Об одном способе реализации скремблера речевого сигнала

О.Х. Расулов (ГУП «UNICON.UZ»)

В статье рассмотрен способ реализации частотного скремблера речевого сигнала на примере построения математической модели.

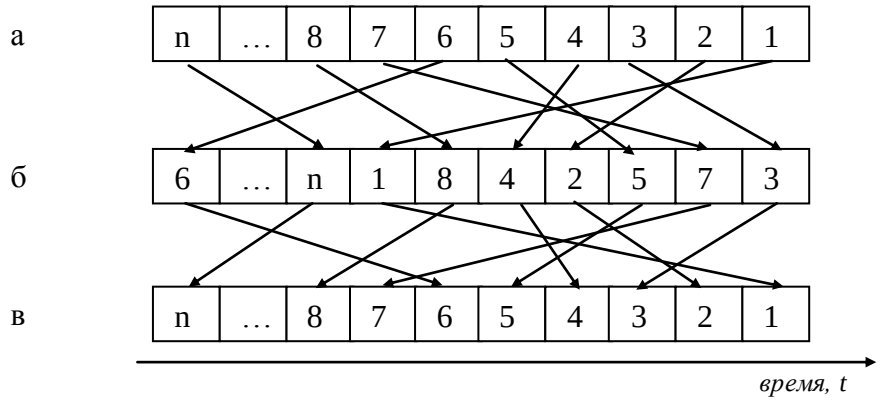
Ушбу мақолада товуш сигнали частотавий сркемблерини математик моделини қуриш мисолида ишлаб чиқиш усули кўриб чикилган.

In this article method of frequency scrambler of speech signal implementation on base of example of mathematical model building is considered.

Скремблеры речевых сигналов применяются в системах связи, к которым предъявляются требования по скрытию истинного содержимого речевого сигнала при его передаче по линиям связи. Основной принцип работы таких устройств основан на перемешивающем преобразовании (перестановке) отсчетов сигнала при передаче и восстановления (обратной перестановке) этих отсчетов на приеме. Результатом таких преобразований является неразборчивость речевого сигнала при его прослушивании в линии передачи. С криптографической точки зрения, правило перестановки является ключом, известным только пользователям системы.

По способу преобразования речевого сигнала существующие скремблеры можно разделить на три основных типа.

А. Скремблеры с перемешиванием сигнала во временной области – «**временные скремблеры**» (рис. 1).



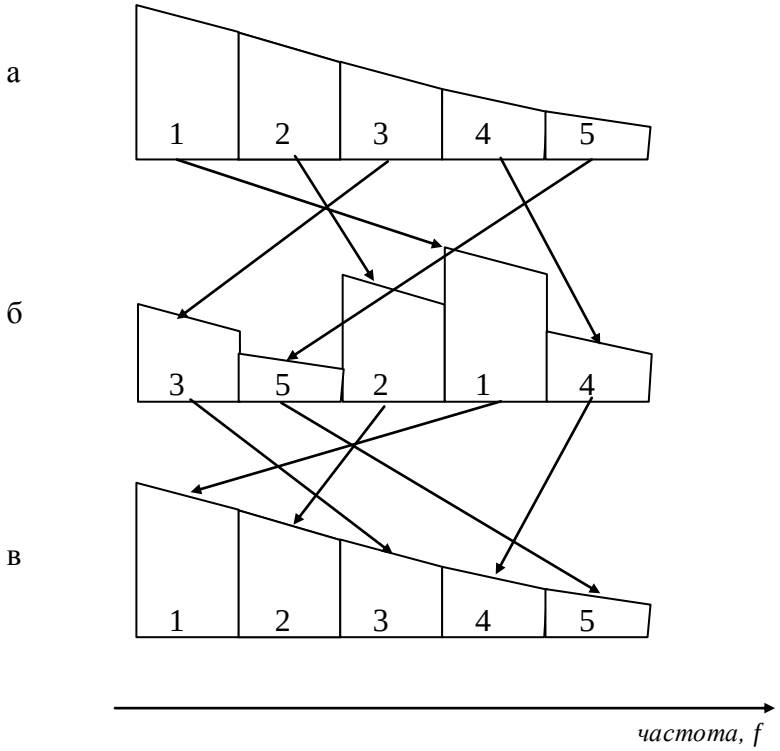
Исходный оцифрованный сигнал (а), сигнал после преобразования (б), сигнал после обратного преобразования (в), n – количество временных отсчетов в буфере (размер буфера). Цифрами обозначены номера временных отсчетов в порядке их поступления от АЦП/передачи в ЦАП.

Рис. 1. Принцип преобразования сигнала временного скремблера.

В общем случае в таких скремблерах поступающие от аналого-цифрового преобразователя отсчеты оцифрованного сигнала накапливаются в буфере (рисунок 1а), после чего отсчеты перемешиваются между собой по заранее определенному правилу (рисунок 1б) и в таком виде передаются в линию связи.

На приемной стороне отсчеты накапливаются в таком же буфере и над ними выполняется обратное преобразование – восстановление речевого сигнала (рисунок 1в).

