ISSN 0868–5886 НАУЧНОЕ ПРИБОРОСТРОЕНИЕ, 2003, том 13, № 3, с. 84–94

ОРИГИНАЛЬНЫЕ СТАТЬИ

УДК 621.391.266.037.372

© А. В. Меркушева

СКРЫТАЯ ПЕРЕДАЧА ИНФОРМАЦИОННЫХ СИГНАЛОВ НА ОСНОВЕ МОДИФИЦИРОВАННОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Среди современных информационно-измерительных систем имеется класс распределенных систем, которые обеспечивают сбор, обработку, детектирование и идентификацию определенных ключевых признаков сигнала для селективного распределения информации по узлам сети ЭВМ. Системы этого типа являются носителями потоков сообщений большой интенсивности с высокой значимостью (зависящей от контекста решаемых системой задач). Одновременно они достаточно уязвимы с точки зрения возможного несанкционированного доступа к сообщениям в каналах связи элементов сети (ЭВМ, кабельных прокладок, концентраторов). Наиболее существенна проблема конфиденциальности в информационных системах с речевыми сигналами. В статье рассмотрен метод обеспечения скрытой передачи речевых сигналов в распределенных информационных системах, основанный на использовании скремблирования с двойным преобразованием сигнала.

ПОСТАНОВКА ЗАДАЧИ. ТРАДИЦИОННЫЕ РЕШЕНИЯ

Поскольку в распределенных системах, как правило, необходимо сохранение конфиденциальности информации, а передача ее между узлами системы и хранение в базах данных в открытом виде нарушает требование конфиденциальности, то в этом случае целесообразно применять скремблирование речевого сигнала. Такие системы работают в режиме реального времени, поэтому закрытие информации осуществляется алгоритмом, который не только дает низкую остаточную разборчивость, большое количество ключей, иммунитет к криптоанализу и сохранение качества речи при умеренной сложности алгоритма, но и выполняется достаточно быстро и вносит минимальные задержки при записи и воспроизведении речевого сигнала.

Первый уровень скремблирования (тактический), являющийся защитой от технически невооруженного прослушивания, использует частотную инверсию и частотную инверсию с тональным маскированием. При этом требование минимальности искажений ограничивает число частотных полос и ведет к снижению количества ключей и к большей остаточной разборчивости. Первая из пяти полос, например, содержит около 40 % энергии сигнала и первую форманту, что после тренировки позволяет понимать скремблированную речь [1].

Второй уровень использует частотное скремблирование с методом БПФ, временно́е и частотно-временно́е скремблирование [2]. Частотное скремблирование с методом БПФ является обобщением метода инверсии, при котором в канал передается временна́я форма $\tilde{s}$ скремблированного сигнала s:

$$\tilde{s} = F_n^{-1} P_n F_n s,$$

где F_n — n-точечные преобразования Фурье, P_n — матрица перестановок.

Метод связан со значительной вычислительной нагрузкой и необходимостью подбора матриц P_n для обеспечения вещественности скремблированного сигнала $\tilde{s}$. Кроме того, ориентируясь на известную форму спектра речевого сигнала, аналитик имеет возможность с помощью критерия восстановления типичной формы частотного спектра сигнала речи подобрать матрицу перестановок $\hat{P}$ и восстановить оценку $\hat{s}$ с помощью процедуры

$$\begin{aligned} &\tilde{s} \to F \cdot \tilde{s} \to \hat{P} \cdot F \cdot \tilde{s} \to F^{-1} \cdot \hat{P} \cdot F \cdot \tilde{s} \cong \hat{s}, \\ &\hat{P} \cong P^{-1}, \quad \hat{s} \cong s, \end{aligned} \qquad (2)$$

где F — оператор БПФ и F^{-1} — обратная операция, т. е. БПФ$^{-1}$.

Метод временно́го скремблирования обеспечивает несколько бо́льшую безопасность, чем метод частотного скремблирования, но включает перестановку временны́х отсчетов на фрейме сигнала и приводит к высокой задержке.

Модификации с обращением временны́х сегментов, со скремблированием временны́х отсчетов или временны́х элементов, содержащих несколько отсчетов сигнала, также не вполне удовлетворительны. Короткие сегменты (40–100 мс) приводят к большой остаточной разборчивости, а длинные

сегменты (300–600 мс) — к значительным задержкам. Кроме того, метод обращения временны́х сегментов не скрывает гласные фонемы и дает искажения на границах сегментов.

Трудности метода скремблирования временны́х элементов, основанного на перестановке сегментов внутри фрейма речевого сигнала, связаны с некоторой противоречивостью требований. Лучшую защиту дают короткие сегменты, но это ведет к искажениям сигнала на границах сегментов и расширению частотной полосы сигнала. Компромиссная длительность 16–60 мс позволяет сохранить определенный баланс "качество—безопасность", но дает задержку при передаче такую, как у спутниковой связи.

