторегрессионная модель (АМ) исследуемого сигнала. Встраивание в сигнал дополнительной информации (например, методом модификации НЗБ отсчетов звукового сигнала) приведет к возникновению эффекта разладки по отношению к АМ, полученной в стационарном режиме (когда не происходит стего-скрытия). Для регистрации разладки используется специальный алгоритм обработки данных на выходе НС, фиксирующий структуру и параметры исходной модели.

Как при обучении, так и при тестировании осуществляется предварительная обработка файлов-СК. С целью уменьшения нестационарности из исходного сигнала $S(t)$ рис. 2 а) исключаются единичные скачки и участки, содержащие серии отсчетов с одинаковыми значениями. Далее сигнал подвергается высокочастотной дискретной фильтрации и полученные значения нормируются от -1 до 1. В результате получаем новый сигнал $\tilde{S}(t)$ рис. 2 б).

Обозначим $\tilde{S} = (\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_N)^T$ — вектор, содержащий последовательность отсчетов обработанного звукового сигнала. Формируется матрица «входных воздействий» $Y = \{y_1, y_2, \ldots, y_{N-\delta}\}$, где $y_i = (\tilde{s}_i, \tilde{s}_{i+1}, \ldots, \tilde{s}_{i+\delta-1})$, $i = 1, 2, \ldots, N - \delta$; δ - длина вектора y_i. Значения векторов y_i далее подаются на входы ИНС. Величины, получаемые на выходе сети, можно представить в виде:

$$\tilde{y}_t = \sum_{i=1}^{\delta} W_i y_{t-i} + A + \eta_t, \qquad (4)$$

где $t = \delta, \delta + 1, \ldots, N$. W_i — матрицы, составленные из весов НС, обеспечивающие прохождение входных воздействий y_{t-i} на выход; A — вектор смещений нейронов сети; η_t — вектор ошибки предсказания значений $\tilde{y}_t$ на выходе НС, имеющий математическое ожидание, равное нулю, и неизвестную матрицу ковариации R_η. При построении АМ модели сигнала рассматривалось несколько вариантов формирования компонент матриц входных воздействий $Y = \{y_1, y_2, \ldots, y_{N-\delta}\}$ [3]. На рис. 3 а) представлен простейший случай линейного предсказания, когда осуществляется прогнозирование всего одного отсчета звукового сигнала. На рис. 3 б) изображен случай векторного предсказания отсчетов сигнала, когда на вход НС подается вектор $y_i = (\tilde{s}_i, \tilde{s}_{i+1}, \ldots, \tilde{s}_{i+\delta-1})$, а на выходе формируется вектор $\tilde{y}_i = (\tilde{s}_{i+\delta}, \tilde{s}_{i+\delta+1}, \ldots \tilde{s}_{i+\delta+l})$, $l < \delta$ — длина предсказываемого сетью вектора; $i < k < i + \delta$. На рис. 3 в) также представлен вариант «внутреннего» векторного предсказания, при котором компоненты вектора Y имеют

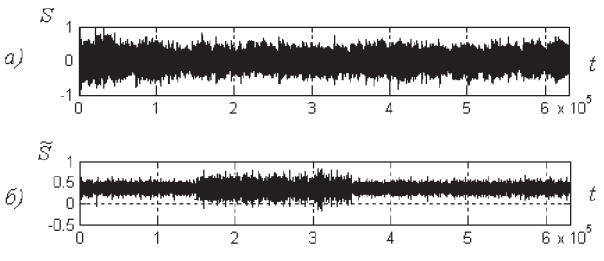

Рис. 2. а) Исходный звуковой сигнал; б) Отфильтрованный звуковой сигнал. По оси X — дискретное время, по Y — значения отсчетов сигналов, нормированные от -1 до 1

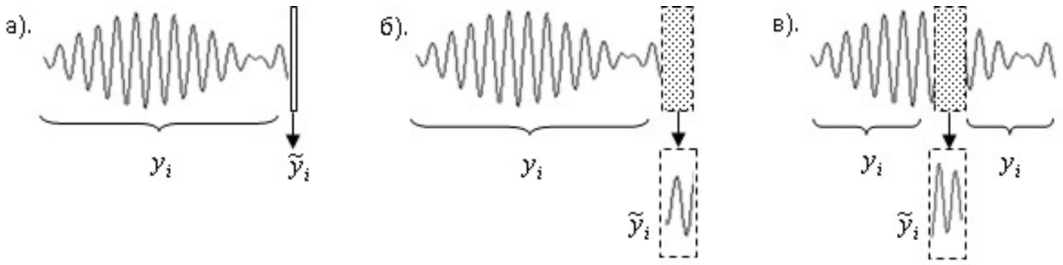

Рис. 3. Варианты формирования компонент y_i матриц "входных воздействий" и векторов $\tilde{y}_i$, прогнозоруемых нейронной сетью: а) случай предсказания одного отсчета звукового файла; б) и в) случаи векторного предсказания