В. Скремблеры с перемешиванием сигнала в частотной области – «**частотные скремблеры**» (рис. 2).



Для примера спектр речевого сигнала разбит на пять полос. Исходный спектр (а), спектр после преобразования (б), спектр после обратного преобразования (в).

Рис. 2. Принцип преобразования сигнала частотного скремблера

В общем случае в таких скремблерах частотный спектр речевого сигнала делится на некоторое количество частотных полос (рисунок 2а) и производится их перемешивание по известному правилу (рисунок 2б), по аналогии с перемешиванием временных отсчетов во временном скремблере. На приемной стороне выполняется восстановление частотного спектра (рисунок 2в). В некоторых реализациях частотных скремблеров каждая (или некоторые) из полос помимо перестановки подвергаются инверсии – расстановке частот полосы в обратном порядке.

В. Скремблеры с перемешиванием сигнала как во временной, так и в частотной области – комбинированные «**частотно-временные скремблеры**».

В общем случае в таких скремблерах считываются частотные спектры речевого сигнала за несколько временных интервалов. В результате формируется единый кадр из частотных полос, которые затем в пределах этого кадра подвергаются перестановке между собой по известному правилу.

Разбиение частотного спектра речевого сигнала на полосы в частотных и частотно-временных скремблерах как правило осуществляется с использованием быстрого преобразования Фурье (БПФ) и обратного БПФ (ОБПФ) (рис. 3).

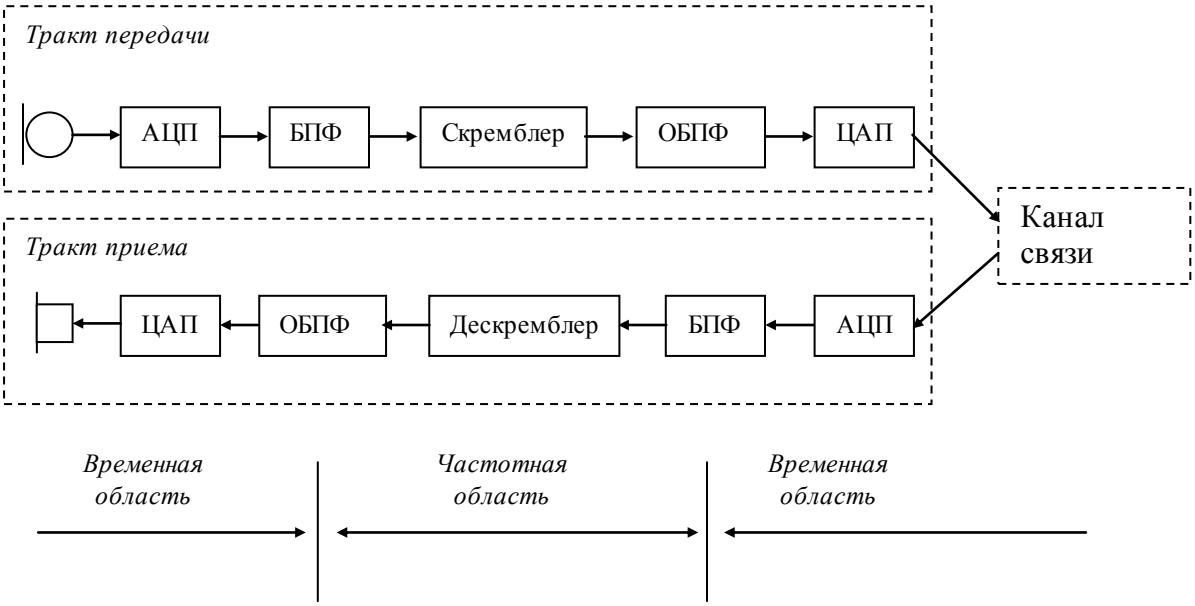


Рис. 3. Обобщенная структура скремблеров с перестановкой частотных полос.

Основой БПФ и ОБПФ является прямое и обратное дискретные преобразования Фурье соответственно:

$$X_k = \sum_{j=0}^{N-1} x_j e^{-i\frac{2\pi kj}{N}}$$ - прямое дискретное преобразование Фурье (1)

$$x_j = \frac{1}{N}\sum_{k=0}^{N-1} X_k e^{i\frac{2\pi kj}{N}}$$ - обратное дискретное преобразование Фурье (2)

где N – порядок преобразования Фурье (количество обрабатываемых отсчетов), X_k – k-й отсчет сигнала в частотной области (k=1…N-1), x_j – j-й отсчет сигнала во временной области (j=1…N-1), i – мнимая единица.

Основным недостатком использования БПФ/ОБПФ является тот факт, что в этих преобразованиях применяются вычисления с комплексными числами, из-за чего фактически каждое сложение состоит из двух операций, а умножение - из шести, что заметно увеличивает итоговые вычислительные затраты, вводит избыточность в вычислительную систему скремблера, а также требует дополнительную ресурсоемкость при приведении комплексных чисел в вещественные для передачи сигнала в ЦАП (в тракте передачи) и АЦП (в тракте приема) согласно рис. 3.

