

УДК 57.087.1:621.391.26

О.Н. Файзулаева

Харьковский национальный университет радиоэлектроники, Харьков

## ТЕХНОЛОГИЯ ВВОДА И ВЫДЕЛЕНИЯ ГОЛОСОВОГО СИГНАЛА ПОЛЬЗОВАТЕЛЯ В СИСТЕМАХ АУТЕНТИФИКАЦИИ

*Рассматриваются технологические аспекты ввода и выделения голосового сигнала пользователя в системах аутентификации. Анализируется использование двух микрофонов для регистрации голосового сигнала пользователя, а также квадратурная схема цифровой обработки материалов регистрации. Оценены возможности адаптивного подавления мешающих сигналов.*

**Ключевые слова:** аутентификация, биометрия, голосовой сигнал, квадратурная обработка.

### Введение

Государственные организации, коммерческие структуры и частные лица заинтересованы в обеспечении безопасности использования современных информационных технологий. Несмотря на то, что на системы безопасности, и системы аутентификации пользователей в частности, выделяются значительные средства, в печати периодически появляются сообщения о несанкционированном доступе посторонних лиц к ресурсам ряда серьезных организаций. Обман и злоупотребления со стороны своих сотрудников наносят ущерб около 6% годовой прибыли, составляя, в среднем, около \$100.000 на каждый случай (в 14,6% случаев потери превысили \$1.000.000) (Association of Certified Fraud Examiners, 2004) [1, 2]. В банковской сфере от злонамеренной деятельности сотрудников финансовые потери могут достигать огромных величин. Несанкционированный доступ к конфиденциальной информации о финансовой деятельности компании, контрактах и планах чреват не только потерями, но и полным банкротством.

Повышение эффективности современных систем аутентификации пользователей связывают с биометрией. Биометрия появилась в конце XIX века как раздел науки, занимающейся количественными биологическими экспериментами с привлечением статистических методов. Полвека назад интерес к биометрии получил новый импульс в связи с появлением биометрических систем безопасности.

Биометрия принадлежит к тем областям современных технологий, темп развития которых значительно увеличился после драматических событий 11 сентября 2001 года в Нью-Йорке. Многократно выросло финансирование биометрических исследований, выполняемых как коммерческими, так и государственными структурами. На рынке биометрических продуктов имеются устоявшиеся лидеры – Identix, Digital Persona, Precise Biometrics, Visionics, Ethentica, BioScript, Secugen, AcSys Biometrics. Одновременно появились корпорации, не специализирующиеся в области биометрии – Sony, LG, Compaq и др., которые выделяют значительные средства в разработку био-

метрических систем [3, 4]. Это говорит о значительном увеличении привлекательности рынка и о том, что в скором будущем биометрические устройства станут привычной частью нашего быта.

Биометрические системы безопасности – это автоматизированные методы и средства идентификации личности посредством измерения уникальных физиологических особенностей или поведенческих характеристик человека и их сравнения с эталонами, хранящимися в соответствующих базах данных.

Первоначально основные усилия по решению стран «восьмерки» были сосредоточены на дактилоскопии (распознавание отпечатков пальцев), распознавании геометрии лица и радужной оболочки глаза. Эти идентификаторы рекомендовано использовать и при изготовлении биометрических паспортов.

В основу работы биометрических систем положена математическая статистика (а именно, проверка гипотез [5]), алгоритмы которой интенсивно используются в ряде современных технических систем, таких как: связь, радиолокация (различные радары), множестве байесовских систем. В качестве двух основных характеристик любой биометрической системы, построенной на основе статистической теории проверки гипотез (тестов), можно принять ошибки первого и второго рода [5, 6]. В теории радиолокации их обычно называют «пропуск цели» и «ложная тревога», а в биометрии, наиболее устоявшиеся понятия – FRR (False Rejection Rate, ложный отказ) и FAR (False Acceptance Rate, ложное распознавание). Первое число характеризует вероятность отказа доступа человеку, имеющему допуск. Второе – вероятность ложного совпадения биометрических характеристик двух людей.

Система тем лучше, чем меньше значение FAR при одинаковых значениях FRR. Иногда используется и сравнительная характеристика EER (Equal Error Rate, равный коэффициент ошибок), определяющая точку в которой графики FRR и FAR пересекаются.

Но не только FAR и FRR определяют качество биометрической системы. Если бы это было только так, то лидирующей технологией было бы распознавание людей по ДНК, для которой FAR и FRR стремятся

к нулю. Но ведь очевидно, что эта технология не применима на сегодняшнем этапе развития человечества!

