

УДК 004.056:061.68

В.М. Федоров, Д.П. Рублев

ОБРАБОТКА ВИБРОАКУСТИЧЕСКИХ ШУМОВ, ВОЗНИКАЮЩИХ ПРИ РАБОТЕ ПОЛЬЗОВАТЕЛЯ С КЛАВИАТУРОЙ*

Рассматривается структура системы записи виброакустических сигналов от клавиатуры для целей идентификации пользователя. Приведены характеристики сигналов, полученных при помощи сенда, рассмотрено введение дополнительного датчика для получения двухканального сигнала, упрощающего проведение шумоочистки и выделения признаков, идентифицирующих как нажатую клавишу, так и пользователя, рассмотрены возможности локализации нажатой клавиши и формирования векторов признаков на основе межканальной корреляции частотной области и коэффициентов преобразования Фурье, кепстральных коэффициентов и коэффициентов линейного предсказания.

Виброакустический сигнал; идентификация пользователя; локализация клавиш; межканальная корреляция; коэффициенты линейного предсказания.

V.M. Fedorov, D.P. Rublev

PROCESSING OF VIBROACOUSTIC NOISE ORIGINATED FROM USER WORK WITH KEYBOARD

In this paper the structure of vibroacoustics signal recording system intended for user identification by keyboard typing noise is reviewed, parameters of signals recorded by system are presented, sensor addition and dual-channel configuration for noise cancellation and feature selection improving both for key and user identification, possibilities for pressed key localization and feature vector forming on a basis of interchannel correlation, Fourier, cepstrum and linear predictive coefficients are considered.

Vibroacoustic signal; user identification; key localizing; interchannel correlation; linear prediction coefficients.

Одной из актуальных задач является аутентификации субъекта с высокой надежностью, точностью, без применения дорогостоящего оборудования и незаметно для испытуемого. Существующие распространенные варианты лишь частично удовлетворяют этим требованиям. Широко распространенная аутентификация (пароли, ключи) не отличается высокой надежностью, системы биометрической аутентификации (распознавание отпечатков пальца, ладони, радужной оболочки, голоса) требуют спецсредств, существует также возможность подмены образца. Аутентификация методом клавиатурного почерка выгодно отличается не требовательностью к аппаратным средствам (используется стандартная клавиатура), возможностью перманентного удаленного использования и прозрачностью для испытуемого. В связи с этим, для контроля доступа к ПЭВМ наибольшее распространение получили клавиатурные методы аутентификации пользователя. Главным недостатком данного метода является, недостаточна точность идентификации, связанная с ограниченным числом доступных анализируемых признаков. Это связано с ограниченным числом параметров, используемых при аутентификации субъекта системой принятия решений. Целью работы является аутентификация пользователя по акустическим шумам, возникающим при работе пользователя, которые возникают как при наборе данных на клавиатуре, так и при использовании манипулятора «мышь». При использовании признаков при использовании клавиатуры возможны два режима аутентификации, по произвольному тексту и при наборе парольной фразы. В связи с этим, первоначальной задачей при разработке системы

* Работа выполнена при поддержке гранта РФФИ №12-07-00674-а.

являлась задача распознавания нажимаемых клавиш клавиатуры при работе. На рис. 1 показана блок-схема системы записи виброакустических шумов. В качестве датчиков использовались плоскостные пьезоакустические датчики, снятый сигнал усиливался малошумящим операционным усилителем 548УН1.

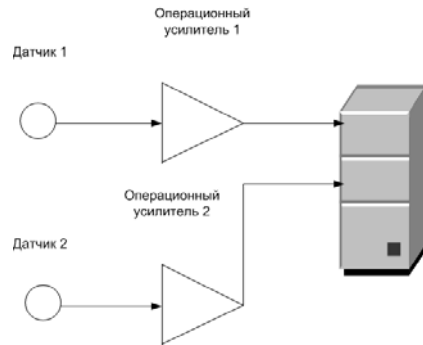


Рис. 1. Структура системы записи виброакустических сигналов

Виброакустические датчики были установлены на выдвижную полку компьютерного стола по обеим сторонам от клавиатуры симметрично относительно её центра. Расстояние между датчиками составляло 65 см. Клавиатура Genius была установлена горизонтально на 4 штатные (2 эластичные и 2 жёсткие) опоры. Оцифровка сигнала производилась средствами внешней звуковой карты Creative при разрядности отсчёта 16 бит и частоте дискретизации 44100 Гц. Имеется ряд экспериментальных объяснений природы отличия шумов при нажатии различных клавиш, причины такого различия описаны в работе [1, 2]. При проведении экспериментов при помощи стенда были получены два сигнала – виброакустический сигнал от нажатия одной клавиши с цифрой "1" и верхнего цифрового ряда клавиш клавиатуры от "1" до "0". Осциллограммы и гистограммы фрагмента стереосигнала, полученного при помощи системы записи при нажатии клавиши "1" приведены на рис. 2, фрагмента сигнала с записью первого нажатия – на рис. 3.

