при передаче речи по каналам коммуникаций, контроля время разговора без оператора в устройствах коммуникаций и других приложениях.

В работе рассмотрены следующие критерии детектирования речи: критерий мощности сигнала, критерий количества пересечений с нулем, критерий динамики изменения мощности сигнала, критерий особенностей речевого сигнала в спектральной области, критерий стационарности, критерий по шлейфу сигнала. Для каждого критерия описан алгоритм применения критерия с возможными параметрами реализации. Детально рассмотрен критерий по шлейфу сигнала, позволяющий детектировать сигналы типа речь, музыка, транспортный шум.

Детектор речи может быть оптимизирован по точности, скорости выполнения задачи, или в некоторой степени компромисса между ними. Наиболее часто детекторы речи требуют больших вычислительных мощностей вследствие использования для анализа большого числа признаков с применением комплексных вычислений. Показано, что использование ограниченного числа критериев детектирования речи и простейших методов обработки позволяют использовать такие алгоритмы детектирования в микропроцессорных устройствах при работе в реальном режиме времени.

## ДЕТЕКТИРОВАНИЕ РЕЧИ РУССКОЯЗЫЧНОГО ДИКТОРА-БИЛИНГВА

Е.О. БАРАНОВСКИЙ

Современные условия жизни общества сопряжены со значительной миграцией населения, в связи с чем много людей пользуются в общении двумя и более языками. Способность владения двумя и более языками называется билингвизмом. Билингвизм является предметом изучения различных наук, каждая из которых рассматривает билингвизм в своей трактовке. В произношении билингвов присутствует явление интерференции (отрицательное влияние одного языка на другой), которое является предметом исследования для систем детектирования речевых сигналов.

Детектирование речи является важной частью современных приложений по обработке речевых сигналов. Алгоритмы детектирование речи используется в системах кодирования и распознавания речи, а также в системах повышения ее качества. Алгоритмы детектирования часто являются наиболее критической частью таких систем, и определяют качество всей системы в целом.

В основе большинства методов обработки речи лежит предположение о том, что свойства речевого сигнала с течением времени медленно изменяются. Это предположение приводит к методам кратковременного анализа, в которых сегменты речевого сигнала выделяются и обрабатываются так, как если бы они были короткими участками отдельных звуков с отличающимися свойствами.

Методика детектирования основана на вычислении мел-частотных кепстральных коэффициентов слов русского языка. В ходе работы были проанализированы слова русского языка, которые произносились различными дикторами. Одним из дикторов был носитель русского языка. В качестве второго диктора выступал диктор-билингв (русскоязычный диктор арабского происхождения). Результаты соответствия вычисляются при помощи алгоритма динамического программирования.

Для того чтобы получить векторы признаков одинаковой длины, нужно сегментировать речевой сигнал на равные части, а затем выполнять преобразования внутри каждого сегмента. Обычно сегменты выбирают таким образом, чтобы они

перекрывались либо наполовину, либо на 2/3. Перекрытие используется для предотвращения потери информации о сигнале на границе.

Для вычисления мел-частотных кестральных коэффициентов, на вход алгоритма подаётся последовательность отсчётов участка сигнала, исследуемого на данной итерации. К данной последовательности применяется весовая функция и затем дискретное преобразование Фурье. Весовая функция используется для уменьшения искажений в Фурье анализе, вызванных конечностью выборки. В качестве весовой функции используется окно Хэммига.

Полученное представление сигнала в частотной области разбивают на диапазоны с помощью банка треугольных фильтров. Границы фильтров рассчитывают в шкале мел. Данная шкала является результатом исследований по способности человеческого уха к восприятию звуков на различных частотах. Перевод в мел-частотную область осуществляется по формуле $B(f)=1127\ln(1+f/700)$.

Количество мел-частотных кепстральных коэффициентов определяется количеством треугольных фильтров. Фильтры применяются к квадратам модулей коэффициентов преобразования Фурье. Полученные значения логарифмируются. Заключительным этапом в вычислении мел-частотных кепстральных коэффициентов является дискретное косинусное преобразование.

## ТЕСТИРОВАНИЕ НА ПРОСТОТУ БОЛЬШИХ ЧИСЕЛ СПЕЦИАЛЬНОГО ВИДА

А.В. ИВАШКЕВИЧ, Е.Д. СТРОЙНИКОВА

С целью создания генератора псевдопростых чисел были реализованы следующие тесты проверки чисел на простоту: Ферма, Миллера–Рабина, Соловея–Штрассена, Лукаса, BPSW. Первые три указанных теста являются вероятностными. Они позволяют очень эффективно отбраковать составные числа, однако не в состоянии строго доказать простоту числа, а лишь позволяют говорить, что число p не является составным с некоторой вероятностью. Наиболее эффективным из этих трех алгоритмов является тест Миллера–Рабина.

Верхняя граница ошибки на одной итерации для теста Миллера–Рабина в 2 раза меньше аналогичной для теста Соловея–Штрассена и в 4 раза — верхней границы ошибки для теста Ферма. Если на одной итерации вероятность ошибочного решения в тесте не превышает 1/4, то на двух итерациях — 1/16, на трех — 1/64. для того чтобы вероятность ошибки не превышала 0,0001, требуется всего 7 итераций, что в 2 раза меньше, чем для теста Соловея–Штрассена.

На основании вышеуказанных алгоритмов был разработан программный модуль генерации простых чисел заданной длины. Для его создания была использованна среда Microsoft Visual Studio 2010 и язык программирования C#.

Основной сложностью при создании модуля генерации стала реализация алгоритмов проверки чисел на простоту.

В результате выполенной работы были получены следующие средние временные результаты генерирования псевдопростых чисел: число длиной 256 бит было сгенерированно за 1 секунду, 512 бит — за 2–3 секунды, 1024 бит — за 55 секунд, 2048 бит — за 600 секунд, 3076 бит — за 7200 секунд.

Созданный программный модуль имеет очень важное практическое применение, так как простые числа являются неотъемлемой частью криптографических алгоритмов, используемых для защиты информации.