Поэтому в ряде работ [1, 2] предложено несколько эмпирических характеристик, позволяющих оценить качество системы. «Устойчивость к подделке» – это эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор. «Устойчивость к окружающей среде» – характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях, таких как изменение освещения или температуры помещения. «Простота использования» показывает насколько сложно воспользоваться биометрическим сканером, возможна ли идентификация «на ходу». Важной характеристикой является «Скорость работы», и «Стоимость системы». Не стоит забывать и то, что биометрическая характеристика человека может изменяться со временем, так что если она неустойчива – это существенный минус.

В настоящее время используемые биометрические системы имеют характеристики FAR и FRR на уровне  $n \cdot 10^{-2}$ . В то время как в современных радарах условная вероятность ложной тревоги находится на уровне  $1 \cdot 10^{-12}$  и ниже. При этом требования к ошибкам 1-го рода не такие жесткие. Именно этот путь является основным для выбора требований к качественным характеристикам биометрических систем.

Однако, к настоящему времени установлено, что перечисленные выше идентификаторы (дактилоскопия, геометрия лица, радужная оболочка глаза) не дают возможность создать качественные и надежные биометрические системы безопасности, поскольку обработке подвергаются ограниченные фиксированные данные (например, отпечаток пальца).

Один из путей решения задачи создания качественных и надежных систем – использование голосовой аутентификации, которая имеет следующие достоинства:

- простота, компактность, низкая стоимость устройств ввода информации;
- ввод информации осуществляется дистанционно, без участия рук;
- реализация процедур аутентификации осуществляется алгоритмически с приемлемыми вычислительными затратами, поскольку обработке подвергается временной ряд;
- динамически меняющаяся парольная фраза, которая для обеспечения требуемых характеристик может наращиваться в процессе оперативной аутентификации;
- работа в темноте и в условиях сильных шумов;
- устойчивая работа в каналах связи для обеспечения удаленной аутентификации.

Определенные надежды связаны с использованием нескольких микрофонов для ввода голосового

пароля. К настоящему времени несколько микрофонов в голосовой аутентификации рассматривалось в следующих работах:

– в [7] рассматривался метод компенсации характеристик канала регистрации с помощью стереозаписи;

– в [8] рассматривался метод оценки расстояния до четырех микрофонов с целью компенсации характеристик канала регистрации.

Использование нескольких микрофонов дает возможность, в первую очередь, реализовать пространственно-временную обработку, которая эффективна, например, для снижения влияния офисных шумов (шум вентилятора, шум компьютера, фоновая речь и т.д.). Одновременно повышается отношение сигнал/шум, которое существенно влияет на качественные характеристики голосовых систем аутентификации.

Введение двух микрофонов требует проведения расчетов, которые связаны с решением оптимизационной задачи – поскольку необходимо обосновать расстояние между микрофонами, которое будет определять диаграмму направленности для регистрируемых длин волн.

При этом необходимо учесть габаритные размеры мобильных устройств (ноутбуки, телефоны и т.д.).

Таким образом, целью данной статьи – оценка эффективности и обоснование технологии построения системы ввода голосового сигнала в вычислительную систему, включая и мобильные устройства, для последующей реализации пространственно-временной обработки.

Объект исследования – процесс пространственно-временной обработки голосового сигнала на основе двухэлементной антенной решетки ненаправленных микрофонов.

Методы исследований – аналитические расчеты, математическое моделирование, анализ результатов и формулирование выводов.

## Методика и результаты исследований

Для проведения расчетов и последующего моделирования системы ввода голосового сигнала рассмотрим рис. 1, на котором используются следующие обозначения. M1 и M2 – микрофоны, размещенные в пространстве на некоторое расстояние  $d$  по оси антенной решетки. Будем полагать, что полезный сигнал поступает по нормали к оси антенной решетки.

Мешающие сигналы могут поступать с произвольных направлений (рис. 1).

Таким образом, первая задача связана с выбором расстояния между микрофонами, которое существенно влияет на вид диаграммы направленности и процедуры последующей обработки.

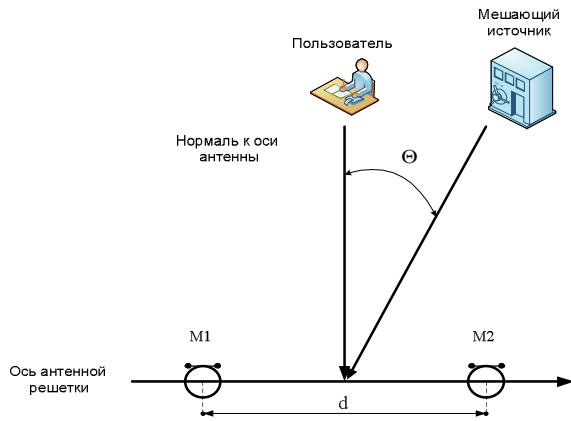


Рис. 1. Антенная решетка, состоящая из двух микрофонов

Аналогичная задача применительно к радиодиапазону была рассмотрена в [9]. Поэтому здесь воспользуемся основными соотношениями, представленными в данной работе, и оценим диаграмму направленности двухэлементной решетки для голосового сигнала.

