УДК 004.056.53

Исследование возможности акустического криптоанализа компьютерных клавиатур

Д.Н. Дяговченко[1], *Ф.А. Афанасьев*[1], *Г.П. Камышанов*[1]

[1]Московский физико-технический институт (государственный университет)

Идея акустического криптоанализа не нова и применялась еще для дешифровки сообщений, набираемых на печатных машинках. Состоит она в том, что любая система издает шумы, которые могут изменяться по некоторым законам в зависимости от состояния этой системы. В современном мире данный тип криптоанализа был применен даже для получения ключей, используемых при работе алгоритма RSA [1]. В этом случае шумы испускали электронные компоненты микросхем [2].

В данном исследовании изучается звук клавиш, издаваемый при их нажатии. Гипотеза нашего исследования состоит в том, что все клавиши клавиатуры издают разные звуки, причем это различие поддается анализу.

Анализ звука состоит из двух этапов. Первый - частотный анализ отдельных частей аудиозаписи нажатия. Второй – обработка спектра клавиши с помощью нейронной сети. На вход сети подаются векторы фиксированной длины, отдельные компоненты которых представляют амплитуды соответствующих частот спектра, на выходе сеть выдает число, соответствующее той или иной букве.

Для успешной работы нейронной сети ее необходимо обучить. Обучение представляет собой отправку набора спектров нажатий клавиш на вход нейронной сети, которым соответствуют определенные числа, характеризующие различные буквы. По этим данным сеть отбрасывает частоты, слабо влияющие на конечный результат (внешние шумы, одинаковые звуки при нажатиях) и выделяет частоты, по которым можно определить, какая из клавиш была нажата. От того, насколько хорошо удастся классифицировать входные данные, зависит качество работы сети после обучения. Соответственно, чем больше статистика, тем лучше сработает распознавание.

Для контроля качества обучения нейронной сети выделяется тестовая группа спектров, на которой нейронная сеть не проходит обучение.

На рис. 1 показан результат обучения нейронной сети для трех букв. Суммарная статистика – 300 нажатий. График «Training» показывает то, как удалось классифицировать данные, полученные для обучения. График «Test» отображает три группы точек, которые не участвовали в обучении (каждая группа включает 17 точек).

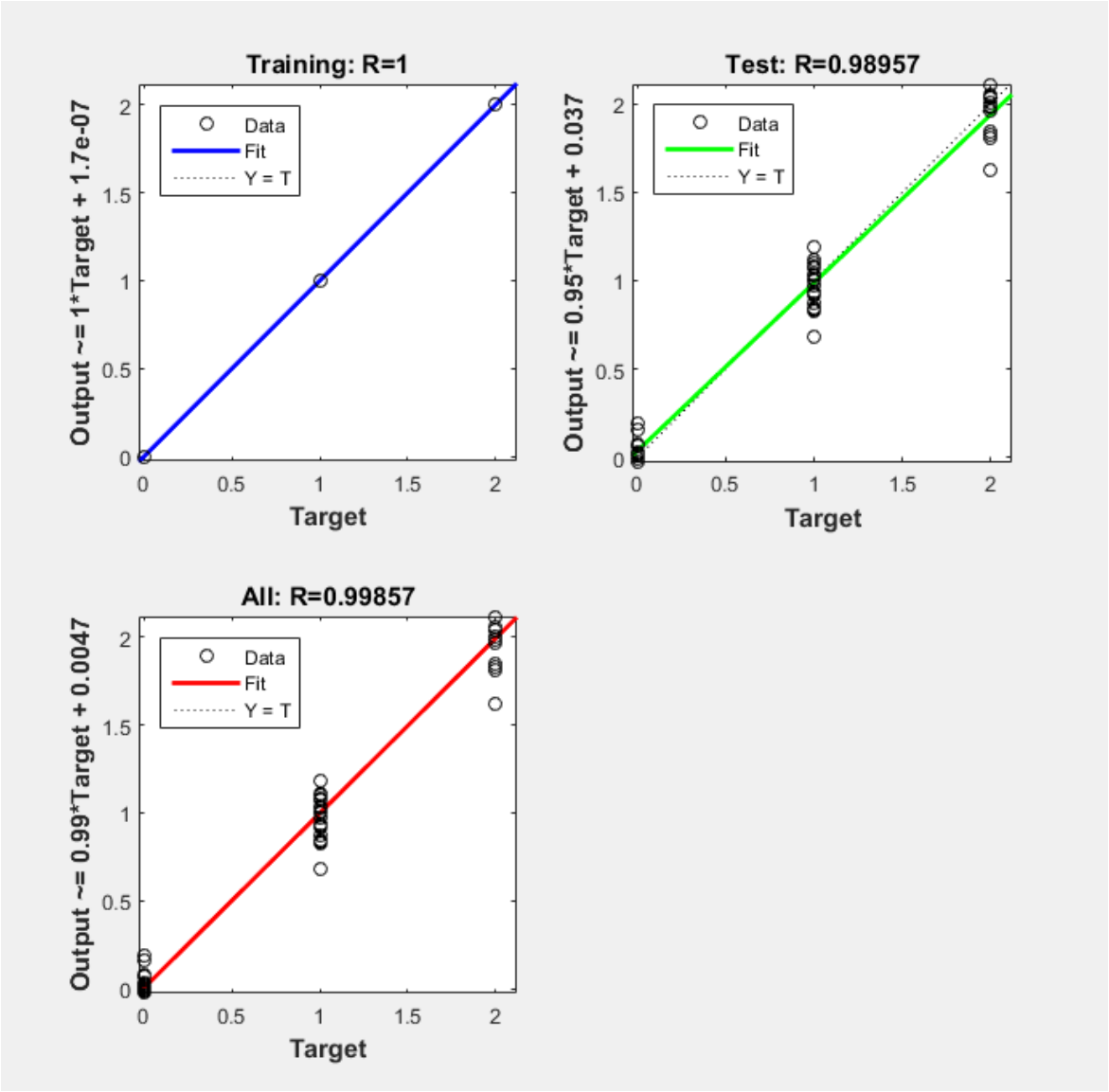

Рис. 1.

Таким образом отработан алгоритм, позволяющий успешно распознавать нажатия клавиш на клавиатуре.

Литература

1. *Daniel Genkin, Adi Shamir, Eran Tromer* RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis - December 18, 2013
2. *Mark Laps, Roy Grace, Bill Sloka* Capacitors for Reduced Microphonics and Sound Emission – Electronic Components, Assembles& Materials Association(ECA), Arlington, VA CARTS 2007 Symposium Proceedings, Albuquerque, NM, March 2007