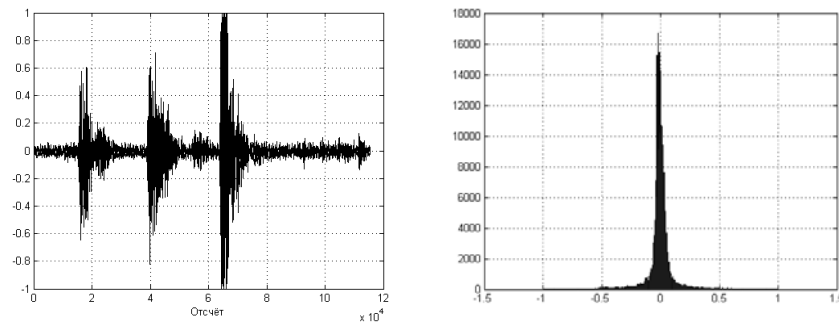


Рис. 2. Осциллограмма и гистограмма фрагмента сигнала, полученного при нажатии на клавишу "1"

Значения смещения m составили $-0,0138$ и $-0,0017$, дисперсии – $0,0167$ и $0,0158$ для каждого из каналов соответственно. Из осциллограммы фрагмента приведенной на рис. 3 ясно, что в начальный момент наблюдается также задержка сигнала.

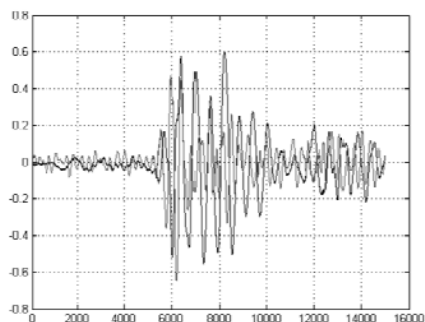
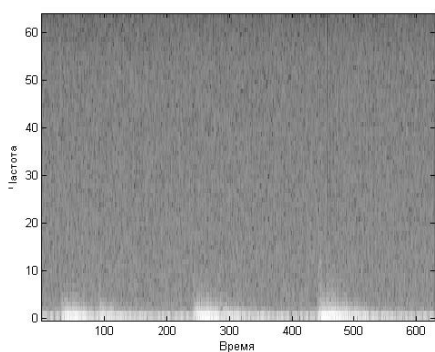
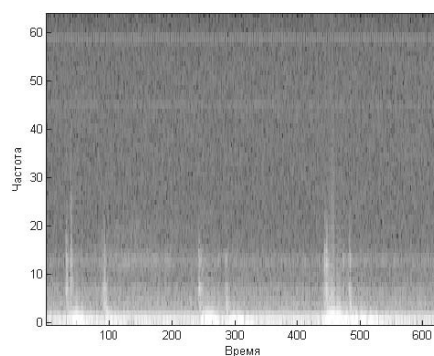


Рис. 3. Фрагмент сигнала

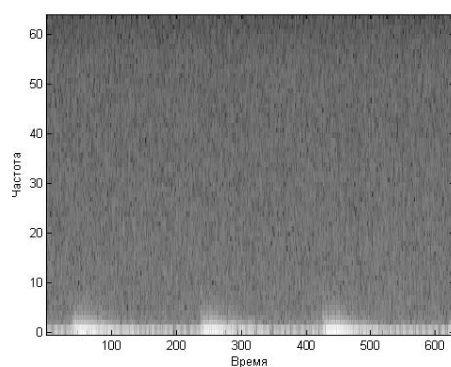
На рис. 4 приведены спектрограммы обоих каналов двух фрагментов сигналов, соответствующих последовательностям нажатых клавиш “1-1-1” и “2-2-2”. По данным спектрограмм возможно определить моменты нажатия клавиш (минимальное значения отношения “сигнал/шум” для интегральной мощности составило 46 дБ), однако их идентификация непосредственно по спектрограммам затруднена ввиду отличий в динамике воздействия во время каждого отдельного нажатия на клавишу.