Основные отличия голосового сигнала – скорость распространения звуковой волны, равная 340 м/с, что приводит к изменению, как длины волны, так и времени задержки. Диаграмма направленности решетки определяется соотношением

$$A(\Theta) = \sum_{i=1}^2 \exp(j(i-1)\Psi),$$

где  $\Psi = 2 \cdot \pi \cdot (d/\lambda_0) \cdot \sin(\Theta)$ ;  $i = 1$  и  $2$  – номер микрофона;  $\lambda_0$  – длина регистрируемой волны;  $\Theta$  – аргумент (угол прихода волны), который изменяется в рассматриваемом случае в пределах от  $0^\circ$  до  $\pm 90^\circ$ . Пределы изменения угла  $\Theta$  обусловлены тем, что микрофоны должны быть установлены, например, на клавиатуре персонального компьютера, под дисплеем ноутбука, на панели планшета и т.д. В этом случае с других направлений звуковая волна на микрофоны не попадет.

Нормированная диаграмма направленности решетки с двух микрофонов, измеренная в децибелах, определяется как

$$G(\Theta)[\text{дБ}] = 10 \lg \{ |A(\Theta)|^2 / 4 \}.$$

Обратим внимание на следующее. В работе [10] было найдено три информативные области, которые влияют на различимость диктора: 100 – 300 Гц (влияние голосового источника), 4 – 5 кГц (грушевидные полости) и 6, 5 – 7,8 кГц – (возможно, влияние согласных). Небольшая область – находится в районе 1 кГц. Результаты работы [10] подтверждают ранее установленные в [11] информативные области спектра речевых сигналов.

В работе [11] было выявлено, что наибольшая информация о дикторе находится в полосах ниже

600 Гц и выше 3000 Гц. Частотный диапазон стандартного телефонного канала 300 – 3400 Гц обрезаем высокие частоты, ухудшая различимость голоса диктора. Поэтому в дальнейшем при выборе расстояния между микрофонами учтем, что необходимо качественно регистрировать голосовой сигнал в диапазоне от 100 Гц до 8 кГц.

В связи с этим, расстояние между микрофонами целесообразно выбрать таким, чтобы диаграмма направленности имела один (или главный) лепесток (нули при  $\Theta = \pm 90^\circ$ ) в процессе регистрации длин волн от 100 Гц до 8 кГц. Такая диаграмма позволит качественно регистрировать сигнал пользователя голосовой системы аутентификации, поступающий по нормали к оси антенны, и ослаблять мешающие звуковые волны с других направлений. Результаты расчета диаграммы направленности для  $d = 10$  мм представлены на рис. 2.

Увеличивать расстояние между микрофонами можно до 20 мм. При этом будет сохраняться один главный лепесток и нули при  $\Theta = \pm 90^\circ$ .

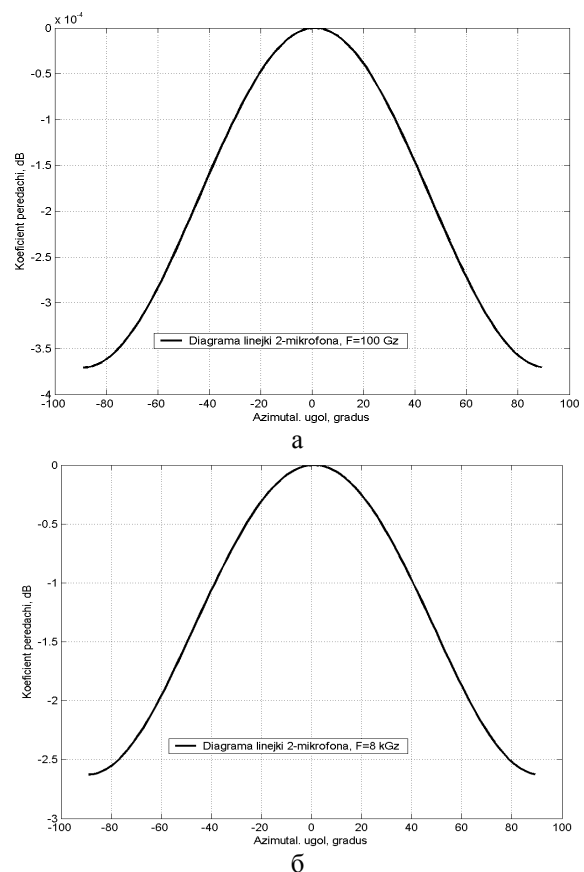


Рис. 2. Диаграмма направленности решетки из 2-х микрофонов для  $d = 10$  мм и частот регистрируемых волн: а – 100 Гц; б – 8 кГц

Дальнейшее увеличение расстояния между микрофонами на частоте регистрируемого сигнала 8 кГц приводит к смещению нулей в точку  $\pm 60^\circ$ . Заметим, что диаграммы направленности отличаются

только коэффициентом передачи. Например, для  $d = 10$  мм коэффициент передачи для волны 100 Гц и 8 кГц отличаются почти на 4 порядка. Для  $d = 20$  мм эта разница еще больше.

