Шарабыров Илья Викторович – e-mail: ilyashar@mail.ru; тел: 89196059521; кафедра вычислительной техники и защиты информации; аспирант.

Vasilyev Vladimir Ivanovich – Federal State Educational Institution of Higher Professional Education "Ufa State Aviation Technical University"; e-mail: vasilyev@ugatu.ac.ru; 12, K. Marx street, Ufa, 450000, Russia; phone: +79173501139; the department of computer engineering and information protection; head of the department; professor.

Sharabyrov Ilya Viktorovich – e-mail: ilyashar@mail.ru; phone: +79196059521; the department of computer engineering and information protection; postgraduate student.

УДК 004.056:061.68

В.М. Федоров, Д.П. Рублев

ИДЕНТИФИКАЦИЯ НАБИРАЕМОГО НА КЛАВИАТУРЕ ТЕКСТА ПО ВИБРОАКУСТИЧЕСКИМ ШУМАМ*

Рассмотрена проблема идентификация нажимаемых клавиш по виброакустическому сигналу, возникающему при работе пользователя с клавиатурой. Показаны возможность съёма идентифицирующих набранный текст данных по физическому (виброакустическому) каналу и преимущества данного метода, приведены модификации рабочего места оператора, описание стенда и программных средств. Рассмотрены особенности виброакустических сигналов, получаемых при работе пользователя с клавиатурой, произведён выбор устойчивых признаков, характеризующих нажатые клавиши из коэффициентов Фурье преобразования, кепстральных коэффициентов, коэффициентов линейного предсказания. Приведена схема синхронизации журнала клавиатурного регистратора и полученного виброакустического сигнала для получения точных сведений о локализации моментов нажатий/отпусканий клавиш и корректного формирования векторов признаков. Показана возможность идентификации клавиш по виброакустическим шумам, возникающим при наборе на клавиатуре, приведены зависимости оценок ошибок нейросетей от количества нейронов в скрытых слоях, выбора активационных функций и количества входных классов.

Виброакустический сигнал; дискретное Фурье преобразование; кепстральные коэффициенты; нейронные сети; коэффициенты линейного предсказания; идентификация.

V.M. Fedorov, D.P. Rublev

IDENTIFICATION OF TEXT TYPED ON KEYBOARD BY VIBROACOUSTICS NOISES

In this paper identification problem for pressed keys by vibroacoustic signal originated from user typing is reviewed. Capabilities of data collection for typed test restoration on vibroacoustic channel and advantages of this technique are shown. Operator's workplace modifications, stand description and software are considered. Features of vibroacoustic signals obtained from user's interaction with keyboard are reviewed, stable features which allow pressed key identification were selected from Fourier transform, cepstral and linear prediction coefficients. Sync scheme for keylogger's log file and vibroacoustics signal for precise localization of keypressing moments with key identification and feature vectors creation is reviewed. Keys identification by vibroacoustics typing noises is showed, dependencies of neural network errors on hidden layers neurons quantity, activation functions and output classes are considered.

Vibroacoustic signal; discrete Fourier transform; cepstral coefficients; neural networks; linear prediction coefficients; identification.

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

Для контроля доступа помимо традиционных средств идентификации широко используются также и биометрические, основанные на контроле факторов, находящихся под влиянием особенностей, установившихся в ходе индивидуального развития биологического субъекта доступа. В качестве подобных средств, не требующих внедрения дополнительного оборудования и организации явных процедур контроля доступа, могут быть использованы средства скрытого контроля взаимодействия пользователя со штатными средствами устройствами ввода информации, в частности клавиатурой, как наиболее распространённым устройством ввода алфавитно-цифровой информации. Эффективность системы идентификации определяется качеством распознавания, зависящим от степени уникальности параметров пользователя. Съём биометрических данных при работе с клавиатурой возможен двумя способами – контролем событий "нажатие/отпускание клавиши" на уровне интерфейса клавиатуры либо системного драйвера (клавиатурный почерк) и контролем взаимодействия с клавиатурой как с физическим объектом [1]. Клавиатурный почерк относится к динамическим (поведенческим) биометрическим характеристикам, описывающим подсознательные действия, привычные для пользователя. Он характеризует динамику ввода парольной фразы либо произвольного текста при помощи клавиатуры. Стандартные драйвер и интерфейс клавиатуры наряду с передачей идентификаторов нажатых клавишах позволяют измерить следующие временные характеристики: время удержания клавиш нажатыми и временных интервалов между нажатиями клавиш.

