

УДК 65.012.8: 621.395

В.И. Корниенко, А.В. Герасина

ГВУЗ «Национальный горный университет», Днепропетровск

АДАПТИВНАЯ СПЕКТРАЛЬНАЯ ФИЛЬТРАЦИЯ В СИСТЕМЕ КОНФИДЕНЦИАЛЬНОЙ ТЕЛЕФОННОЙ СВЯЗИ С ЗАШУМЛЕНИЕМ КАНАЛОВ

Исследованы характеристики алгоритмов адаптивной фильтрации сигналов в спектральной (частотной и время-частотной) области. Путем моделирования оценена эффективность использования спектральных адаптивных фильтров в системе конфиденциальной телефонной связи с зашумлением каналов.

Ключевые слова: конфиденциальная связь, зашумление каналов, адаптивная фильтрация, спектральный фильтр.

Введение

Проблема защиты конфиденциальной информации является одной из важных задач при передаче речи по телефонным каналам связи.

Для защиты информации в проводных каналах связи используется маскировка передаваемой информации с помощью зашумления линии передачи в рабочем диапазоне частот и последующей обработки информации для получателя путем вычитания шумового сигнала из смешанного сигнала от передающего абонента и генератора шума [1].

Постановка задачи. В системе с зашумлением каналов защита информации заключается в преобразовании (перед вычитанием опорного и смешанного сигналов) из временной области в спектральную (частотную или время-частотную – вейвлет) и обратное преобразование обработанного сигнала из спектральной области во временную [1]. Это приводит к снижению объема вычислений за счет возможности использования алгоритмов быстрого преобразования Фурье (БПФ) [2] или вейвлет-преобразования (БВВП) [3]. Для реализации такого вычитания используются адаптивные фильтры (АФ). В них процесс адаптации включает оценивание искомого выхода фильтра и его коэффициентов для достижения требуемой цели.

Наиболее широко распространенным типом структуры АФ является архитектура с конечной импульсной характеристикой (КИХ). Эти фильтры сходятся нерекурсивно к решению уравнения Винера – Хопфа. АФ с бесконечной импульсной характеристикой оптимально рекурсивно оцениваются с помощью фильтра Калмана. Синтез этих фильтров зависит от ошибки оценивания:

$$e(n) = x(n) - \hat{x}(n),$$

где $x(n)$ – случайная величина, которую необходимо оценить, $\hat{x}(n)$ – оценка $x(n)$, n – текущий такт.

При этом нерекурсивная оценка $\hat{x}(n)$ определяется с помощью конечного линейного полинома входного сигнала $y(n)$ [2]:

$$\hat{x}(n) = \sum_{k=0}^{N-1} y(n-k) \cdot h_k,$$

где h_k – веса нерекурсивного фильтра КИХ-типа, а N – размерность полинома. Это винеровская оценка конечной выборки (блока) данных. Однако, если иметь дело с бесконечным временным рядом, то предпочтительной является рекурсивная (или калмановская) оценка, которая основана на авторегрессионной модели процесса генерации сигнала.

Цель статьи: исследование характеристик алгоритмов адаптивной фильтрации в спектральной области и оценка эффективности их использования в системе конфиденциальной телефонной связи с зашумлением каналов.

Система конфиденциальной связи

Система конфиденциальной телефонной связи в проводных каналах [1] включает (рис. 1) генератор шума (ГШ) в рабочем диапазоне частот, цифровой спектральный адаптивный фильтр (САФ), коммутирующее устройство (КУ), аналого-цифровой преобразователь (АЦП), сумматор (Σ) и цифро-аналоговый преобразователь (ЦАП).

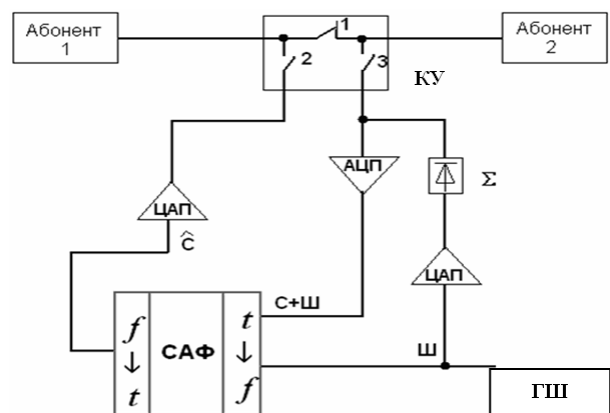


Рис. 1. Структура системы конфиденциальной связи с зашумлением канала

В отсутствие передачи конфиденциальной информации КУ напрямую соединяет абонентов, а при

ее передаче в КУ разрывается прямая связь 1 между линиями и абоненты слышат шумовые помехи от ГШ. Цифровой САФ обрабатывает смесь сигнала от абонента 2 и ГШ и сигнал ГШ, в результате выдает принимающему абоненту 1 очищенную от шума информацию.