Таким образом, возможное расстояние между микрофонами должно выбираться в пределах от 10 до 20 мм. При этом, как будет показано ниже, это расстояние целесообразно выбирать ближе к 20 мм, что позволит проще подавлять высокочастотные помеховые сигналы.

Наряду с преимуществами (удобство размещения микрофонов на мобильных «гаджетах» и наличие одного лепестка в диаграмме направленности для диапазона регистрируемых волн) такое размещение микрофонов имеет и существенные недостатки. Из теории антенных решеток известно, что для качественной обработки сигналов оптимальное расстояние между элементами должно выбираться из условия  $d = \lambda/2$ , где  $\lambda$  – длина регистрируемых волн. В случае, если расстояние между элементами решетки  $d < \lambda/2$ , то не будет качественного подавления сигналов поступающих с других направлений.

Дальнейшие процедуры связаны с цифровой обработкой сигналов, обусловленных зарегистрированными звуковыми волнами. Требования к временной дискретизации сигналов установлены в [12] и для диапазона регистрируемых волн будут составлять около 60 кГц. Далее необходимо определить структурную схему процедур обработки.

В отличие от [13], где задачи локализации источника звука решаются за счет систем TDOA (Time-Difference-Of-Arrival – разность времени прихода сигнала), при обработке будет дополнительно учитываться квадратурная составляющая регистрируемых сигналов. Качественное формирование и учет квадратурной составляющей зарегистрированного сигнала, даст возможность более тонко восстановить его структуру, что является очень важным в процессе аутентификации пользователя.

Структурная схема такой обработки рассмотрена в [9, 14] и представлена на рис. 3. При этом используются следующие обозначения: M1 и M2 – микрофоны, как и ранее, разнесенные в пространстве на расстояние  $d$  по оси антенной решетки;  $\pi/2$  – программные формирователи квадратурной составляющей голосового сигнала;  $\omega_i$  – весовые коэффициенты;  $i = 1, \dots, 4$ ; X – умножители, реализующие весовую обработку; + – сумматор.

При воздействии узкополосного помехового сигнала в пределах углов  $0^\circ < \Theta < 55^\circ$  представленная схема обработки обеспечивает качественное подавление указанного воздействия при постоянных весовых коэффициентах:  $\omega_1 = 0.5$ ,  $\omega_2 = 0.5$ ,  $\omega_3 = 0.5$ ,  $\omega_4 = -0.5$ . При этом обязательным является разнесение микрофонов на расстояние  $d = \lambda/2$ . Здесь  $\lambda$  – длина волны помехового сигнала. Заме-

тим, что для подавления помехового сигнала из второй четверти (углы  $-55^\circ < \Theta < 0^\circ$ ) величина коэффициентов должна быть изменена следующим образом:  $\omega_1 = 0.5$ ,  $\omega_2 = 0.5$ ,  $\omega_3 = -0.5$ ,  $\omega_4 = 0.5$ , что составляет определенную трудность в практической реализации указанных процедур обработки. Кроме этого, качество подавления помехового сигнала снижается и при уменьшении расстояния между микрофонами до 20 мм.

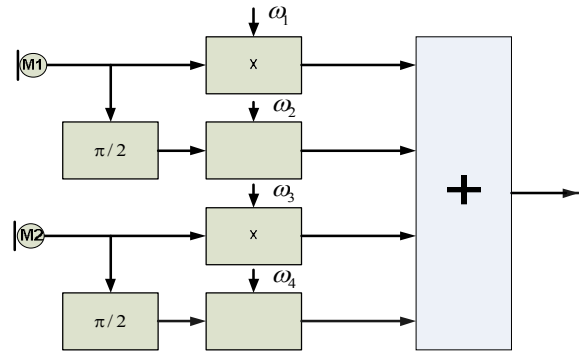


Рис. 3. Структурная схема устройства обработки

С целью повышения качества подавления помеховых сигналов для систем аутентификации было исследовано влияние применения адаптивного алгоритма расчета весовых коэффициентов [15]. Процедуры расчета весовых коэффициентов сводились к следующему. Сигнал ошибки для  $i$ -го канала и  $j$ -го такта обработки определим как разность между входным сигналом и выходом системы обработки, т.е.

$$\varepsilon_{ij} = x_{ij} - X_j^T \cdot W_j,$$

где  $x_{ij}$  – входной сигнал  $i$ -го канала и  $j$ -го такта обработки;  $X_j^T = (x_{1j}, x_{2j}, x_{3j}, x_{4j})$  – вектор входных сигналов  $j$ -го такта обработки;  $W_j^T = (\omega_{1j}, \omega_{2j}, \omega_{3j}, \omega_{4j})$  – вектор весовых коэффициентов для  $j$ -го такта обработки;  $X_j^T \cdot W_j$  – выходной сигнал системы обработки;  $T$  – знак транспонирования.