вид $y_i = (\tilde{s}_i, \tilde{s}_{i+1}, ..., \tilde{s}_{i+k-1}, \tilde{s}_{i+k}, \tilde{s}_{i+k+l}, \tilde{s}_{i+k+l+1}, ... \tilde{s}_{i+\delta-1})$, $i = 1, 2, ..., N - \delta$. Наилучшие результаты в смысле точности восстановления сигнала были получены при использовании векторного предсказания внутри вектора отсчетов (рис. 3 в).

Параметры W_i, $i = \overline{1, \delta}$ и A из (4) определяются в ходе обучения нейронной НС. Оценка матрицы ковариации вектора η_t авторегрессионной модели и математическое ожидание СКО проводится в ходе тестирования сети после обучения на тех же данных [6]:

$$R_\eta = \frac{1}{N}\sum_{t=1}^{N}(y_t - \tilde{y}_t)(y_t - \tilde{y}_t)^T, \qquad (5)$$
$$M_z = spR_\eta,$$

где y_t — вектор из обучающей (тестирующей) выборки данных; $\tilde{y}_t$ — предсказываемый сетью вектор. В качестве компонентов вектора параметров θ АМ модели, используемого для обнаружения разладки, рассматривается СКО выхода НС.

Были также рассмотрены несколько моделей данных, подаваемых на входы ИНС, которые представлены на рис. 4. На рис. 4 а) представлен случай, когда компоненты матрицы входных воздействий Y формируются только из отсчетов анализируемого сигнала. На рис. 4 б) приводится схема формирования компонент матрицы Y значениями, полученными после применения различных статистических стегоаналитических критериев. В этом случае анализируется уже не сигнал, а разладка ищется по отношению к последовательности результатов статистических алгоритмов СА, применяемых к СК. На рис. 4 в) представлен случай, формирования вектора входных воздействий на основе как отсчетов анализируемого сигнала, так и результатов применения к СК статистических стего-атак в виде $Y = \{y_1, y_2, ..., y_{N-\delta}, M_1, M_2, ... M_k\}$, где M_i, $i = 1, 2, ... k$ значения, полученные в результате применения к СК статистических стегоатак. Величины M_i здесь выступают в роли сопутствующих или управляющих параметров (УП) НС.

4. СТАТИСТИЧЕСКИЕ АЛГОРИТМЫ СТЕГОАНАЛИЗА

В рамках рассматриваемого подхода в работе были реализованы следующие статистические стего-атаки: атака по критерию частот переходов значений в потоке НЗБ отсчетов сигнала, атака по критерию длин битовых серий, атака по критерию хи-квадрат. Данные стегоатаки применялись как по отдельности, так и в рамках нейросетевой модели в качестве УП или в качестве самостоятельных данных, используемых для обучения и тестирования НС. Кратко рассмотрим перечисленные статистические критерии.

Метод оценки числа переходов значений в потоке НЗБ анализируемого контейнера. Между младшими битами имеются существенные корреляционные связи, которые могут нарушаться при встраивании данных. Зависимость между битами в соответствующих байтовых разрядах отсчетов имеет марковский характер [5]. При этом параметры зависимости определяются номером разряда. Число переходов в потоке НЗБ из 0 в 0, из 0 в 1, из 1 в 0, из 1 в 1 различно для файла-контейнера и файла, содержащего встроенную информацию. При стегоскрытии данных с некоторой вероятностью P_ε меняется вид закона распределения НЗБ. Как правило, распределение младших бит приобретает случайный характер, соответственно, частоты переходов в потоке НЗБ отсчетов звукового файла будут примерно одинаковы в тех областях файла, где содержится скрытая инфор-