Количество сегментов 8, удобное для аппаратной реализации, дает число ключей всего 40320 (8!), которое еще снижается при отборе перестановок по shift-фактору. Хорошими являются по разным оценкам не более 10 % общего количества перестановок [2, 3]. Кроме того, скремблирование медленно меняющегося сигнала дает невысокий уровень безопасности. В частности, если фрейм равен длительности фонемы, то скремблирование лишь ухудшает качество фонемы, сохраняя ее распознаваемость.

Метод частотно-временно́го скремблирования включает в качестве фаз этап частотного скремблирования и этап перестановок временных отсче́тов и некоторым образом объединяет недостатки, свойственные каждому из этапов.

Совершенствование методов скремблирования возможно путем введения новых видов преобразования сигнала, существенно снижающих остаточную разборчивость, значительно повышающих количество ключей и обладающих быстрым алгоритмом реализации. Предложенный в [4], [5] метод, отвечающий таким требованиям, основан на двухфазной процедуре, которая реализует преобразование вейвлет-отображения речевого сигнала Н-эквивалентными матрицами.

Анализ время-частотных и вейвлет-преобразований нестационарных сигналов в информационно-измерительных системах (ИИС) показал, что обработка в вейвлет-области является эффективным методом идентификации свойств сигнала и адаптивной фильтрации с подстройкой порога дискриминации в соответствии с изменением характеристик сопутствующего шума. Метод вейвлет-преобразования применен при разработке алгоритма идентификации типа интервала речь / пауза (шум) и вейвлет-фильтрации речевого сигнала [6, 7, 8].

Здесь мы решаем задачу применения вейвлет-преобразования для скрытной передачи речевой информации.

ОБЩИЕ ХАРАКТЕРИСТИКИ ПРИМЕНЕНИЯ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ ДЛЯ ЦЕЛЕЙ СКРЕМБЛИРОВАНИЯ

Применение вейвлет-преобразования в алгоритме скремблирования позволяет использовать такие его важные свойства, как наличие быстрых алгоритмов преобразования и полное восстановление сигнала, включая фазовые соотношения частотных компонент.

Использование Н-эквивалентных матриц позволяет добиться высокой безопасности скремблированного сигнала, поскольку эта фаза преобразования на вейвлет-отображении сигнала реализует превращение каждой компоненты вектора вейвлет-коэффициентов в функцию от всех остальных компонент. Таким образом, вейвлет-образ полностью меняет свою структуру и, следовательно, структуру время-частотного портрета речевого сигнала. Это изменение происходит так, как если бы каждый элемент живописного полотна заменили взвешенной суммой всех остальных его элементов. При этом мощность множества Н-эквивалентных матриц настолько велика, что по количеству ключей метод существенно превосходит традиционные методы скремблирования.

Вейвлет-преобразованием (ВП) преодолевается недостаток частотных скремблеров, имеющих равномерное разбиение частотной полосы сигнала на субполосы. ВП имеет диадное разбиение частотной полосы и постоянное относительное разрешение во всем диапазоне частот сигнала. Это позволяет уменьшить ширину субполос в низкочастотной области и получить более равномерное распределение энергии сигнала по субполосам.

Для выполнения вейвлет-преобразования скремблер включает 4 каскада блоков квадратурно-зеркальных фильтров, на выходе которых получаются двоично-децимированные коэффициенты вейвлет-преобразования речевого сигнала. Использование коротких вейвлет-фильтров позволяет выполнять преобразование в реальном времени. Коэффициенты фильтра определяются видом используемого вейвлет-базиса. Выбор вида базиса и порядок его изменения (синхронизировано с приемником) является дополнительной степенью свободы при формировании ключа скремблирования.

Блок квадратурно-зеркальных фильтров состоит из низкочастотного фильтра $\{h_i\}_{i=1,\ 2...}$, выход которого дает аппроксимацию сигнала на текущем масштабе, и полосового фильтра $\{g_i\}_{i=1,\ 2...}$, выход которого дает детали как разницу аппроксимации на двух соседних уровнях масштаба.

Коэффициенты импульсной характеристики фильтра низкой частоты $\{h_i\}_{i=1,\ 2,...}$ соответствуют

уравнению связи между масштабирующими функциями на двух соседних уровнях разложения [9]

$$\varphi(t) = \sqrt{2} \cdot \sum_n h_n . \varphi(2t - n). \quad (3)$$

Коэффициенты импульсной характеристики фильтра высокой частоты $\{g_i\}_{i=1,\,2,\ldots}$ соответствуют уравнению связи между масштабирующей и вейвлет-функциями на двух соседних уровнях разложения

$$\psi(t) = \sqrt{2} \cdot \sum_n g_n . \varphi(2t - n), \quad (4)$$

где $\varphi(t)$, $\psi(t)$ — масштабирующая и вейвлет-функция на текущем уровне разложения; $\varphi(2t-n)$, $\psi(2t-n)$ — масштабирующая и вейвлет-функция на предыдущем уровне разложения.

