ДЕТЕКТИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В АУДИО- И ГРАФИЧЕСКИХ ФАЙЛАХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Сазановец И. А.
Кафедра системного программирования и компьютерной безопасности, Гродненский государственный университет имени Янки Купалы
Гродно, Республика Беларусь
E-mail: sazanovec_ia_13@mf.grsu.by

В работе рассматриваются методы сокрытия информации и детекирования скрытых данных в цифровых изображениях и аудиофайлах. В частности, рассматривается применение методов машинного обучения, таких, как нейронные сети, для детекирования фактов стеганографии.

Введение. Стеганография

В сфере информационной безопасности хорошо известен термин «стеганография». Методы этой дисциплины позволяют незаметно передавать одни данные на фоне других. Наибольший интерес представляют методы именно цифровой стеганографии, в которой и данные, которые скрываются, и данные, на фоне которых скрываются, представлены цифровыми файлами.

I. Методы сокрытия информации в аудио- и графических файлах

Существуют различные методы цифровой стеганографии. Их можно разделить на две группы:

- методы, использующие особенности информационные систем;
- методы, использующие статистические свойства файла-контейнера (файла, который служит фоном и готорый виден и/или слышен субъекту).

В качестве примеров первой группы могут служить методы сокрытия в альтернативных потоках файловой системы NTFS и склеивание JPEG изображения с RAR архивом. Для детектирования фактов сокрытия такими методами можно применять детерминированные алгоритмы.

Во втором случае у файла-контейнера изменяется небольшая часть информации так, чтобы, с одной стороны, в этих изменениях и была закодирована информация, а с другой стороны, чтобы эти изменения были незаметны. Для этих целей в качестве контейнера, часто применяют изображения и аудиофайлы, причем информация записывается именно в область данных, а не в метаинформацию файла.

В случае с изображеними методы стеганографии можно разделить на два класса[1]:

- методы, использующие пространственную плоскость;
- методы, использующие частотную плоскость.

К первым относятся метод наименьшего значащего бита (где информация записывается в младшие биты байтов RGB-представления пикселов) и его разновидности. Во втором случае вначале применяется преобразование изображения в частотную область, потом внедреятся информация, затем применяется обратное преобразование для получения файла изображения.

С аудиопотоком дела обстоят схожим образом. Здесь также методы можно разделить на две группы:

- методы, использующие временную плоскость;
- методы, использующие частотную плоскость.

К первым, как и в случае с изображениями, относятся метод наименьшего значащего бита и его разновидности. Во втором случае сначала происходит преобразование временной плоскости в частотную, потом запись скрываемой информации и затем обратное преобразование, чтобы получить звуковой поток.

В качестве преобразования в частотную плоскость и обратно часто используют прямое и обратное дискретные преобразования Фурье.

Для методов в пространственной и временной плоскостях характерны большая емкость, но слабая устойчивость к пережатию или изменению формата. Для методов в частотной области, наоборот – меньшая емкость, но большая устойчивость.

Акцент во всех этих методах делается на то, чтобы человек не заметил и не услышал ничего подозрительного. Например, одним из способов стеганографии в аудиофайлах является способ записи интересующей информации в верхние частоты (около 20-22 кГц). Люди редко слышат столь высокие частоты. А в изображениях метод наименьшего значащего бита работает так, что его изменение, пусть даже и во всех трех каналах (красном, зеленом, синем), вызовет слишком слабое для человеческого глаза изменение цвета.

Все это делает детектирование такой стеганографии субъективными методами крайне неэффективным. Поэтому для этих целей следует применять компьютерные технологии.

II. Методы детектирования стеганографической информации

Методы детектирования информации меняются в зависимости от ситуации [2]:

- если доступен только файл-контейнер;
- если дотупен файл-контейнер (который, предположительно, со скрытой информацией) и оригинальный файл – то применятся сравнение этих файлов;
- если доступен файл контейнера и сообщение (не эффективно, если сообщение перед скрытием было зашифровано);
- если известен файл контейнера и алгоритм/инструмент скрытия.