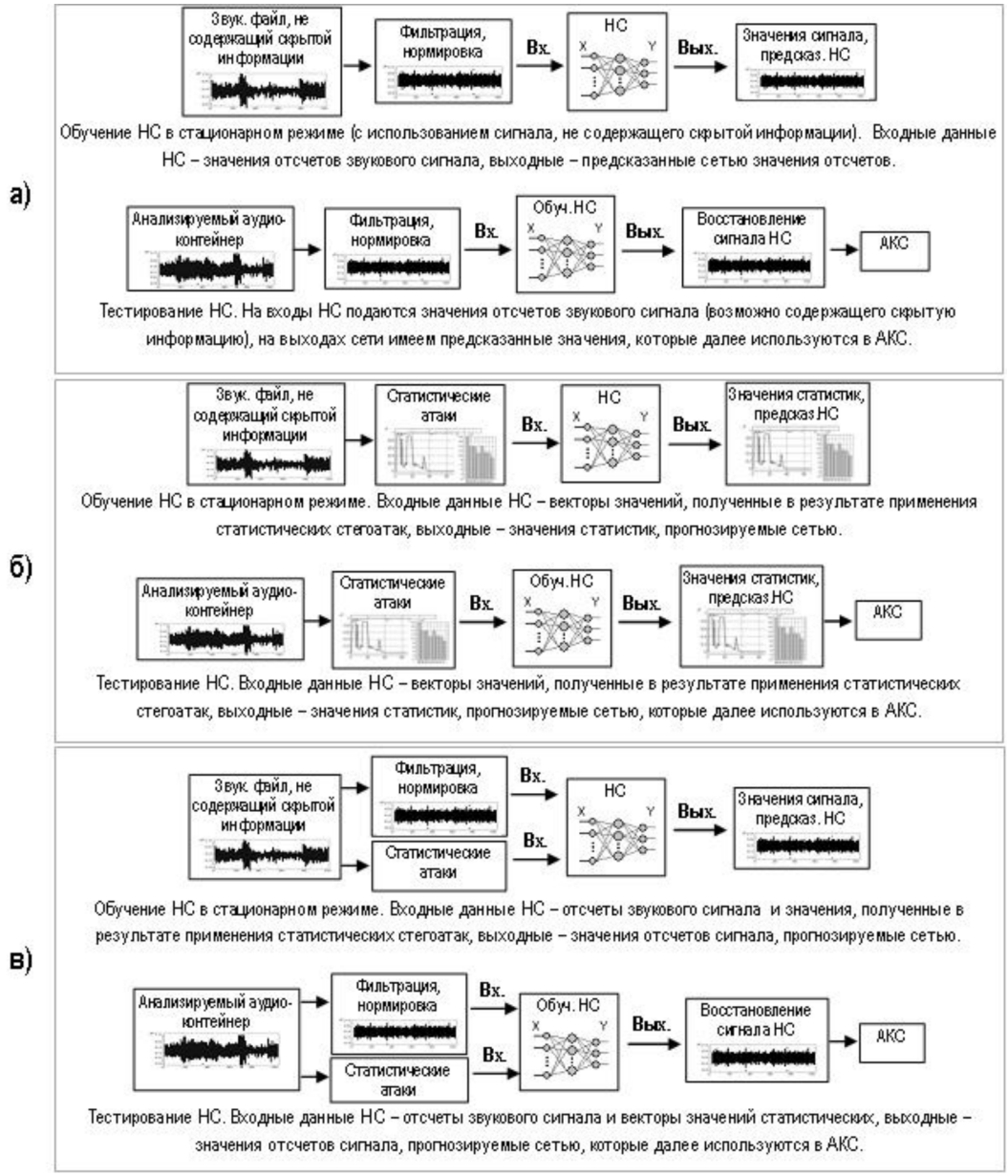

Рис. 4. Схемы обучения и тестирования нейронных сетей для различных типов входных данных

мация рис. 5 б), чего нельзя сказать о незаполненных областях контейнера рис. 5 а).

Статистический критерий для оценки частот переходов битовых значений можно сформулировать следующим образом: анализируемый файл разбивается на K блоков одинаковой длины, выбирается некоторое пороговое значение h_M. Далее вычисляются значения статистик

$$\mathrm{M}_j = \left[\frac{(\mu_{00} - \mu_{01})^2}{2} + \frac{(\mu_{11} - \mu_{10})^2}{2} \right]_j, \qquad (6)$$

$$j = 1, 2, \ldots K$$

μ_{ij} — количество переходов в потоке НЗБ из i в j $(i, j = 0,1)$. В случае если $M_j < h_M$ считается, что в j-м блоке содержится скрытая информация.