Клавиатурный почерк могут характеризовать и другие параметры, описанные в [2, 3]: общее время набора парольной фразы, частота возникновения ошибок при наборе, факт использования дополнительных клавиш (использование числовой клавиатуры), особенности ввода заглавных букв (использование клавиши Shift или Caps Lock) и т. д. Выделяют два варианта идентификации пользователя по клавиатурному почерку:

- по набору произвольно выбранного текста;
- по набору специально выбранной ключевой фразы.

Оба способа включают режимы обучения и идентификации. В режиме обучения производится считывание параметров работы с клавиатурой, расчёт и сохранение эталонных характеристик пользователя. В режиме идентификации происходит статистическая обработка вновь получаемых результатов наблюдений за текущими параметрами работы пользователя с клавиатурой, исключение сильных отклонений и сравнение с ранее сохранёнными эталонными характеристиками. Для идентификации пользователя как правило используют классификаторы на основе гауссовских смешанных моделей, дисперсионного и регрессионного анализа либо нейронных сетей. Последний позволяет производить дообучение системы идентификации построенной на его основе и с наибольшей точностью идентифицировать пользователя по клавиатурному почерку.

Привлекательность использования клавиатурного почерка основана на отсутствии дорогостоящих устройств ввода биометрических параметров для идентификации и возможность контроля за процессом использования данной ПЭВМ легальным пользователем. Тем не менее, данный метод не позволяет достичь низкого уровня ошибок первого и второго рода и, как правило, применяется в составе многофакторных схем аутентификации.

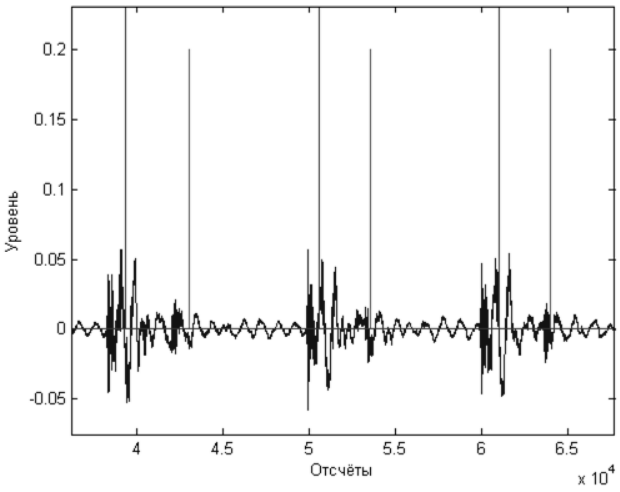
Предлагаемый метод, основанный на регистрации виброакустических шумов при наборе данных с клавиатуры позволяет повысить точность идентификации пользователей при незначительном увеличении дополнительного оборудования: виброакустические датчики, устанавливаются непосредственно на рабочем столе пользователя, данные с которых вводятся в звуковую карту для дальнейшего ана-

лиза. Использование двух датчиков позволяет повысить надежность системы и повысить точность идентификации пользователя. Также данный подход даёт возможность производить идентификацию пользователя вне зависимости от целостности программно-аппаратного окружения, нарушение которой может иметь место при подключении аппаратных эмуляторов клавиатурного почерка либо внедрении модифицированных драйверов клавиатуры в составе программных эмуляторов.

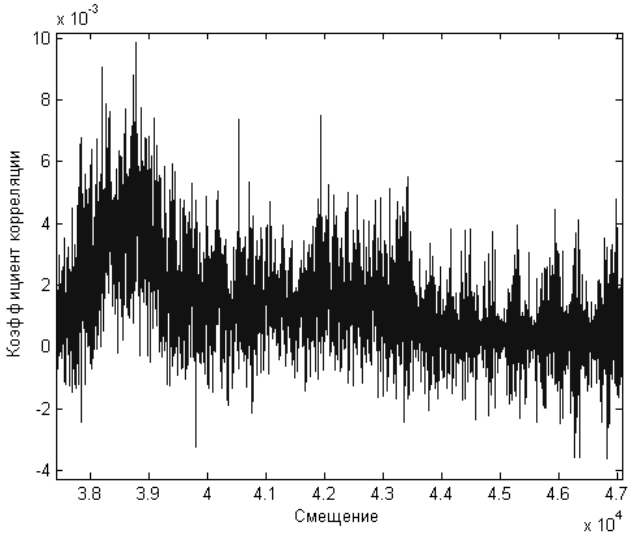
Для целей идентификации пользователя по набираемому тексту необходимо решение задачи идентификации нажимаемых клавиш по виброакустическому либо акустическому сигналам. Основная сложность при обучении системы распознавания объясняется неоднозначностью выделения из виброакустического сигнала моментов нажатия/отпускания клавиш.