Коэффициенты фильтров $\{g_i\}_{i=1,\,2,\ldots}$ и $\{h_i\}_{i=1,\,2,\ldots}$ связаны соотношением

$$g_n = (-1)^n \cdot h_{-n+2t+1}. \quad (5)$$

Для базисных функций вейвлет-преобразования с компактной областью определения фильтры $\{h_i\}_{i=1,\,2,\ldots}$ и $\{g_i\}_{i=1,\,2,\ldots}$ систематизированы в [10] и доступны в программных средствах.

Блок анализа, реализуемый каскадом квадратурно-зеркальных фильтров (КЗФ), осуществляет преобразование коэффициентов аппроксимации масштаба (j–1)-уровня к j-му уровню согласно соотношению

$$c_k^j = \sum_n h_{n-2k} \cdot c_n^{j-1}, \quad (6)$$

где c_k^j — коэффициенты аппроксимации сигнала на j-ом уровне.

Этот же блок КЗФ на основе полосового фильтра $\{g_i\}_{i=1,\,2,\ldots}$ определяет коэффициенты $\{d_k^j\}_{k=1,2,\ldots}$ разложения разности аппроксимаций на уровнях j–1 и j согласно соотношению

$$d_k^j = \sum_n g_{n-2k} \cdot d_n^{j-1}, \quad (7)$$

где d_k^j — коэффициент деталей, дающий отличие аппроксимации на соседних уровнях масштаба. Аппроксимацией на нулевом уровне масштаба являются отсчеты сигнала.

Таким образом, в результате вейвлет-преобразования получается экономное представление сигнала на J уровнях разложения. Коэффициенты вейвлет-разложения подвергаются скремблированию с использованием Н-эквивалентных матриц **S**, которые получаются путем перестановок строк и столбцов в матрицах Адамара

$$\mathbf{S} = \frac{1}{N^{1/2}} \mathbf{P}_1 \cdot \mathbf{H} \cdot \mathbf{P}_2, \quad (8)$$

где $\mathbf{P}_1$ — матрица перестановки строк, $\mathbf{P}_2$ — матрица перестановки столбцов, N — порядок матрицы Адамара **H**.

ОПИСАНИЕ ПРОЦЕДУРЫ СКРЕМБЛИРОВАНИЯ

Процедура скремблирования включает получение матрицы Адамара **H** требуемой размерности; генерацию матриц $\mathbf{P}_1$ и $\mathbf{P}_2$; умножение некоторых строк и некоторых столбцов на –1; получение Н-эквивалентной матрицы для скремблирования фрейма сигнала.

Матрицы Адамара $\mathbf{H}_N$ (порядок $N = 2$, $N = 4n$ или $N = 2^n$) при дополнительной нормировке $\frac{1}{N^{1/2}}\mathbf{H}_N$ удовлетворяют свойству ортогональности

$$\mathbf{H}^{-1} = (1/N) \cdot \mathbf{H}^T. \quad (9)$$

Получение матриц Адамара порядка более 4 реализуется с помощью алгоритма Сильвестера [11], согласно которому Н-матрица размерности $N_1 \times N_2$ может быть получена как кронекерово произведение матриц размерностей N_1 и N_2:

$$\mathbf{H}_{N_1 \times N_2} = \mathbf{H}_{N_1} \otimes \mathbf{H}_{N_2}, \quad (10)$$

где $\otimes$ — символ кронекерова произведения матриц, которое выражается правилом

$$\mathbf{H}_{N_1} \otimes \mathbf{H}_{N_2} = \begin{bmatrix} [\mathbf{H}_{N_1}]_{11} \cdot \mathbf{H}_{N_2} & [\mathbf{H}_{N_1}]_{12} \cdot \mathbf{H}_{N_2} & \cdots & [\mathbf{H}_{N_1}]_{1N_1} \cdot \mathbf{H}_{N_2} \\ [\mathbf{H}_{N_1}]_{21} \cdot \mathbf{H}_{N_2} & [\mathbf{H}_{N_1}]_{22} \cdot \mathbf{H}_{N_2} & \cdots & [\mathbf{H}_{N_1}]_{2N_1} \cdot \mathbf{H}_{N_2} \\ \cdots & \cdots & \cdots & \cdots \\ [\mathbf{H}_{N_1}]_{N_1 1} \cdot \mathbf{H}_{N_2} & [\mathbf{H}_{N_1}]_{N_1 2} \cdot \mathbf{H}_{N_2} & \cdots & [\mathbf{H}_{N_1}]_{N_1 N_1} \cdot \mathbf{H}_{N_2} \end{bmatrix}, \quad (11)$$