На рис. 6 представлен результат применения описанного метода.

На практике данный критерий способен выявлять стеганографическое скрытие при последовательной модификации младших бит, когда наблюдается резкий скачек статистики M_j, в случае же псевдослучайного выбора отсчетов сигнала для встраивания в них стегоданных, данный статистический критерий не

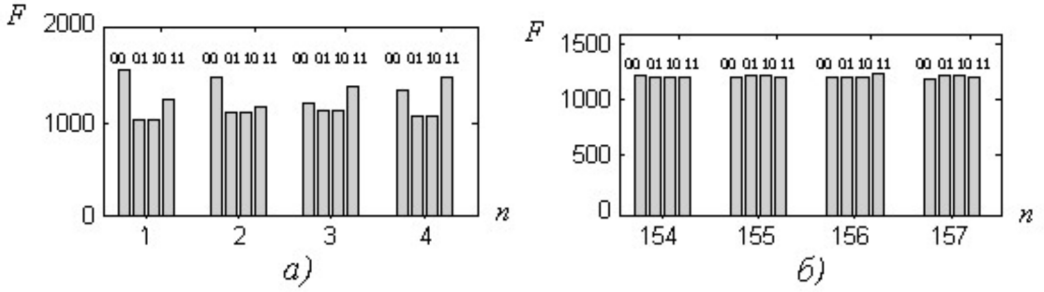

Рис. 5. Гистограммы частот переходов битовых значений в потоке НЗБ отсчетов звукового файла: по оси X — номера блоков, на которые разбивается аудио-файл, по Y — частоты битовых переходов. а) Область файла без стего-скрытия; б) Участок файла, содержащий скрытые данные

способен выявить факт информационного скрытия. Как показали результаты экспериментов данный критерий можно использовать для формирования векторов входных воздействий НС или в качестве УП НС. При отсутствии стеганографического скрытия значения M_j будут колебаться относительно некоторого среднего значения и это не приведет к возрастанию числа ложных тревог, а резкое изменение статистик M_j отразится на выходных данных НС, что будет зафиксировано АКС.

Еще один критерий, позволяющий выявлять факт стеганографического скрытия, основан на *подсчете статистики длин битовых серий* в аудио-контейнере. Под α-серией длины n понимается последовательность, состоящая из одинаковых бит вида $\alpha\alpha\ldots\alpha$ где $\alpha \in \{0,1\}$, $n = 1,2,\ldots N$ [5]. Количество α-серий большой длины является более устойчивой характеристикой, чем число битовых переходов в младших разрядах. На рис. 7 а) приведены графики частот появления 0-х α-серий различной длины (для 1-х аналогично) в зависимости от их расположения в файле-контейнере. По оси абсцисс отложены номера блоков, на которые разбивается звуковой файл, по оси ординат частоты α-серий для каждого блока. Видно, что в областях файла, содержащих скрытые данные увеличиваются частоты для α-серий единичной длины и одновременно происходит уменьшение количества α-серий длины больше 1. На рис. 7 б) представлены кривые распределения длин серий 0 бит для незаполненного (серая кривая) и заполненного контейнера (черная кривая).

На практике данный критерий устойчиво показывает статистически значимые различия в случае слабо выраженной Марковской зависимости в НЗБ контейнера. В то же время, он не позволяет фиксировать факт стего-скрытия при незначительных объемах встраиваемых данных и их «рассеиванию» по всему звуковому файлу.

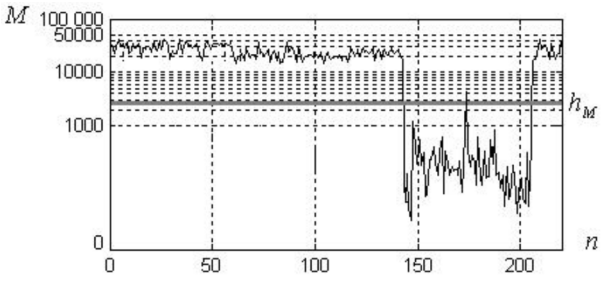

Рис. 6. Статистический критерий оценки частот битовых переходов НЗБ звукового файла: по оси X — номера блоков, на которые разбивается файл, по Y — значение статистики, h_M — пороговое значение