В соответствии с данными [4–6] скорость ввода для оператора ПЭВМ составляет до 300 символов в минуту при средней длительности удержания клавиши порядка 70–150 мс. Этого времени достаточно, чтобы разделить сигналы, возникающие при нажатии и отпускании клавиши. Для идентификации пользователя в предыдущих работах из записанного виброакустического сигнала произвольного текста набранного каждым пользователем удалялись паузы между нажатиями/отпускания клавиш клавиатуры [7, 8]. Предварительно виброакустические сигналы фильтровались по методике, описанной в [5, 9]. Однако для исследования методов идентификации нажимаемых клавиш необходима достоверная информация о точном коде клавиши и времени её нажатия с точностью до миллисекунд.

Данная проблема была решена применением на этапе обучения системы программного кейлоггера для получения точного значения временных меток, соответствующих моментам нажатия/отпускания клавиш. Для регистрации нажатий на клавиши использовался регистратор нажатий клавиш (“кейлоггер”) “Basic Key Logger” распространяемый по лицензии GPL v.2. В результате его работы формировался файл журнала, содержащий ASCII-строки с указанием полного кода нажатых/отпущенных клавиш, временных меток нажатия/отпускания клавиш, и признаков нажатия/отпускания. Получаемые временны*е* метки имеют выраженный сдвиг относительно времени начала аудиозаписи по причине влияния на скорость загрузки программ и переходы в рабочие режимы окружения операционной системы, изменяющегося при каждом запуске процесса записи, а также особенностей динамики работы пользователя с клавиатурой. Как было установлено в результате экспериментов, величина сдвига менялась от записи к записи и для тестового стенда находилась в пределах 200-10000 отсчётов (0,05-0,2 с) при частоте дискретизации 48 кГц. Информативный виброакустический сигнал, записанный на стенде, как предшествует моменту нажатия клавиши, так и наблюдается после него. В то же время, для корректного формирования векторов признаков необходима точность выделения фрагментов сигнала порядка 0,01 с. Точная величина смещения для выравнивания моментов нажатия/отпускания находилась следующим образом. При помощи преобразования Гильберта вычислялись огибающая и мгновенная фаза виброакустического сигнала, которые затем использовались для формирования значений взаимной корреляции с единичными импульсами, соответствующих моментам нажатий/отпусканий клавиш, полученным из журнала кейлоггера. В результате экспериментов было установлено, что более точную локализацию импульсов даёт использование мгновенной фазы сигнала. Примеры сопоставления моментов нажатия/отпускания клавиш с осциллограммой сигнала и фрагмент полученной взаимной корреляции приведены на рис. 1,а,б.



а



б

Рис. 1. Моменты нажатия/отпускания клавиш, совмещённые с осциллограммой сигнала (а) и значения коэффициента корреляции (б)

В качестве векторов признаков аналогично работе [1] формировались выборки виброакустических шумов возникающих при нажатии/отпускании клавиш. В качестве векторов признаков использовались коэффициенты преобразования Фурье, начиная со второго [10], вычисленные на участках виброакустического сигнала, выделенных при помощи сопоставления журнала событий кейлоггера с виброакустическим сигналом. Длина фрагмента, на котором вычислялся вектор признаков, выбиралась исходя из отсутствия временны*х* перекрытий с последующими нажатиями и отпусканиями клавиш. В качестве признаков были рассмотрены следующие: кепстральные коэффициенты, вычисленные по коэффициентам линейного предсказания, коэффициенты линейного предсказания, коэффициенты преобразования Фурье [7, 9]. Основным требованиям, предъявляемым к векторам, используемым для идентификации клавиш являлась устойчивость. Размерность

вектора признака определялась эмпирически для всех типов рассматриваемых векторов. Проведенные исследования показали, что для идентификации клавиш по виброакустическим сигналам, возникающим при наборе произвольного текста наиболее устойчивыми признаками являются коэффициенты преобразования Фурье. Формирования векторов признаков производилось в окнах виброакустического сигнала максимальной длиной 5000 отсчётов. В качестве нейронной сети использовался двухслойный персептрон с двумя скрытыми слоями и количеством выходов соответственно количеству распознаваемых клавиш. На рис. 2 показаны ответы нейронной сети на обучающей и тестовой выборках. Векторы признаков были сформированы на фрагментах виброакустического сигнала, соответствующих нажатиям и отпусканиям 2-х клавиш.