где $\left[\mathbf{H}_{N_1}\right]_{ij}$ — элемент матрицы $\mathbf{H}_{N_1}$, стоящий на пересечении i-го столбца и j-й строки; N_1 — размерность матрицы H_{N_1}; $\left[H_{N_1}\right]_{ij} \cdot \mathbf{H}_{N_2}$ — результат умножения матрицы $\mathbf{H}_{N2}$ на элемент $\left[\mathbf{H}_{N_1}\right]_{ij}$ матрицы.

Таким образом, используя кронекерово произведение, из Н-матрицы второго порядка $\mathbf{H}_2$ можно построить другую Н-матрицу любого порядка 2^n. Для получения матриц Адамара с размерностями типа $N=p^n+1$, где p — простое число, можно использовать схему Палея [12].

СКРЕМБЛИРОВАНИЕ ВЕЙВЛЕТ-КОЭФФИЦИЕНТОВ

Скремблирование выполняется на временно́м сегменте сигнала. Величина сегмента определяет задержку скремблирования, которая должна быть в пределах 10–100 мс. Слишком малая величина сегмента не обеспечивает достаточной безопасности скремблирования. При частоте дискретизации 22.05 кГц сегмент может быть выбран в 256 отсчетов при длине сегмента 11.6 мс.

На сегменте выполняется вейвлет-преобразование, результатом которого является совокупность наборов коэффициентов $\left\{d_k^1\right\}_{k=1,\ldots,128}$, $\left\{d_k^2\right\}_{k=1,\ldots,64}$, $\left\{d_k^3\right\}_{k=1,\ldots,32}$, $\left\{d_k^4\right\}_{k=1,\ldots,16}$, $\left\{c_k^4\right\}_{k=1,\ldots,16}$. Общее количество коэффициентов равно числу отсчетов на сегменте. Над этими коэффициентами выполняется преобразование с использованием матриц Адамара. Можно использовать два варианта скремблирования вейвлет-коэффициентов: с конкатенацией или без конкатенации строк, содержащих вейвлет-коэффициенты в разных пространствах разложения.

Способ скремблирования с конкатенацией строк

Способ предполагает объединение вейвлет-коэффициентов во всех пространствах разложения

$$\left\{u_k\right\}_{k=1,\ldots,256} = \left\{d_k^1\right\}_{k=1,\ldots,128} \cup \left\{d_k^2\right\}_{k=1,\ldots,64} \cup \cup \left\{d_k^3\right\}_{k=1,\ldots,32} \cup \left\{d_k^4\right\}_{k=1,\ldots,16} \cup \left\{c_k^4\right\}_{k=1,\ldots,16}$$

и представление в виде единого вектора

$$\mathbf{u} = \left[d_1^1, d_2^1, \ldots, d_{128}^1, d_1^2, d_2^2, \ldots, d_{64}^2, d_1^3, d_2^3, \ldots, d_{32}^3, \ldots, d_1^4, d_2^4, \ldots, d_{16}^4, \ldots, c_1^4, c_2^4, \ldots, c_{16}^4\right]. \quad (13)$$

При способе с конкатенацией скремблирование выполняется путем преобразования вектора $\mathbf{u}$ с помощью Н-эквивалентной матрицы $\mathbf{S}$. Вектор $\mathbf{v}$ скремблированных коэффициентов на сегменте сигнала определяется соотношением

$$\mathbf{v} = \mathbf{S} \cdot \mathbf{u}. \quad (14)$$

Способ скремблирования без конкатенации строк

Способ предполагает использование нескольких матриц Адамара для скремблирования сегмента сигнала. Число матриц соответствует количеству наборов вейвлет-коэффициентов. При четырехуровневом вейвлет-разложении для скремблирования пяти наборов коэффициентов $\left\{d_k^1\right\}_{k=1,\ldots,128}$, $\left\{d_k^2\right\}_{k=1,\ldots,64}$, $\left\{d_k^3\right\}_{k=1,\ldots,32}$, $\left\{d_k^4\right\}_{k=1,\ldots,16}$, $\left\{c_k^4\right\}_{k=1,\ldots,16}$ предложено использовать пять матриц Адамара соответствующей размерности: $\mathbf{H}_{1(128\times128)}$, $\mathbf{H}_{2(64\times64)}$, $\mathbf{H}_{3(32\times32)}$, $\mathbf{H}_{4(16\times16)}$, $\mathbf{H}_{5(16\times16)}$.

