АППАРАТНЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ

Г.В. ДАВЫДОВ, А.И. КУХАРЕНКО, В.А. ПОПОВ, А.А. ТЕРЕНЯ

Генераторы случайных чисел (ГСЧ) широко применяются для создания криптостойких паролей, ключей шифрования, защиты каналов передачи данных и др. Удобно реализовать генератор случайных чисел программными средствами. Однако существует опасность, что алгоритм формирования случайных чисел станет известен нарушителю. Поэтому в системах защиты информации предпочтительно использовать аппаратные генераторы случайных чисел.

Важно при создании ГСЧ использовать источник случайного процесса с высокой энтропией. Известно, что максимальной энтропией при прочих равных условиях обладает так называемый «белый» шум.

Для получения «белого» шума в разработанном ГСЧ использован тепловой шум диода. После усиления шумового сигнала он преобразовывался в цифровую форму с помощью восьмибитового АЦП, выполненного на базе микроконтроллера AT90USB1286. Оцифрованный сигнал передавался по шине USB на персональный компьютер. С помощью программного пакета HEX Editor выполнена оценка плотности распределения вероятностей оцифрованного сигнала по его реализации длительностью 30 мин (6400000 выборок). Получена гистограмма этой оценки. Установлено, что сформированный цифровой «белый» шум имеет распределение вероятностей, близкое к гауссовому.

Конечной целью работы было создание ГСЧ с равномерным распределением цифрового сигнала в диапазоне чисел от 0 до 255. для этого из восьмибитовой выборки цифрового «белого» шума брался один младший разряд. Из полученных n младших разрядов формировалось n-битное значение случайной величины. Получено распределение случайных чисел сформированных из младших разрядов 8-ми разрядных выборок оцифрованного «белого» шума.

Для получения более равномерного распределения случайных величин был разработан специальный алгоритм. Суть алгоритма: из восьмибитовой выборки оцифрованного «белого» шума берётся один младший разряд. Полученные n младшие разряды суммируются по модулю 2. Из вычисленных k значений формировалось k-битное значение случайной величины. По полученным графикам можно судить о степени равномерности распределения случайных чисел. Стоит отметить, что данный алгоритм заметно улучшает распределение, но при этом снижает скорость генерирования последовательности случайных чисел.

Разработанный ГСЧ планируется использовать при создании синтезаторов речеподобных сигналов для систем защиты речевой информации.

АНАЛИЗ КРИТЕРИЕВ ДЕТЕКТИРОВАНИЯ РЕЧИ

ДМ.А. БОРИСЕВИЧ, Г.В. ДАВЫДОВ

Детектор речи предназначен для разделения речи и не речевых сигналов (например, звуковых вызовов факсов, модемов и телефонов, музыки, атмосферных звуковых помех, шума транспорта, длительных пауз в речевых сообщениях и других акустических сигналов, не являющихся речевыми). Детектор речи является необходимым устройством для многих современных устройств телекоммуникаций и средств защиты информации для отделения речи от пауз и сжатия сигналов путём удаления не речевых участков, удаления окружающих шумов во время пауз

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