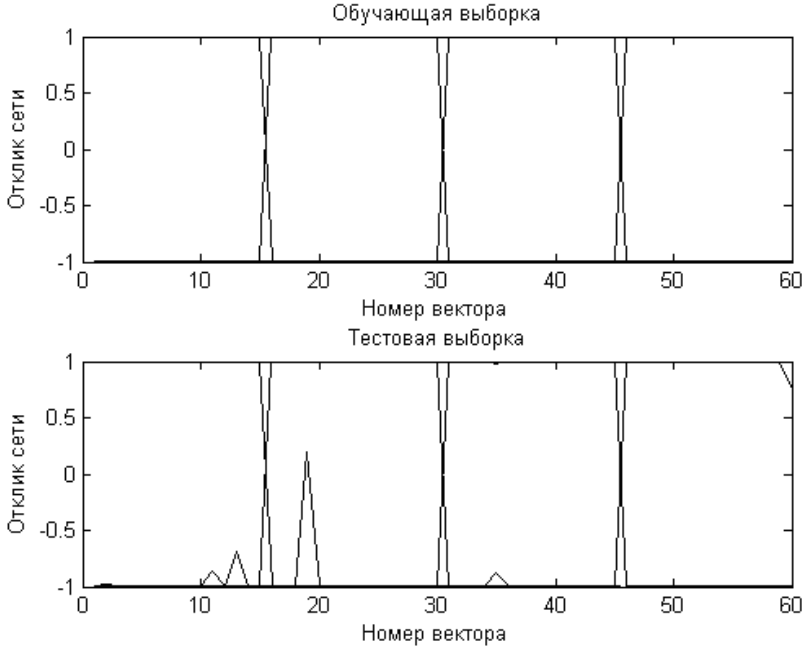


Рис. 2. Выходы нейронной сети при классификации 4-х событий

Получена зависимость ошибки от изменения количества коэффициентов в пределах [4]. Результаты для нейросетей с тангенциальными и сигмоидальными активационными функциями скрытых слоёв приведены в табл. 1. Значение в каждой ячейке таблицы является усреднённым для 20 обученных сетей. Обучения и тестирование проводилось на выборках по 60 примеров каждая, из которых 30 соответствовали нажатию и 30 отпусканию клавиш.

Таблица 1

Зависимость средней ошибки обученной нейросети от длины вектора признаков и активационных функций скрытых слоёв

Количество коэффициентов	4	8	16	32	64	128	256	512	1024	2048
μ_E(tansig)	0.17	0.04	0.06	0.09	0.04	0.07	0.12	0.14	0.24	0.30
μ_E(logsig)	0.16	0.01	0.02	0.03	0.02	0.02	0.02	0.02	0.05	0.06

Начиная с количества коэффициентов 128–256 дальнейшее увеличение длины вектора не привело к улучшению классификации. При этом сеть с сигмоидальными активационными функциями нейронов скрытых слоёв показала лучшие результаты по сравнению с сетью с тангенциальными функциями. Для оценки влияния количества нейронов в скрытых слоях были проведены серии экспериментов с нейросетями на основе 20, 50 и 100 нейронов в каждом из двух скрытых слоёв. Результаты экспериментов приведены в табл. 2.

Таблица 2

Зависимость средней ошибки обученной нейросети от длины вектора признаков и размерности скрытых слоёв

Количество коэффициентов	4	8	16	32	64	128	256	512	1024	2048
μ_E (tansig) 20×20	0.17	0.03	0.03	0.05	0.03	0.04	0.03	0.05	0.06	0.06
μ_E (tansig) 50×50	0.12	0.01	0.01	0.02	0.01	0.02	0.01	0.03	0.03	0.06
μ_E (tansig) 100×100	0.12	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.03	0.05
μ_E (logsig) 20×20	0.14	0.01	0.01	0.03	0.03	0.02	0.01	0.03	0.03	0.05
μ_E (logsig) 50×50	0.15	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.03
μ_E (logsig) 100×100	0.18	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.01

На основе полученных данных в задаче распознавания клавиш можно сделать вывод о целесообразности ограничения количества коэффициентов в векторе признаков величинами 128–256 при выборе размерности скрытого слоя 50 нейронов с сигмоидальными функциями активации.