Каждый последующий весовой коэффициент  $i$ -го канала  $W_{i+1}$  равен сумме предыдущего коэффициента этого канала  $W_{ij}$  и переменной составляющей, пропорциональной значениям ошибки в этом канале

$$W_{i+1} = W_{ij} + 2 \cdot \mu \cdot x_{ij} \cdot \varepsilon_{ij},$$

где  $\mu$  – это коэффициент, который определяет устойчивость и сходимость процесса адаптации.

Представленные процедуры адаптивного расчета весовых коэффициентов в литературе имеют название алгоритма минимума среднеквадратического отклонения Уидроу-Хоффа. На величину коэффициента, определяющего устойчивость и сходи-

мость процесса адаптации, накладываются следующие ограничения

$$0 < \mu < 1/\lambda_{\max},$$

где  $\lambda_{\max}$  – максимум собственного значения корреляционной матрицы входных сигналов.

Предлагается следующая технология применения рассмотренных процедур во время аутентификации пользователя.

На первом этапе (идентификации пользователя, например, с использованием пароля) выполняется уточнение весовых коэффициентов с учетом текущей помеховой и шумовой обстановки в помещении. Длительность уточнения величины коэффициентов зависит от величины коэффициента  $\mu$ , меньшему значению коэффициента соответствует большее время адаптации. На втором этапе – во время ввода голосового сигнала пользователя используются коэффициенты, полученные на предыдущем этапе. При этом целесообразно регистрировать как входные сигналы, так и результаты обработки. Они могут потребоваться в процессе последующей обработки.

Для формирования квадратурной составляющей целесообразно использовать преобразование Гильберта-Хуанга, которое обеспечивает не только качественную обработку сигналов с нестационарными и нелинейными искажениями, но и дает возможность повысить отношение сигнал/шум за счет исключения зашумленной первой модовой функции [12].

Результаты использования рассмотренных процедур представлены на рисунках, которые представлены ниже. При этом на рис. 4 показан процесс адаптации по помеховому сигналу с частотой 7700 Гц. Анализ рисунков показывает, что при  $\mu=0,002$  для адаптации достаточно обработать 150, ..., 250 дискрет помехового сигнала. В то же время при  $\mu=0,001$  – число обрабатываемых дискрет увеличивается до значения более 300. Уточнение величины весовых коэффициентов позволяет уменьшить амплитудные значения помехового сигнала почти в 5 раз.

На рис. 5 ( $\Theta = 70^\circ$ ) представлены результаты обработки смеси полезного (4500 Гц) и помехового (7700 Гц) сигналов. При этом результат системы обработки показан сплошной линией, а эталонный сигнал штриховой линией.

Анализ рисунков свидетельствует о более качественной обработке адаптивных процедур, которая слабо зависит от угла прихода помехового сигнала. В качестве критерия качества обработки рассматривался коэффициент корреляции. Величины этого коэффициента при  $\Theta = 70^\circ$  были равны: 0,77 – постоянные весовые коэффициенты; 0,9 – адаптивные коэффициенты.

Недостатком рассмотренной схемы обработки является недостаточное ее качество при низкой частоте помехового сигнала (помеха действует в начале канала тональной частоты). В этом случае, достаточно сложно рассчитать оптимальную величину весовых коэффициентов, из-за малого разнеса микрофонов.

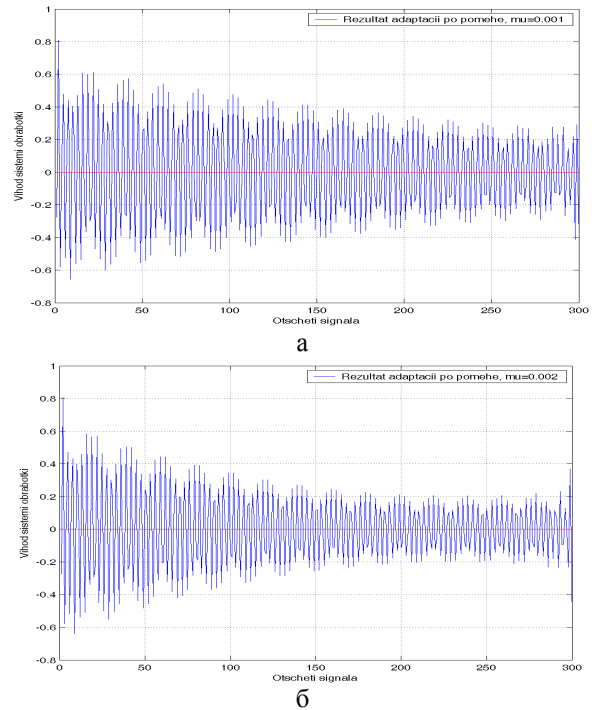


Рис. 4. Процесс адаптации по помеховому сигналу 7700 Гц, решетка из 2-х микрофонов для  $d = 20$  мм: а –  $\mu=0,001$ ; б –  $\mu=0,002$