Алгоритм обработки состоит в:

а) преобразовании данных из временной в спектральную область от ГШ (опорного канала)

$$X(n, f) - |x(n, f_1), x(n, f_2), \dots, x(n, f_N)| = \text{TF}|X(n)| = \\ = F|x(n), x(n-1), \dots, x(n-N+1)|$$

и телефонной линии (основного канала)

$$Z(n, f) = \text{TF}|Z(n)| = |z(n, f_1), z(n, f_2), \dots, z(n, f_N)|;$$

б) свертке (умножении) для блока данных опорного канала в спектральной области с коэффициентами фильтра:

$$Y(n, f) = H^*(n, f) \bullet X(n, f_i)$$

или $y(n, f_i) = h^*(n, f_i) \bullet x(n, f_i), i = 1, 2, \dots, N$;

в) компенсации (вычитании) блока данных опорного канала из блока данных основного канала:

$$E(n, f) - |e(n, f_1), e(n, f_2), \dots, e(n, f_N)| = Z(n, f) - Y(n, f)$$

или $e(n, f_i) = z(n, f_i) - y(n, f_i)$;

г) настройке коэффициентов АФ:

$$H(n+1, f) = H(n, f) + k \bullet E(n, f) \bullet X(n, f)$$

или $h(n+1, f_i) = h(n, f_i) + k \bullet e(n, f_i) \bullet x(n, f_i)$;

д) преобразовании данных из спектральной области во временную:

$$|e(n), e(n-1), \dots, e(n-N+1)| = \text{FT}|e(n, f_1), e(n, f_2), \dots, e(n, f_N)| = \\ = \text{FT}|E(n, f)|,$$

где: TF, FT – операции быстрого прямого и обратного преобразования, например, Фурье (БПФ) или вейвлет (БВВП); * – комплексное сопряжение; $H(n, f) = |h(n, f_1), h(n, f_2), \dots, h(n, f_N)|$ – вектор коэффициентов АФ размерностью N ; f – спектральный отсчет.

Настройка коэффициентов АФ закончится когда поправки в среднем станут равными нулю:

$$M\{e(n, f) \bullet x(n, f)\} = M\{z(n, f) - h(n, f) \bullet x(n, f)\} = 0,$$

где $M\{\}$ – усреднение во времени.

Это будет достигнуто когда весовые коэффициенты равны коэффициентам корреляции между спектральными компонентами основного и опорного сигналов:

$$h(n, f) = M\{z(n, f) \bullet x(n, f)\} / M\{x(n, f) \bullet x(n, f)\}.$$

Алгоритмы адаптивной фильтрации в спектральной области

Преимущества реализации АФ в спектральной области (в отличие временной области) заключается в уменьшении числа вычислений, что достигается путем замены свертки входного сигнала с импульсной пере-

ходной характеристикой АФ на произведения трансформант (результатов преобразования Фурье или вейвлет преобразования). При этом также улучшаются свойства сходимости адаптивного процесса.

Рассмотрим два типа АФ с обработкой сигналов в спектральной области [2].

Блочный МНК-АФ (БМНК) является по существу идентичной реализацией в спектральной области блочного алгоритма МНК с обработкой сигналов во временной области. В этом алгоритме данные группируются в блоки по N выборок, а весовые коэффициенты фильтра поддерживаются постоянными в пределах каждого блока. Во время обработки k -го блока используют следующие уравнения для АФ:

$$h(k+1) = h(k) + \mu \sum_{i=0}^{N-1} e(kN+i)x(kN+i) = \\ = h(k) + \mu \nabla(k);$$

$$y(kN+i) = h^T(k) \cdot x(kN+i), \quad i = 0, 1, \dots, N-1,$$

где μ – коэффициент; ∇ – знак градиента; $h(k)$ – вектор весовых коэффициентов фильтра во время обработки k -го блока:

$$h^T(k) = [h_0(k), h_1(k), \dots, h_{N-1}(k)],$$

а $x^T(n) = [x(n), x(n-1), \dots, x(n-N+1)]$.

В БМНК-фильтре для каждого блока размерностью N требуется пять $2N$ -мерных БПФ (или БВВП) и два комплексных умножения для $2N$ чисел. Чтобы получить N выборок выходного сигнала с помощью обычного МНК-АФ, требуется $2N^2$ вещественных умножений.

Результаты снижения объемов вычислений при использовании алгоритма БМНК (по сравнению с МНК) при использовании БПФ и БВВП приведены в табл. 1.