Скремблирование выполняется путем преобразования векторов коэффициентов вейвлет-разложения

$$\mathbf{u}_1 = \left[d_1^1, d_2^1, \ldots, d_{128}^1\right], \quad \mathbf{u}_2 = \left[d_1^2, d_2^2, \ldots, d_{64}^2\right],$$
$$\mathbf{u}_3 = \left[d_1^3, d_2^3, \ldots, d_{32}^3\right], \quad \mathbf{u}_4 = \left[d_1^4, d_2^4, \ldots, d_{16}^4\right],$$
$$\mathbf{u}_5 = \left[c_1^4, c_2^4, \ldots, c_{16}^4\right]$$

с помощью набора Н-эквивалентных матриц $\boldsymbol{S}_i$

$$\mathbf{v}_i = \mathbf{S}_i \cdot \mathbf{u}_i \qquad i = 1, \ldots, 5, \quad (15)$$

где $\mathbf{v}_i$ — векторы скремблированных коэффициентов на сегменте сигнала; $\mathbf{S}_i = \frac{1}{N_i}\mathbf{P}_{1i} \cdot \mathbf{H}_i \cdot \mathbf{P}_{2i}$ — набор Н-эквивалентных матриц соответствующей размерности.

Таким образом, вариант с конкатенацией вейвлет-коэффициентов позволяет выполнять скремблирование путем линейной комбинации коэффициентов на всех пространствах разложения, соответствующих разным частотным полосам сигнала. Поэтому метод может быть условно отнесен к время-частотным методам скремблирования, которые обеспечивают более высокую безопасность, но требуют большего объема вычислений, поскольку используют матрицы Адамара высокой размерности.

Метод без конкатенации вейвлет-коэффициентов предполагает выполнение линейной комбинации коэффициентов отдельно в каждом пространстве разложения и поэтому может быть

условно отнесен к методам временно́го скремблирования, которые обладают меньшей безопасностью и выполняют меньше вычислений, используя матрицы Адамара меньшей размерности.

ДЕСКРЕМБЛИРОВАНИЕ ВЕЙВЛЕТ-КОЭФФИЦИЕНТОВ

Дескремблирование включает преобразование вейвлет-коэффициентов с помощью обратных Н-эквивалентных матриц $\boldsymbol{S}^{-1}$ и последующее восстановление сигнала обратным вейвлет-преобразованием, с использованием сопряженных квадратурных фильтров h^* и g^*. Дескремблированный сигнал определяется преобразованием

$$\hat{\mathbf{s}} = \mathbf{W}^{-1} \cdot \mathbf{S}^{-1} \cdot \mathbf{v}^T, \tag{16}$$

где $\hat{\mathbf{s}}$ — дескремблированный сигнал; $\mathbf{W}^{-1}$ — обратное вейвлет-преобразование; $\mathbf{S}^{-1} = \frac{1}{N^{1/2}} (\mathbf{P}_1 \cdot \mathbf{H} \cdot \mathbf{P}_2)^{-1}$ — обратная Н-эквивалентная матрица. Преимуществом матриц Адамара является то, что процесс дескремблирования выполняется за счет процедуры получения $\mathbf{S}^{-1}$ простым транспонированием нормированной ортогональной матрицы

$$\mathbf{S}^{-1} = \frac{1}{N^{1/2}} (\mathbf{P}_1 \cdot \mathbf{H} \cdot \mathbf{P}_2)^{-1} = \frac{1}{N^{1/2}} (\mathbf{P}_1 \cdot \mathbf{H} \cdot \mathbf{P}_2)^T. \tag{17}$$

Таким образом, использование в процессе скремблирования и дескремблирования нормированной ортогональной матрицы позволяет заменить сложную операцию обращения матрицы на операцию ее транспонирования, которая выполняется достаточно быстро и не вносит дополнительных задержек.

При выполнении дескремблирования сигнала для варианта с конкатенацией вейвлет-коэффициентов получается вектор, содержащий упорядоченные вейвлет-коэффициенты

$$\begin{aligned} \mathbf{u} = \big[& d_1^1, d_2^1, \ldots, d_{128}^1, d_1^2, d_2^2, \ldots, \\ & d_{64}^2, d_1^3, d_2^3, \ldots, d_{32}^3, \ldots, d_1^4, d_2^4, \ldots, \\ & d_{16}^4, \ldots, c_1^4, c_2^4, \ldots, c_{16}^4 \big], \end{aligned} \tag{18}$$

и при отсутствии ошибок скремблирования и дескремблирования имеется полное восстановление речевого сигнала: $\hat{\mathbf{u}} = \mathbf{u}$.