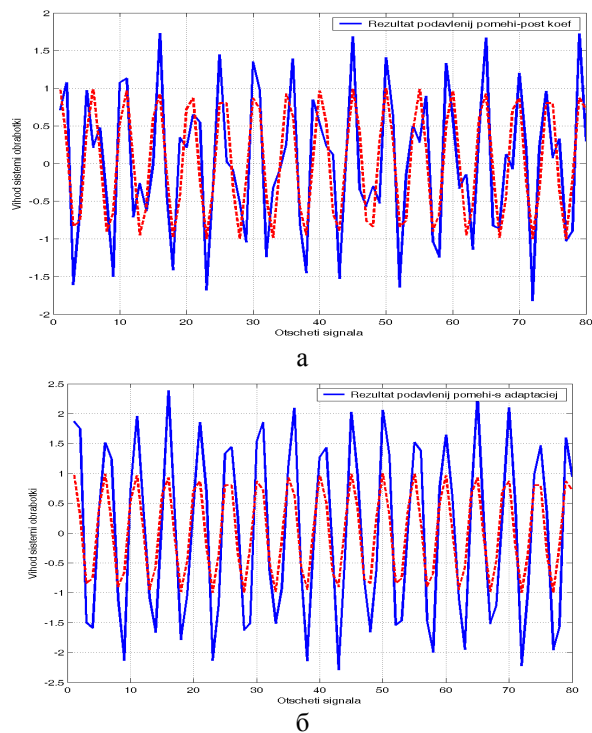


Рис. 5. Результат регистрации полезного сигнала 4500 Гц, помеха – 7700 Гц, решетка из 2-х микрофонов для  $d = 20$  мм: а – постоянные коэффициенты; б – адаптивные коэффициенты

Для устранения этого недостатка можно, конечно, установить дополнительный микрофон, чтобы обеспечить большее расстояние между микрофонами, и в дальнейшем использовать рассмотренные выше процедуры обработки. Но этот вариант

потребує введення додаткового каналу реєстрації. Крім цього, різниця мікрофонів повинна становити приблизно 70 мм і більше, що не завжди можна реалізувати на мобільних пристроях. Тому нижче розглянемо варіант алгоритмічного пересчету реєструваного сигналу для третього віртуального мікрофона, який розташований на відстані рівній половині довжини хвилі поміхового сигналу. Будемо полагати, що нам відомо на якому відстані необхідно розташувати мікрофони для подавлення діючої поміхи (іли, інакше, відома частота поміхового сигналу) і її кут приходу. Отримати ці дані можна використавшись співвідношеннями, представленими в [13].

Для розрахунку матеріалів реєстрації третього віртуального мікрофона необхідно взяти різницю часу затримки по відношенню до другого мікрофону. Ця різниця може бути пересчитана в кількість інтервалів дискретизації з точністю до сотих долей. Після цього, проводиться пересчет даних реєстрації другого мікрофона. Аналогічна корекція вимагається і для матеріалів реєстрації першого мікрофона. Далі проводиться обробка «затриманих» матеріалів реєстрації з постійними ваговими коефіцієнтами, запропонованими в [9, 14]. Результати обробки «откоректованих» матеріалів реєстрації з використанням розглянутого підходу представлені на рис. 6.

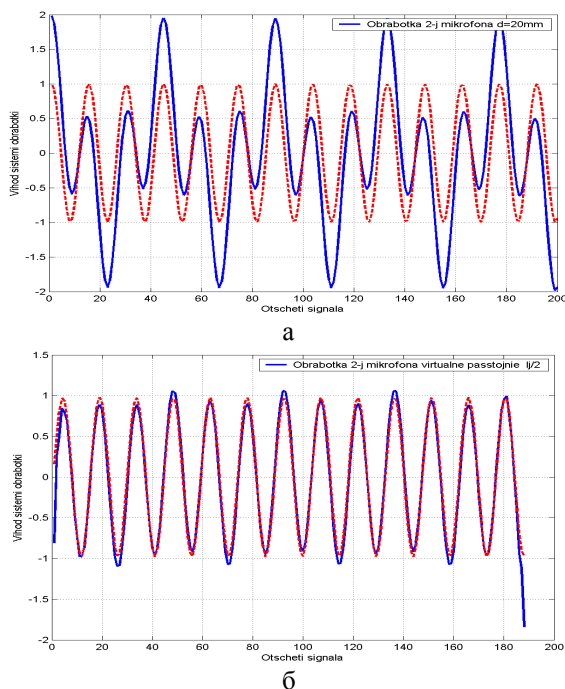


Рис. 6. Результат реєстрації корисного сигналу 500 Гц, поміха – 1500 Гц, решітка з 2-х мікрофонів: а – відстань  $d = 20$  мм; б – відстань  $d = \lambda_n / 2$