Таблица 1

Снижение объемов вычислений для БМНК-фильтра

N	32	64	256	1024
$\frac{\text{БМНК}}{\text{МНК}}$ (БПФ)	0,91	0,53	0,17	0,053
$\frac{\text{БМНК}}{\text{МНК}}$ (БВВП)	0,23	0,11	0,028	0,0071

При обработке по алгоритму БМНК каждого блока данных два БПФ (БВВП) необходимы для наложения ограничений во временной области, чтобы вторая половина весовых коэффициентов равнялась нулю. Это требуется для реализации строго линейной свертки входного сигнала фильтра и импульсной характеристики. В БМНК-АФ, выполняющем обработку сигналов в спектральной области без наложения ограничений (БОБМНК), это требование снимается, что дает более простой АФ (табл. 2).

Таблиця 2

Снижение объемов вычислений
для БОБМНК-фильтра

N	32	64	256	1024
$\frac{\text{БОБМНК}}{\text{МНК}}$ (БПФ)	0,59	0,34	0,11	0,033
$\frac{\text{БОБМНК}}{\text{МНК}}$ (БВВП)	0,14	0,077	0,016	0,0051

Моделирование спектрального адаптивного фильтра

Моделирование выполнялось в среде Matlab с помощью пакета программ Filter Designer.

В качестве тестового РС использовалась сумма гармоник с частотами 400, 1000 и 3000 Гц длительностью $T=22,5$ мс (период стационарности речевого сигнала). Соответственно, количество отсчетов сигнала с частотой дискретизации $F_D=8$ кГц составило $N=T \cdot F_D=180$. Для частотной области количество отсчетов принято $N_q=1024$, тогда частотное разрешение спектра составляет $\Delta F = F_D / N_q = 7,81$ Гц.

Программа моделирования включала определение значения величины средней ошибки ($\bar{\varepsilon}$) между тестовым сигналом и его оценкой на выходе САФ для различных значений порядка фильтра $M=\{64, 128, 512\}$ в условиях вариации уровня шумов $n_{\text{var}}=\{0, 0,05, 0,15, 0,5\}$.

В результате моделирования были получены значения средней ошибки, приведенные на рис. 2.

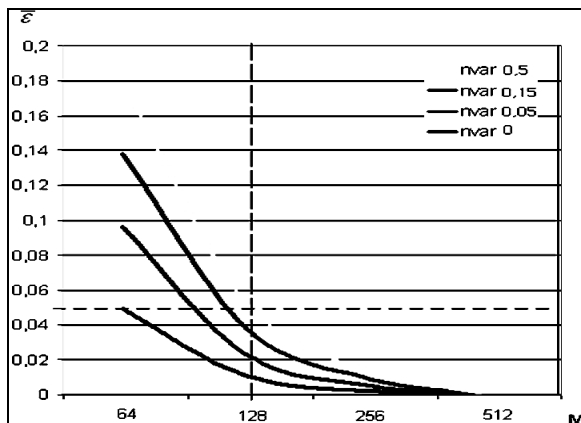
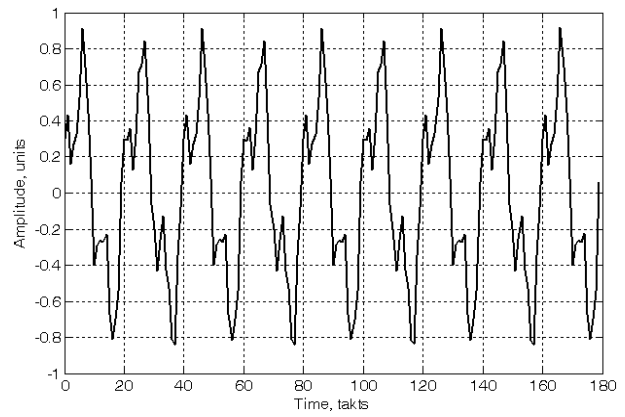


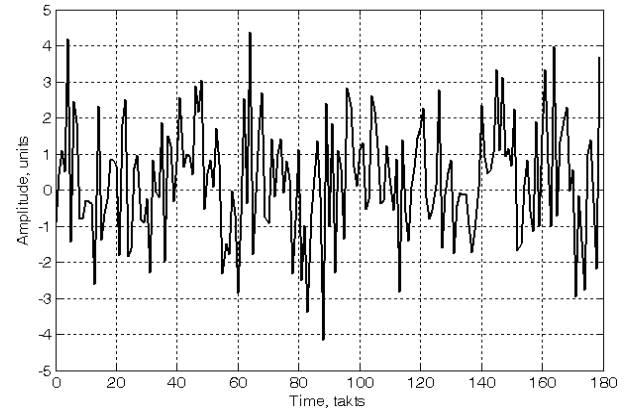
Рис. 2. Значения средней ошибки САФ

Если задаться допустимым значением средней ошибки восстановления РС $\bar{\varepsilon}_{\text{доп}} \leq 0,05$ (5%), то для уровня шума $n_{\text{var}} \leq 0,5$ согласно графику (рис. 2) порядок САФ должен быть $M \leq 128$, а при $\bar{\varepsilon}_{\text{доп}} \leq 0,02$ (2%) – $M \leq 213$.