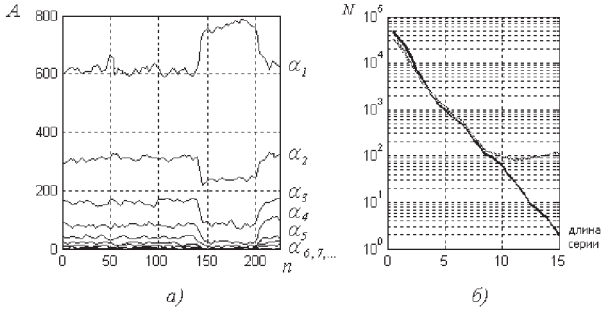

Рис. 7. а) Графики частот появления 0-х α-серий различной длины (для 1-х аналогично) в зависимости от их расположения в файле-контейнере: по оси X — номера блоков, на которые разбивается звуковой файл, по оси Y — частоты α-серий для каждого блока; б) кривые распределения длин серий 0 бит для незаполненного (серая кривая) и заполненного контейнера (черная кривая)

Соответствие реально наблюдаемой статистики ожидаемой обычно проверяется при помощи критерия хи-квадрат [1]. Проверка может осуществляться на уровне монобитов, дибитов и т.д. Как показали результаты экспериментов, изменение статистики хи-квадрат является достаточно устойчивым демаскирующим признаком способным выявлять факт информационного скрытия даже при 10% заполнении контейнера. Значения статистики хи-квадрат также могут быть использованы в качестве УП ИНС. Кроме этого в набор УП включались начальные моменты первого порядка и центральные моменты второго порядка, вычисляемые на отрезках анализируемого сигнала.

5. ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ

При проведении исследований в качестве СК рассматривались звуковые файлы формата wav. Данный формат аудио-файлов наиболее часто используется в программах стеганографического скрытия. В форматы, предусматривающие кодирование (MPEG) скрытие информации чаще всего производится в специальные секции, т.е. в поля, предназначенные для комментариев, или просто производится запись данных в конец файла. Были проанализированы результаты работы широко известных стеганографических утилит S-Tools, Stegomagic, Steganos for Windows, Steganos Security Suite, Fox Secret.

Практическая реализация рассмотренных вариантов алгоритмов СА производилась в среде Matlab. Она включает несколько шагов. Сначала производится обучение НС в стационарном режиме (верхние схемы рис. 4а)-в)) при использовании реализаций СП без скрытой информации. В процессе тестирования сети производится настройка параметров системы на вероятность ложного обнаружения разладки, определяется порог принятия решений $h(t)$. Далее на входы обученной НС подаются векторы входных воздействий, сформированные согласно одной из схем рис 4. На выходе сети имеем предсказанные значения $\tilde{y}_t$. Параллельно вычисляются СКО предсказания НС очередного вектора y_t

$$Z_t^{(1)} = z_t = \frac{1}{r}\sum_{i=1}^{r}\left(y_t^{(i)} - \tilde{y}_t^{(i)}\right)^2, \qquad (7)$$

где $y_t^{(i)}$ — вектор значений, подаваемый на входы НС, а $\tilde{y}_t^{(i)}$ — вектор, полученный на выходе сети. Решающее правило, настроенное на определение скачка среднего значения СКО выхода НС, имеет следующий вид [3]:

$$\left.\frac{\partial \ln \omega(z_t/\theta)}{\partial \ln \theta}\right|_{\theta=\theta_0} = \frac{z_t - m_z \cdot \xi}{\sigma_z},$$
$$g_t = \left[g_{t-1} + \frac{z_t - m_z \cdot \xi}{\sigma_z}\right]^+, \qquad (8)$$

$t_\alpha = \inf\{t : g_t \ge h\}$, $g_0 = 0$, $\tilde{t}_0 = t_\alpha - n_\alpha + 1$, $0 < \xi < 2$ - коэффициент «чувствительности» к ложным тревогам, m_z и σ_z (математическое ожидание и дисперсия, оцениваются в ходе тестирования НС).