С целью уменьшения вычислительных затрат при реализации скремблеров использующих частотные перестановки проведены исследования по выброру эффективного способа частотно-временных преобразований сигнала, исключающего вычисления с комплексными числами.

Исследования существующих способов частотно-временных преобразований сигнала показали, что наиболее приемлемым с точки зрения практической реализации в скремблерах является использование дискретного преобразования Хартли (ДПХ) [1]

$$X_k = \sum_{j=0}^{N-1} x_j \left[\cos\frac{2\pi jk}{N} + \sin\frac{2\pi jk}{N}\right]$$ - прямое ДПХ (3)

$$x_j = \frac{1}{N}\sum_{k=0}^{N-1} X_k \left[\cos\frac{2\pi jk}{N} + \sin\frac{2\pi jk}{N} \right]$$ - обратное ДПХ (4)

Дискретные преобразования Фурье и Хартли связаны между собой соотношениями:

$H(f)$=Re[$F(f)$] - Im[$F(f)$] (5)

$F(f)$=[$H(f)$ + $H(-f)$]/2 + i [$H(f)$ - $H(-f)$]/2 (6)

где $H(f)$ – функция преобразования Хартли (3), $F(f)$ – функция преобразования Фурье (1), Re – вещественная часть комплексного числа, Im – мнимая часть комплексного числа.

Как видно из (3), ДПХ оперирует только вещественными числами. Существуют способы ускорения (оптимизации) вычислений ДПХ – быстрое преобразование Хартли (БПХ) [2].

В ходе исследований в среде MATLAB создана модель частотно-временного скремблера. В основе модели лежит структура скремблера, показанная на рисунке 3, в которой вместо модулей БПФ/ОБПФ использованы модули ДПХ (рис. 4).

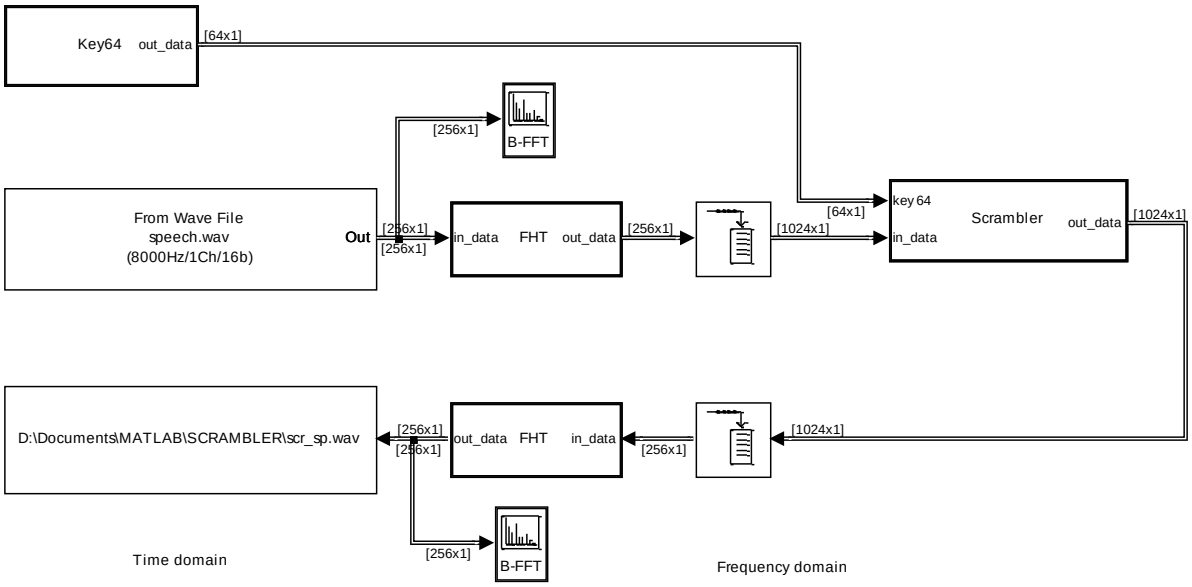


Рис. 4. Модель скремблера с использованием преобразавания Хартли (фрагмент тракта передачи).

Оценка качества восстановленного речевого сигнала (на выходе тракта приема) показала идентичные результаты при использовании ДПФ и ДПХ для частотно-временных преобразований.

Выводы:

Выбранный способ частотно-временного преобразования позволяет существенно снизить трудоемкость арифметических операций. По результатам моделирования в среде MATLAB, способ является более эффективным по сравнению с использованием преобразований Фурье и может быть применен при реализации частотных и частотно-временных скремблеров речевого сигнала.

Список использованной литературы:

1. Брейсуэлл Р. Преобразование Хартли. М.:Мир 1990

2. Сергеев В. В., Усачев А. В. Новый алгоритм быстрого преобразования Хартли. Компьютерная оптика. № 7 1990.