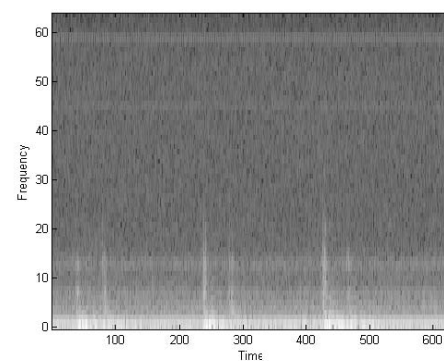
Спектрограмма при наборе “1-1-1”, канал L



Спектрограмма при наборе “1-1-1”, канал R



Спектрограмма при наборе “2-2-2”, канал L



Спектрограмма при наборе “2-2-2”, канал R

Рис. 4. Спектрограммы обоих каналов двух фрагментов сигналов, соответствующих последовательностям нажатых клавиш “1-1-1” и “2-2-2”

Для возможности идентификации местоположения клавиши была исследована корреляция каналов записи и её производные. На рис. 5 приведены графики коэффициентов межканальной взаимной корреляции во временной области фрагмента сигнала, соответствующего нажатию клавиши “1”, полученные в скользящих окнах при длинах 4096, 16384 и 32768 соответственно.

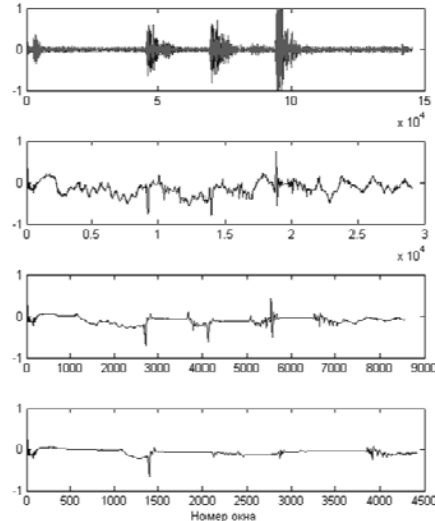


Рис. 5. Коэффициенты корреляции исходного сигнала в скользящем окне

Из графиков видно, что на графиках наблюдаются пики в начальные моменты информативных сигналов нажатия клавиш, вместе с тем межканальная корреляция во временной области также не позволяет установить величину временной задержки и локализовать клавишу. Для оценки зависимости коэффициента корреляции от задержки по времени для того же сигнала была получена развёртка межканальной корреляции [3] во временной области при длине окна 1024 отсчёта в соответствии с выражениями:

$$\hat{R}_{xy}(m) = \begin{cases} \sum_{n=0}^{N-m-1} x_{n+m} y_n^* & m \geq 0 \\ \hat{R}_{yx}^*(-m) & m < 0 \end{cases}$$

где m – смещение; x_n – отсчёты окна канала L; y_n – отсчёты окна канала R; N – длина окна; приведённая на рис. 6.

Вблизи нулевого смещения (элемента с индексом 1024) наблюдается минимум значения взаимной корреляции, смещающийся с течением времени. Для сравнения была получена аналогичная развёртка для акустического сигнала с цифрового стереомикрофона, приведённая на рис. 7.

Колебания максимума корреляции относительно нулевого смещения выражены слабо, наблюдается выраженная фрагментация сигнала с выделением временных отрезков, соответствующих упругим колебаниям и отрезков, соответствующих механическому перемещению клавиш. Однако, как показали предыдущие работы авторов, использование акустического канала на практике приводит к повышенному уровню помех, в том числе, совпадающих по характеристикам с информативным сигналом.