Из вектора $\mathbf{u}$ могут быть выделены отдельные группы вейвлет-коэффициентов для каждого из пространств разложения:

$$\begin{aligned} \{d_k^1\}_{k=1,\ldots,128} &= \{u_k\}_{k=1,\ldots,128}, \\ \{d_k^2\}_{k=1,\ldots,64} &= \{u_k\}_{k=129,\ldots,192}, \\ \{d_k^3\}_{k=1,\ldots,32} &= \{u_k\}_{k=193,,224}, \\ \{d_k^4\}_{k=1,\ldots,16} &= \{u_k\}_{k=225,\ldots,240}, \\ \{c_k^4\}_{k=1,\ldots,16} &= \{u_k\}_{k=241,\ldots,256}. \end{aligned} \tag{19}$$

В варианте без конкатенации вейвлет-коэффициентов они могут быть получены непосредственно из соотношения

$$\hat{\mathbf{u}}_i = \mathbf{S}_i^{-1} \cdot \mathbf{v}_i^T, \tag{20}$$

где также при отсутствии ошибок скремблирования и дескремблирования $\hat{\mathbf{u}}_i = \mathbf{u}_i$,

$$\begin{aligned} &\mathbf{u}_1 = \left[d_1^1, d_2^1, \ldots, d_{128}^1\right], \quad \mathbf{u}_2 = \left[d_1^2, d_2^2, \ldots, d_{64}^2\right], \\ &\mathbf{u}_3 = \left[d_1^3, d_2^3, \ldots, d_{32}^3\right], \quad \mathbf{u}_4 = \left[d_1^4, d_2^4, \ldots, d_{16}^4\right], \\ &\mathbf{u}_5 = \left[c_1^4, c_2^4, \ldots, c_{16}^4\right]. \end{aligned} \tag{21}$$

Восстановление сигнала из дескремблированных вейвлет-коэффициентов выполняется с помощью схемы синтеза, которая заключается в получении c_{i-1} из c_i и d_i [10]. Для этого используется набор квадратурно-зеркальных фильтров h_n и g_n. Входом этих фильтров служат коэффициенты $\{c_k^J\}_{k=1,2,\ldots}$ и $\{d_k^j\}_{k=1,2,\ldots}$ при j = 1, 2, …, J. Восстановление все более точной аппроксимации выполняется с помощью сопряженных фильтров согласно соотношению

$$c_m^{j-1} = \sum_k h_{m-2k}^j . c_k^j + g_{m-2k}^j . d_k^j. \tag{22}$$

Таким образом, скремблер, основанный на вейвлет-преобразовании, не вносит дополнительных искажений в сигнал, поскольку использует свойство полного восстановления, характерное для вейвлет-преобразования. При выборе биортогонального вейвлет-базиса фильтры разложения и восстановления имеют линейную фазовую характеристику и не вносят дополнительных фазовых искажений. Для биортогонального базиса фильтры разложения и восстановления могут иметь разную длину, и это позволяет балансировать объем вычислений при скремблировании и дескремблировании.

Распределенная система обработки речевой информации может использовать аналоговые и цифровые каналы связи. Сигнал, содержащий

конфиденциальную информацию, может передаваться по аналоговому каналу, соединяющему компьютеры через модем, или по цифровому каналу в локальной или глобальной компьютерной сети.

АЛГОРИТМЫ ЗАЩИТЫ СИГНАЛА В АНАЛОГОВОМ И ЦИФРОВОМ КАНАЛАХ СВЯЗИ

Защита сигнала в аналоговом канале может быть обеспечена разработанным методом скремблирования с дополнительными преобразованиями сигнала в цифровую и аналоговую формы (рис. 1, а). Алгоритм включает вейвлет-преобразование сегмента речевого сигнала, преобразование коэффициентов с помощью Н-эквивалентной матрицы и обратное ВП, которое позволяет получить скремблированный сигнал в аналоговой форме.

Защита сигнала, передаваемого по цифровому каналу, осуществляется применением алгоритма, представленного на рис. 1, б. После Н-эквивалентного преобразования вейвлет-коэффициентов производится формирование пакетов данных для передачи по цифровому каналу. На стороне декодера выполняется дескремблирование с помощью транспонированных Н-эквивалентных матриц и обратное ВП, которое позволяет восстановить исходный сигнал в цифровой форме.