Тестовый и зашумленный (при $n_{\text{var}}=0,5$) сигналы приведены на рис. 3, а их спектры и спектр восстановленного с помощью САФ РС – на рис. 4.

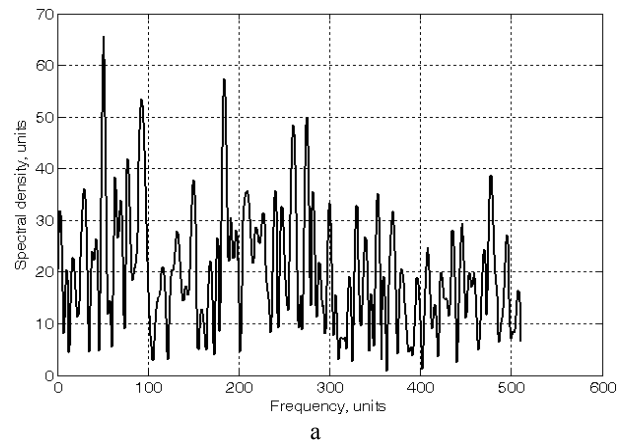


а

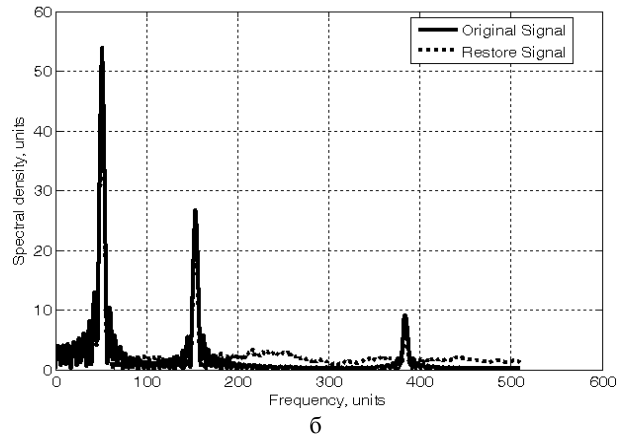


б

Рис. 3. Тестовый (а) и зашумленный (б) сигналы



а



б

Рис. 4. Спектр зашумленного (а), тестового и восстановленного (б) сигналов

Выводы

Исследования алгоритмов адаптивной фильтрации в спектральной области показало, что использование алгоритмов быстрого преобразования Фурье (или вейвлет преобразования) позволяют снизить объем вычислений не менее, чем в 20 (140) раз для блоков данных размером в 1024 отсчета.

В результате моделирования установлено, что для восстановления зашумленного речевого сигнала с точностью не хуже 5 % порядок адаптивного спектрального фильтра должен быть не менее 128.

Дальнейшие исследования должны быть направлены на техническую реализацию полученных результатов.

Список литературы

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К.: Юниор, 2003. – 496 с.
2. Адаптивные фильтры: Пер. с англ. / Под ред. К.Ф.Н. Коуэна и П.М. Гранта. – М.: Мир, 1988. – 392 с.
3. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в Matlab. / Н.К. Смоленцев – М.: ДМК Пресс, 2005. – 304 с.

Поступила в редколлегию 20.12.2012

Рецензент: д-р техн. наук, проф. М.А. Алексеев, ГВУЗ «Национальный горный университет», Днепропетровск.

АДАПТИВНА СПЕКТРАЛЬНА ФІЛЬТРАЦІЯ В СИСТЕМІ КОНФІДЕНЦІЙНОГО ТЕЛЕФОННОГО ЗВ'ЯЗКУ ІЗ ЗАШУМЛЕННЯМ КАНАЛІВ

В.І. Корнієнко, О.В. Герасіна

Досліджені характеристики алгоритмів адаптивної фільтрації сигналів в спектральній (частотній і час-частотній) області. Шляхом моделювання оцінена ефективність використання спектральних адаптивних фільтрів в системі конфіденційного телефонного зв'язку із зашумленням каналів.

Ключові слова: конфіденційний зв'язок, зашумлення каналів, адаптивна фільтрація, спектральний фільтр.

ADAPTIVE SPECTRAL FILTRATION IN CONFIDENTIAL TELEPHONE COMMUNICATION NETWORK FROM THE CHANNELS WITH NOISE

V.I. Korniyenko, A.V. Gerasina

Descriptions of algorithms of adaptive filtration of signals are investigational in a spectral (frequency and time-frequency) region. By a simulation efficiency of the use of spectral adaptive filters is appraised in a confidential telephone communication network from the channels with noise.

Keywords: confidential connection, channels with noise, adaptive filtration, spectral filter.