Графики откликов нейронной сети приведены на рис. 3.

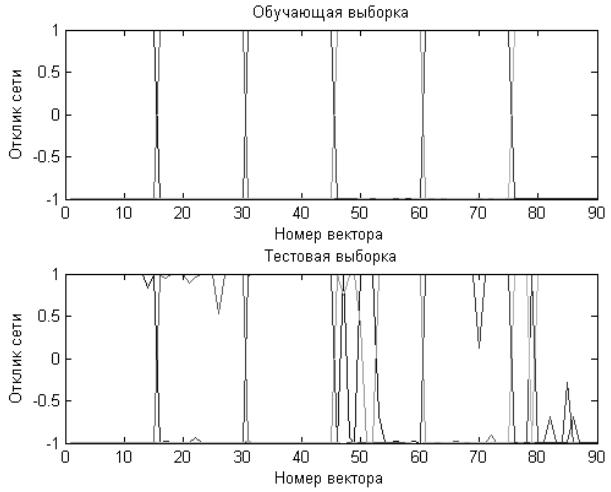


Рис. 3. Классификация векторов признаков 6-ти классов

Установлено, что при увеличении количества классов точность распознавания снижается. Так для 6-ти классов для сети 50x50x6 была получена оценка средней ошибки классификации, равная 0.1317 при значении 0.017 для 4-х классов.

Выводы. Для целей идентификации клавиш наилучшие результаты показывают сети с сигмоидальными функциями активации, двумя скрытыми слоями и 50 нейронами в каждом слое. Практически применимое максимальное количество классов для нейросетей составляет 3, таким образом для идентификации клавиш необходимо применение дихотомической схемы. Наиболее устойчивыми признаками в задаче идентификации клавиш по виброакустическим сигналам, возникающим при наборе произвольного текста, являются коэффициенты преобразования Фурье.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Rublev D., Fedorov V., Makarevich O.* Digital Camera Identification System, Aksaray, Turkey SIN '13, November 26-28 2013. – P. 297-300.
2. *Ilonen J.* Keystroke Dynamics // Lappeenranta University of Technology. 2008.
3. *Федоров В.М., Рублев Д.П.* Идентификация пользователя по виброакустическим шумам, возникающим при наборе парольной фразы на клавиатуре // Сб. трудов конференции «Системотехника-2013». – Таганрог, 2013. – С. 158-163.
4. *Фёдоров В.М., Рублёв Д.П.* Методы предварительной обработки виброакустических сигналов от клавиатуры возникающих при наборе текста // Информационное противодействие угрозам терроризма. – 2012. – № 18. – С. 172-175.
5. *Фёдоров В.М., Рублёв Д.П.* Фильтрация виброакустических сигналов от клавиатуры и манипулятора мышь, возникающих при работе оператора // Информационное противодействие угрозам терроризма. – 2012. – № 19. – С. 160-162.
6. *Федоров В.М., Рублев Д.П.* Обработка виброакустических шумов, возникающих при работе пользователя с клавиатурой // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 75-81.
7. *Бабенко Л.К., Федоров В.М., Юрков П.Ю.* Аутентификация диктора с использованием изменяемого множества ключевых слов // Известия ТРТУ. – 2004. – № 1 (36). – С. 128.
8. *Федоров В.М., Рублев Д.П., Панченко Е.М.* Сегментация виброакустических сигналов, возникающих при нажатии/отпускании клавиш клавиатуры // Материалы докладов конференции «Информационная безопасность 2013». – Таганрог, 2013.
9. *Федоров В.М., Рублев Д.П.* Автоматическая система обнаружения речевых сообщений при мониторинге радиообмена // Сб. трудов конференции «Системотехника-2013». – Таганрог, 2013. – С. 152-158.
10. *Федоров В.М., Рублев Д.П., Панченко Е.М.* Идентификация пользователя по виброакустическим шумам, возникающим при наборе произвольного текста на клавиатуре // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 241-246.

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

Федоров Владимир Михайлович – Южный федеральный университет; e-mail: vladmih@rambler.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; к.ф.-м.н.; доцент.

Рублёв Дмитрий Павлович – e-mail: rublev-d@yandex.ru; к.т.н.; доцент.

Fedorov Vladimir Mikhailovich – Southern Federal University; e-mail: vladmih@rambler.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; cand. of phis.-math. sc.; associate professor.

Rublev Dmitry Pavlovich – e-mail: rublev-d@yandex.ru; cand. of eng. sc.; associate professor.