На рис. 6  $\lambda_n$  – довжина хвилі поміхового сигналу. Аналіз представлених залежностей свідчить про значительне підвищення якості обробки з використанням третього віртуального

мікрофона. При цьому пред'являються не достаточні високі вимоги до куту приходу поміхового сигналу (приблизно  $\pm 10^\circ$ ) [13].

Обобщая изложенное выше, можно предложить следующую технологию ввода и выделения голосового сигнала в процессе аутентификации пользователя (рис. 7). На первом этапе реализуется вариант адаптивного формирования весовых коэффициентов (блоки 1, ..., 3). Решение о качестве формирования весовых коэффициентов формируется в блоке 4, где происходит сравнение среднеквадратических отклонений входного поміхового сигнала и сигнала с выхода системы обробки. При уменьшении величины среднеквадратического отклонения, что является фактом формирования оптимальных значений весовых коэффициентов, весовые коэффициенты фиксируются и производится ввод голосового сигнала пользователя системы аутентификации. В дальнейшем осуществляется обробка смеси голосового и поміхового сигналов с помощью адаптивной схемы обробки (блоки 5, ..., 8).

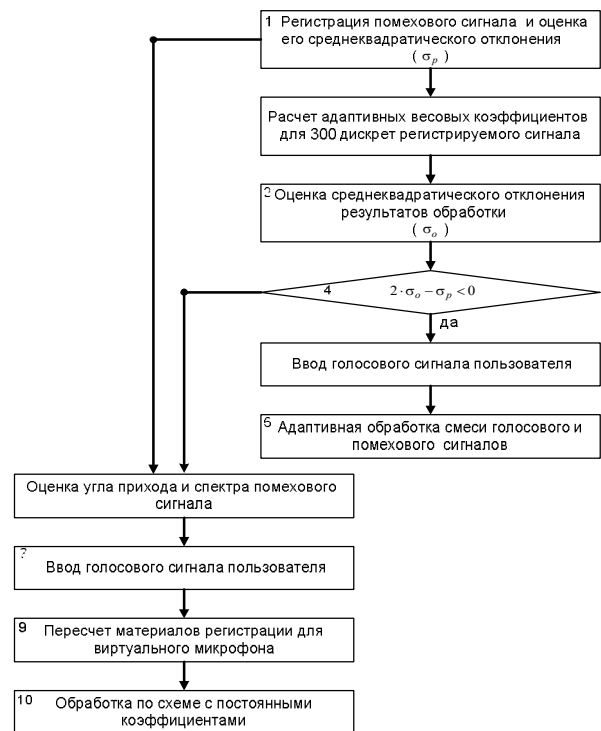


Рис. 7. Технологія введення та виділення голосового сигналу

Если рассчитанное среднеквадратическое отклонение после обробки первых 300 дискрет поміхового сигнала с адаптивными ваговими коефіцієнтами не уменьшается, то это является признаком наличия в поміхе низкочастотной составляющей. В этом случае оценивается кут прихода и спектр мешающего сигнала. Полученные оценки являются исходными данными для пересчета материалов реєстрації второго мікрофона к месту расположения третьего виртуального мікрофона, а также коррекции материалов реєстрації в первом мікрофоне. Далее

осуществляется выделение голосового сигнала с постоянными весовыми коэффициентами.

## Выводы и направления дальнейших исследований

Технология ввода и выделения голосового сигнала сводится к следующему. Два микрофона должны располагаться на расстоянии примерно 20 мм. Для выделения голосового сигнала пользователя необходимо использовать квадратурную схему, рассмотренную выше. Формирование квадратурной составляющей целесообразно выполнять с помощью преобразования Гильберта-Хуанга. Для зашумленных сигналов из обработки исключается первая модовая функция. Подавление высокочастотной составляющей помехового сигнала осуществляется с помощью адаптивной весовой обработки. Низкочастотную составляющую мешающего сигнала можно подавлять, используя процедуры пересчета регистрируемого сигнала на третий виртуальный микрофон и использования схемы выделения сигнала с постоянными коэффициентами.

Дальнейшие исследования будут ориентированы на экспериментальную оценку реальных мешающих сигналов (работа серверов, коммутационной аппаратуры, компьютеров локальной сети и т.д.), а также проверку предложенной технологии ввода и выделения голосовых сигналов пользователя. Кроме этого, требуются дополнительные исследования процедур формирования адаптивных весовых коэффициентов, которые будут удовлетворять всему диапазону голосового сигнала (от 100 до 8000 Гц).