КОЛИЧЕСТВО КЛЮЧЕЙ

При выполнении алгоритма скремблирования задается базовый ключ и ключ сеанса. Ключ сеанса обеспечивает генерацию Н-эквивалентной матрицы и изменяется на каждом сегменте сигнала. Базовый ключ изменяется редко и задает последовательность ключей сеанса. Большее количество

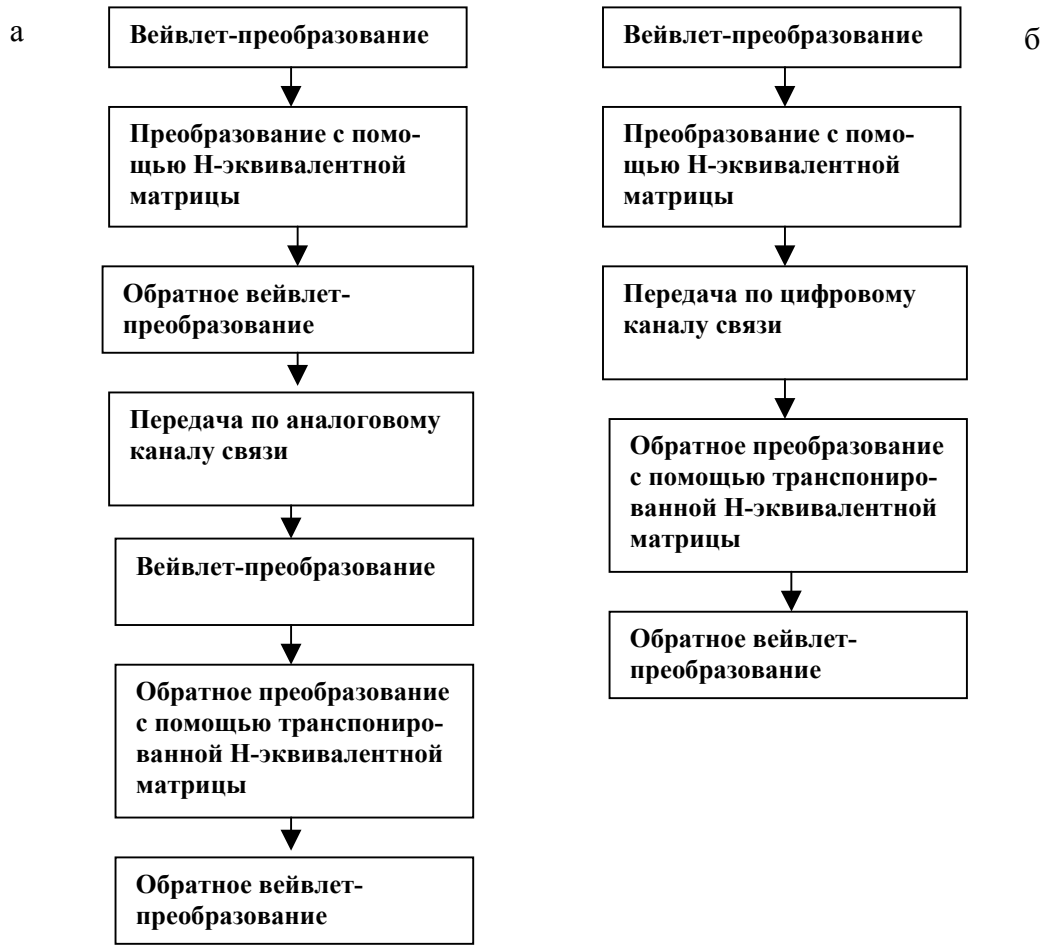

Рис. 1. Варианты алгоритма скремблирования в аналоговом (а) и цифровом (б) каналах связи

ключей сеанса дает высокую защищенность системы и позволяет реже изменять базовый ключ, поэтому количество ключей сеанса является важной характеристикой алгоритма скремблирования.

Для алгоритма скремблирования с конкатенацией вейвлет-коэффициентов число ключей сеанса определяется количеством H-эквивалентных матриц, размерность которых зависит от длины конкатенированного вектора вейвлет-коэффициентов

$$K = \left(2^N \cdot N!\right)^2, \qquad (23)$$

где N — размерность H-эквивалентной матрицы, равная длине сегмента сигнала; K — количество ключей. Зависимость логарифма количества ключей от длины сегмента сигнала приведена в табл. 1. Для алгоритма без конкатенации количество ключей определяется количеством H-эквивалентных матриц в каждом пространстве вейвлет-разложения

Табл. 1. Зависимость количества ключей от длины сегмента сигнала для формы алгоритма скремблирования с конкатенацией вейвлет-коэффициентов

N	lg(K)	N	lg(K)
64	108	256	584
128	254	512	1381

Табл. 2. Зависимость количества ключей от длины сегмента сигнала для формы алгоритма скремблирования без конкатенации вейвлет-коэффициентов

N	Число пространств	lg(K)
128	4	44
	5	32
	6	25
	7	21
256	4	108
	5	81
	6	63
	7	52
512	4	254
	5	192
	6	153
	7	127

$$K = \left(2^{\frac{N}{M}} \cdot \left(\frac{N}{M}\right)!\right)^2, \qquad (24)$$

где M — число подпространств вейвлет-разложения; N — длина сегмента; K — количество ключей. Зависимость количества ключей от длины сегмента сигнала приведена в табл. 2. Некоторые H-эквивалентные матрицы, которые производятся в соответствии с алгоритмом Сельвестера, повторяются, поэтому реальное число ключей несколько меньше, чем число ключей, указанное в табл. 1 и 2.