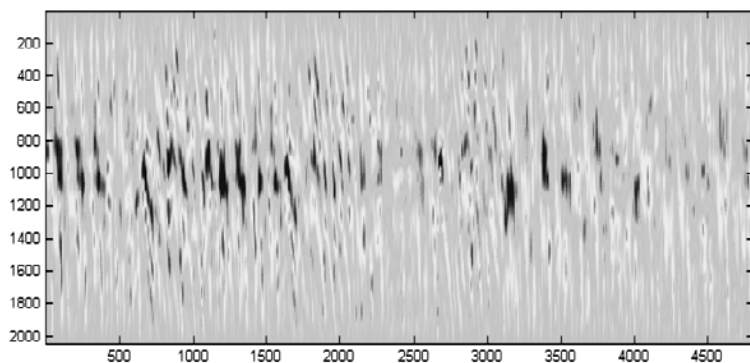


Рис. 6. Развёртка межканальной взаимной корреляции во временной области

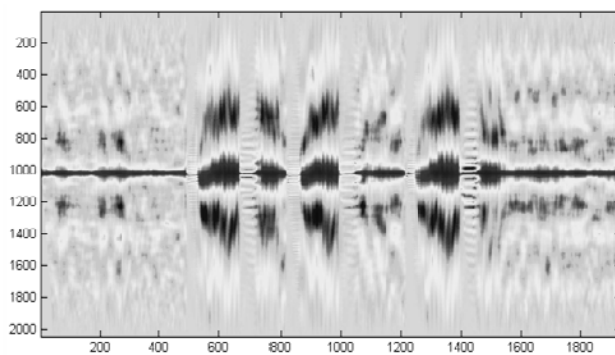


Рис. 7. Развёртка межканальной взаимной корреляции акустического стереосигнала

Для оценки задержек, присутствующих в виброакустическом сигнале и, соответственно, возможности позиционирования клавиш на их основе целесообразно реализовать операцию взаимной корреляции в частотной области. Примеры взаимной корреляции спектрограмм двух каналов и график индексов максимальных элементов приведены на рис. 8.

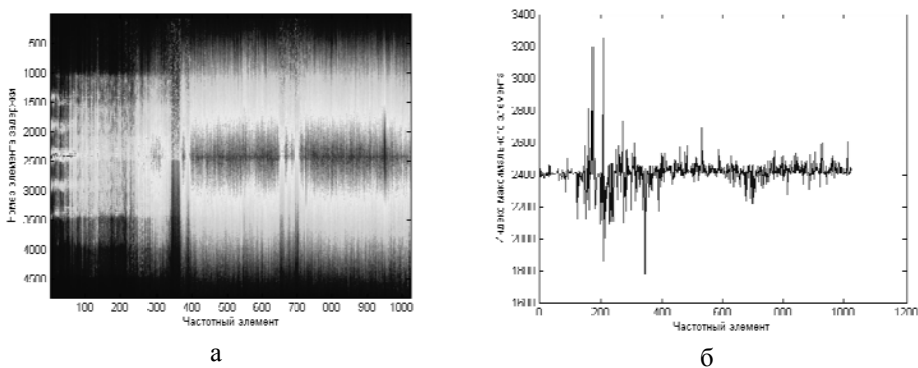


Рис. 8. Взаимная корреляция спектрограмм двух каналов (а) и график индексов максимальных элементов (б)

Идентификацию клавиш по записанным сигналам предполагается производить за два этапа. На первом определяется местоположение (окрестность) клавиши на основе корреляции в частотной области, на втором планируется производить непосредственно идентификацию по выделенным из акустического сигнала признакам клавиши.

Обзор литературных источников [1, 2] показывает, что основная доля выполненных работ использует в качестве признаков или коэффициенты разложения сигнала в ряд Фурье или кепстр.

Кроме того, виброакустический сигнал с соседних клавиш имеет схожий спектр сигнала. На рис. 9 показан спектр сигнала с клавиш с цифрами «один» и «два». Использование коэффициентов Фурье для распознавания данных сигналов не позволит идентифицировать клавиши. Авторами предложено использование дополнительного виброакустического датчика укрепленного на компьютерном столе на расстоянии до 1 метра от основного. Такой подход позволит более точно определить местонахождение клавиши, от которой был зафиксирован виброакустический сигнал. Предварительные экспериментальные результаты показали перспективность данного подхода.