Если предположить, что в результате скрытия в отсчетах звукового файла изменится вид закона распределения в соответствующих битовых плоскостях, то должны измениться величины m_z и σ_z, т.е. возникнет смещение $m_z \to m_z'$ и $\sigma_z \to \sigma_z'$. В этом случае можно использовать АКС в форме (2) и записать решающее правило в виде [7]:

$$g_t = \left[g_{t-1} + c_1\frac{(z_t - m_z^{(0)}\cdot\zeta)}{(\sigma_z^{(0)})^2} + c_2\frac{(z_t - m_z^{(0)}\cdot\zeta)^2 - (\sigma_z^{(0)})^2}{(\sigma_z^{(0)})^3}\right]^+, \qquad (9)$$

$$c_1 = \frac{(m_z' - m_z)}{\sqrt{(m_z' - m_z)^2 + (\sigma_z' - \sigma_z)^2}},$$

$$c_2 = \frac{(\sigma_z' - \sigma_z)}{\sqrt{(m_z' - m_z)^2 + (\sigma_z' - \sigma_z)^2}},$$

где $g_0 = 1$, ζ — параметр чувствительности алгоритма к ложным тревогам, $\tilde{t}_0 = t_a - n_a + 1$, $\theta_0 = (0.5(m_z + m_z'),\ 0.5(\sigma_z + \sigma_z'))^T$; c_1, c_2 — компоненты вектора разладки для параметров m_z и σ_z соответственно.

Как показали результаты экспериментов, применение решающего правила в форме (9) позволяет более точно (с меньшим запаздыванием) фиксировать момент обнаружения разладки, однако число ложных тревог оказалось выше, чем при использовании АКС в форме (8). На рис. 8 а) приведена временная диаграмма СКО восстановления сигнала НС, на рис. 8 б) и 8 в) в логарифмическом масштабе приведены графики кумулятивных сумм, фиксирующие моменты возникновения разладки в форме (8) и (9).

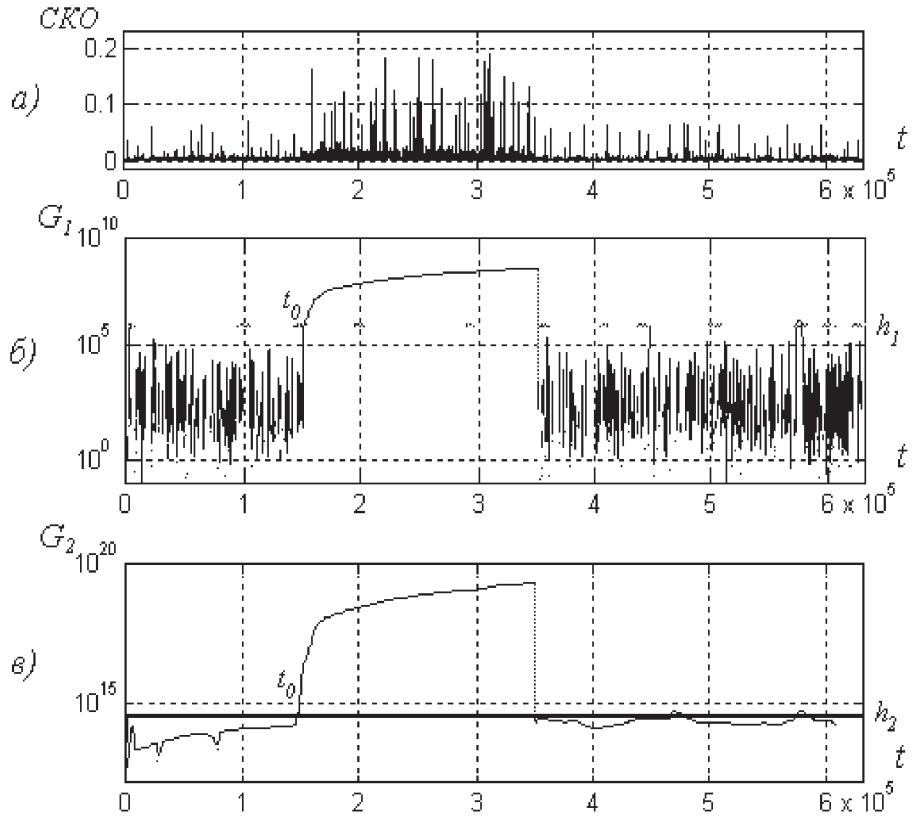

Рис. 8. а) Временная диаграмма СКО восстановления звукового сигнала нейронной сетью; б), в) Графики кумулятивных сумм, фиксирующие момент возникновения разладки

Описанные алгоритмы обнаружения разладки показали возможность своего применения для выявления стеганографического скрытия. В ряде случаев они оказались эффективнее известных статистических методов. Тестирование проводилось на специально сформированном наборе из 108 звуковых файлов, в которые производилось скрытие информации с использованием перечисленных выше стеганографических утилит. Результаты тестирования для звуковых образцов имеющих 50% и более заполнение скрываемой информацией приведены в таблице.