Особенно трудно справиться с задачей детектирования, если доступен только файл контейнера. Написать детерминированный алгоритм для такого случая крайне затруднительно. Однако для решения этой задачи могут использоваться методы машинного обучения и, в частности, искусственные нейронные сети.

III. Методы машинного обучения

Искусственная нейронная сеть – это математическая модель работы биологической нейронной сети. Ее главной задачей является обработка данных.

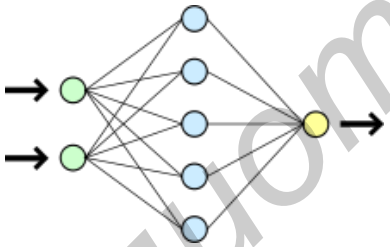

Рис. 1 – Пример нейронной сети

Сама нейронная сеть (как биологическая, так и ее математическая модель) состоит из большого числа нейронов, каждый из которых сам по себе также обрабатывает информацию (см. рис. 1). Она, по определению, является распределенной системой вычислений, притом устойчивой к ошибкам. Это значит, что даже если небольшой процент нейронов и приведет к неправильным результатам, но большая часть сделает верное решение, то и вся нейронная сеть тоже будет склоняться к правильному результату. Эта особенность делает применение искусственных нейронных сетей удобными для решения задач с нечеткой логикой.

Нейроны соеденены специальными связями, и эти связи имеют различнуй вес (значимость, или коэффициент, на который умножается входной сигнал). И эти веса не постоянные, а в процессе обучения изменяются. Как именно – зависит от алгоритма обучения.

Каждый стеганографический алгоритм вносит свои искажения в контейнер. Это означает, что имея примеры стеганоконтейнеров и чистых контейнеров, можно обучить искусственную нейронную сеть, и в дальнейшем она будет обрабатывать новые, еще не известные ей файлы, применяя к ним знания, полученные ранее. Это дает два преимущества: гибкость и универсальность. Гибкость заключается в способности нейронной сети к обучению. А универсальность в том, что можно обучить нейронную сеть детектировать применения различных алгоритмов. Так, в случае с изображениями можно применить следующий алгоритм[3]. Вначале из пекселей цифрового изображения получают пространство признаков. В качестве признаков можно использовать статистические моменты в частотной области гистограмм вейвлет-коэффициентов, в частности, вычисленных до глубины разложения 3. В качестве нейронной сети можно использовать сеть радикально-базисных функций (RBF-сети). Метод состоит в анализе пространства признаков имеющейся базы изображений. Обучение сети – смешанное (вначале – без учителя, потом минимизируют среднеквадратичную ошибку с учителем, затем для уточнения параметров сети используют метод градиентного спуска). В результате после анализа пространство признаков разделяется на две группы: стего и контейнеры.

Выводы

Существуют различные способы спрятать информацию в цифровых изображениях и аудиофайлах. А вот детектировать факты такого сокрытия значительно труднее. Для человека искажения в файлах будут незаметными. Детерминированные алгоритмы едва ли можно спроектировать. Однако для решения этой задачи можно использовать методы машинного обучения. Так, обучив нейронную сеть, можно с достаточной долей вероятности обнаруживать стеганоконтейнеры.

Список литературы

1. A Survey of Image Steganography Techniques /Mehdi Hussain, Mureed Hussain. // International Journal of Advanced Science and Technology. – 2013. – Vol. 54. – P. 116–117.
2. Steganalysis: Detecting hidden information with computer forensic analysis / Pierre Richer. SANS Institute, 2003. – P. 4–5.
3. Абденов, А. Ж. Использование нейронных сетей в слепых методах обнаружения встроенной стеганографической информации в цифровых изображениях / А. Ж. Абденов, Л. С. Леонов. // Ползуновский вестник. – 2010. – Vol. 2. – P. 221–224.