## Список литературы

1. Сорокин В.Н. Распознавание личности по голосу: аналитический обзор / В.Н. Сорокин, В.В. Вьюгин, А.А. Тананыкин // Информационные процессы. – М.: РАН. – 2012. – Том 12, № 1. – С. 1-30.
2. Форум сообщества практиков конкурентной разведки. [Электрон. ресурс]. – Режим доступа до Internet-ресурсу: <http://forum.razved.info>.
3. Обзор новейших технологий. [Электрон. ресурс]. – Режим доступа до Internet-ресурсу: <http://www.bellabs.ru/SF>.
4. Сравнительный анализ специализированных систем управления доступом на базе биометрии / В.М. Лукашенко, С.А. Миценко, Ю.Ю. Терещенко, Е.П. Лукацкая // Режим доступа до Internet-ресурсу: [http://www.rusnauka.com/35\\_OINBG\\_2010/Informatica/76318.doc.htm](http://www.rusnauka.com/35_OINBG_2010/Informatica/76318.doc.htm).
5. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 1999. – 479 с.
6. Теоретические основы радиолокации / под ред. Я.Д. Ширмана. – М.: Сов. радио. 1970. – 560 с.
7. Murthy H.A., Robust text-independent speaker identification over telephone channels / H.A. Murthy, F. Beaufays, K.P. Heck, M. Weintraub // IEEE Trans. Speech and Audio Process., v.7, 1999, S. 554-558.
8. Wang L. Robust distant speaker recognition based on position-dependent CMN by combining speaker-specific GMM with speaker-adapted HMM / L. Wang, N. Kitaoka, S. Nakagawa // Speech Communication, v. 49, 2007, S. 501-513.
9. Монзинго Р.А. Адаптивные антенные решетки: Введение в теорию / Р.А. Монзинго, Т.У. Миллер. – М.: Радио и связь, 1986. – 448 с.
10. Lu X. An investigation of dependencies between frequency components and speaker characteristics for text-independent speaker identification / X. Lu, J. Dang // Speech Communication, v.50, N4, 2007, S.312-322.
11. Besacier L., Bonastre J.-F. Subband architecture for automatic speaker recognition / L. Besacier, J.-F. Bonastre // Signal Process., v.80, 2000, S.1245-1259.
12. Белоусова Е.Э. Анализ влияния частоты дискретизации на качество формирования квадратурной составляющей аналитического сигнала / Е.Э. Белоусова, Н.С. Пастушенко, О.Н. Пастушенко. – Восточно-Европейский журнал передовых технологий. – 2013. – № 1/9(61) – С. 8-13.
13. Мокрецов А.В. Погрешность определения угла местоположения источника звука микрофонной системой с алгоритмом пространственно-временной обработки сигнала / А.В. Мокрецов // Инженерный вестник Дона. – 2012. – № 3 – С. 52-54.
14. Адаптивная компенсация помех в каналах связи / Ю.И. Лосев, А.Г. Бердников, Э.Ш. Гойхман, Б.Д. Сизов. – М.: Радио и связь, 1988. – 208 с.
15. Уидроу Б. Компенсация помех. Принципы построения и применения / Б. Уидроу // ТИИЭР. – 1975. – № 12 – С. 69-97.

Поступила в редколлегию 6.11.2013

**Рецензент:** д-р техн. наук, проф. В.В. Поповский, Харьковский национальный университет радиоэлектроники, Харьков.

## ТЕХНОЛОГІЯ ВВЕДЕННЯ І ВИДІЛЕННЯ ГОЛОСОВОГО СИГНАЛУ КОРИСТУВАЧА В СИСТЕМАХ АУТЕНТИФІКАЦІЇ

О.М. Файзулаева

Розглядаються технологічні аспекти введення і виділення голосового сигналу користувача в системах аутентифікації. Аналізується використання двох мікрофонів для реєстрації голосового сигналу користувача, а також схема квадратури цифрової обробки матеріалів реєстрації. Оцінені можливості адаптивного придушення сигналів, що заважають.

**Ключові слова:** аутентифікація, біометрія, голосовий сигнал, обробка квадратури.

## TECHNOLOGY OF INPUT AND SELECTION OF VOCAL SIGNAL OF USER IS IN THE SYSTEMS OF AUTHENTICATION

O.N. Fayzulaeva

Examined technological aspects of input and selection of vocal signal of user in the systems of authentication. The use of two microphones is analysed for registration of vocal signal of user, and also squaring chart of digital treatment of materials of registration. Possibilities of adaptive suppression of mixing signals are appraised.

**Keywords:** authentication, biometrics, vocal signal, squaring treatment.