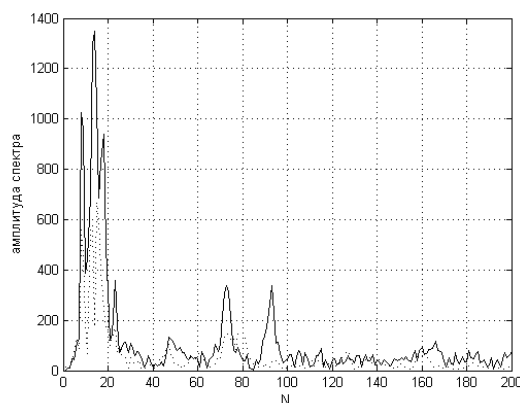


Рис. 9. Амплитуда спектра виброакустического сигнала при нажатии клавиши: сплошная линия – от клавиши с цифрой «единица», пунктирная – от клавиши с цифрой «три»

Основной проблемой является выявление устойчивых признаков для идентификации клавиш по виброакустическому сигналу. Как уже отмечалось выше, в качестве признаков для распознавания нажатой клавиши используются коэффициенты разложения в ряд Фурье или кепстр в классическом понимании этого понятия. В работах авторов [4] использовался кепстр, вычисленный по коэффициентам линейного предсказания для идентификации диктора по голосу. В отличие от методов Фурье-преобразования, базирующихся на спектральном анализе, линейное предсказание речи относится к классу методов параметрического моделирования, которые пытаются моделировать спектр как авторегрессионный процесс. Существует три основных способа расчета коэффициентов линейного предсказания: ковариационные методы, базирующиеся на ковариационной матрице (называемые чистым методом наименьших квадратов), автокорреляционные методы и периодические (или гармонические) методы. Более подробно различия в этих подходах можно найти в [5]. Применение автокорреляционного метода в задачах распознавания, в частности речи, обусловлено присущими ему вычислительной эффективностью и стабильностью. Наиболее эффективно коэффициенты линейного предсказания

можно вычислить при использовании рекурсии Левинсона-Дарбина [3]. На рис. 10 показана дисперсия коэффициентов кепстра для виброакустического сигнала возникающего при нажатии клавиши на клавиатуре.

Как видно из рисунка, согласно дисперсионному критерию, можно ограничиться первыми 30 коэффициентами кепстра. Для распознавания нажатой клавиши предполагается использовать нейронные сети и гауссовские смешанные модели.

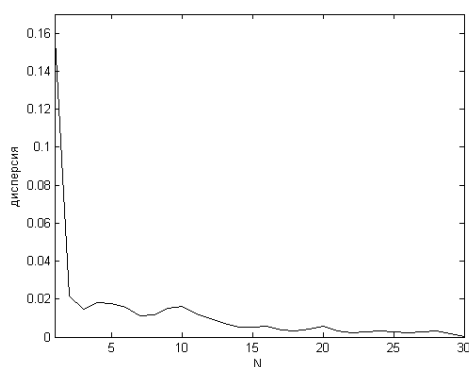


Рис. 10. Дисперсия коэффициента кепстра для виброакустического сигнала при нажатии и отпускания клавиши клавиатуры

Предварительные результаты показали более устойчивые результаты распознавания клавиш при использовании кепстра, вычисленного по коэффициентам линейного предсказания.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Dmitri Asonov, Rakesh Agrawal.* Keyboard Acoustic Emanations // IEEE Symposium on Security and Privacy. – 2004. – P. 3-11.
2. *Yigael Berger, Avishai Wool, Arie Yeredor.* Dictionary Attacks Using Keyboard Acoustic Emanations, Alexandria, Virginia, USA CCS'06, 2006, 3. – P. 245-254.
3. *Рабинер Л.Р., Шафер Р.В.* Цифровая обработка речевых сигналов: Пер. с англ. / Под ред. М.В. Назарова, Ю.Н. Прохорова. – М.: Радио и связь, 1981. – 495 с.
4. *Макаревич О.Б., Бабенко Л.К., Федоров В.М., Юрков П.Ю.* Текстонезависимая аутентификация/идентификация по голосу в системах управления доступом // X Всероссийская научно-практическая конференция “Проблемы информационной безопасности в системе высшей школы”. – М.: МИФИ, 2003. – С. 28-29.
5. *Маркел Дж., Грэй А.Х.* Линейное предсказание речи: Пер с англ. / Под ред. Ю.Н. Прохорова, В.С. Звездина. – М.: Связь, 1980. – 308 с.

Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Федоров Владимир Михайлович – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: vladmih@rambler.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Рублёв Дмитрий Павлович – e-mail: rublev-d@yandex.ru; кафедра безопасности информационных технологий; доцент.

Fedorov Vladimir Mikhailovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: vladmih@rambler.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

Rublev Dmitry Pavlovich – e-mail: rublev-d@yandex.ru; the department of security in data processing technologies; associate professor.