На результаты работы алгоритма в значительной степени влияют отношение длины скрываемого сообщения и длины СК, алгоритм по которому происходит встраивания информации, число байтовых разрядов, подвергшихся модификации, а также характеристики самого СК такие как отношение сигнал-шум и наличие в контейнере областей существенной нестационарности. Запаздывание обнаружения разладок оценивалось исходя из $\tilde{\tau} = t_{\text{скр}} - t_0 + 1$, где $t_{\text{скр}}$ известный момент начала области стего-скрытия, t_0 момент обнаружения разладки. В случае от-

Таблица 1

Результаты применения нейросетевого алгоритма выявления стеганографического скрытия

Программы стеганографического скрытия	S-Tools	Stego magic	Steganos for Windows	Fox Secret	Steganos Security Suite
Процент верного обнаружения стегоскрытия	82,4%	92%	86%	90%	77%

сутствия ошибок 1-го и 2-го рода значение запаздывания составляло $280 < \tilde{\tau} < 1900$.

Была показана принципиальная возможность использования результатов статистических критериев в качестве данных для формирования АМ модели и в качестве управляющих параметров НС. В частности при анализе белого шума, содержащего стего-данные в НЗБ, алгоритм обнаружения разладки в форме (8), реализованный по схеме а) на рис. 4 не способен определить начало области скрытия, а в случае использования дополнительных управляющих параметров (рис. 4в)) это становится возможным. Подобный подход позволяет свести к минимуму ошибки классификации и одновременно увеличить эффективность нейросетевого алгоритма обнаружения разладок. В тоже время, следует отметить, что методика выбора управляющих параметров для ИНС требует дополнительных исследований.

СПИСОК ЛИТЕРАТУРЫ

1. *Грибунин В.Г.* Цифровая стеганография / В.Г. Грибунин. — СПб. : СОЛОН-Пресс, 2002. — 280 с.

2. *Bergman C., Davidson J.* An Artificial Neural Network for Wavelet Steganalysis, October 1, 2004—September 31, 2006. — (www.mfrc.ameslab.gov/R-D_Reports/Artificial_Neural_Network_for_ Steganalysis_Final.pdf)

3. *Дрюченко М.А., Сирота А.А.* Нейросетевой алгоритм выявления стеганографически скрытых сообщений методом обнаружения «разладки» / М. А. Дрюченко, А. А. Сирота // Радиотехника. — 2008. — № 11. — С. 24—28.

4. *Никифоров И.В.* Последовательное обнаружение изменения свойств временных рядов / И. В. Никифоров. — М. : Наука, 1984. — 199 с.

5. *Барсуков В.С.* Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации / В. С. Барсуков, А. П. Романцов // "Специальная Техника". — 2000. — № 1.

6. *Сирота А.А.* Обнаружение микроколебаний объектов на основе нейросетевых алгоритмов обработки данных голографического интерферометра / А. А. Сирота, В. Г. Попов, В. А. Шульгин // Изв. вузов. Радиоэлектроника. — 2007. — 50, № 3-4, [ч. 2]. — С. 31—41.

7. *Сирота А.А., Никольский В.И.* Использование методов обнаружения «разладки» для тестирования аномальных измерений в процессе испытаний радиопеленгационных систем / А. А. Сирота, В. И. Никольский // Радиотехника. — 2007. — № 5. — С. 18—22.

Дрюченко Михаил Анатольевич — аспирант кафедры информационных систем Воронежского государственного университета. Email: aldram@box.vsi.ru

Сирота Александр Анатольевич — д.т.н., проф., каф информационных систем, Воронежский государственный университет. Тел. (4732)208-724. E-mail: sir@cs.vsu.ru

Dryuchenko M.A. — Postgraduate student, Voronezh State University, Computer Science Faculty, Information Systems department. Email: aldram@box.vsi.ru

Sirota Aleksandr A. — Doctor of Technic Sciences, Professor, the dept. of the Information Systems, Voronezh State University. Tel. (4732)208-909. E-mail: sir@cs.vsu.ru