Анализ показывает, что предложенный метод скремблирования имеет количество ключей, превышающее число ключей в методах частотного, временно́го и время-частотного скремблирования.

СПЕКТР СКРЕМБЛИРОВАННОГО СИГНАЛА

Описанный алгоритм реализован в среде Matlab 5.3 и выполнено скремблирование с конкатенацией и без конкатенации вейвлет-коэффициентов в пространствах разложения речевого сигнала. Наиболее сложен для скремблирования сигнал, представляющий собой гласные фонемы [13], который плохо скрывается существующими методами частотного, временно́го и время-частотного скремблирования. Поэтому для проверки предложенного метода скремблирования использованы сегменты, содержащие гласные фонемы. На рис. 2 приведены графики, которые представляют сегмент исходного сигнала фонемы (i:) и его скремблированную форму. В результате скремблирования формантная частота фонемы скрыта и не видна на графике. Двухмерная форма (в пространстве разложения сигнала время—индекс)

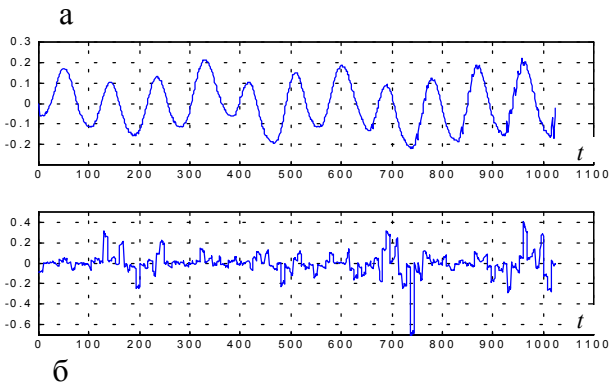

Рис. 2. Исходный (а) и скремблированный (б) сигналы

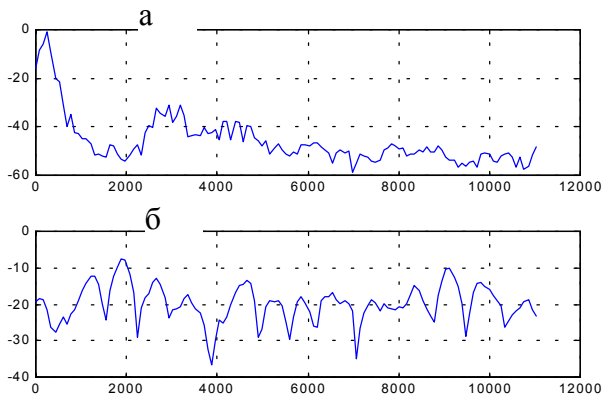

Рис. 3. Спектры мощности исходного (а) и скремблированного (б) сигналов

вейвлет-представлений исходного и скремблированного сигналов демонстрирует более равномерное распределение вейвлет-коэффициентов по уровням разложения в скремблированном сигнале. Сравнение (рис. 3) спектров мощности исходного и скремблированного сигналов также показывает, что скремблированный сигнал имеет почти равномерное распределение мощности по частотному диапазону.

Аналогичные результаты получены для других фонем. Таким образом, можно заключить, что в результате скремблирования вейвлет-коэффициентов с использованием матриц Адамара узкополосный сигнал приобретает спектр мощности, близкий к равномерному спектру.

ОСТАТОЧНАЯ ИНФОРМАТИВНОСТЬ СКРЕМБЛИРОВАННОГО СИГНАЛА

Мера качества алгоритма скремблирования — это количество информации $I(s,\tilde{s})$ об исходном сигнале s, которое содержится в скремблированной форме сигнала $\tilde{s}$. С использованием меры Шеннона остаточное количество информации определяется разностью энтропии $H(s)$ исходного сигнала и условной энтропии $H_{\tilde{s}}(s)$ сигнала по его скремблированной форме [14],[15]

$$I(s,\tilde{s}) = H(s) - H_{\tilde{s}}(s). \qquad (25)$$

Энтропия $H_{\tilde{s}}(s)$ — средняя энтропия (условная по распределению скремблированного сигнала) определяется выражением

$$H_{\tilde{s}}(s) = \sum_{j=1}^{N} P(\tilde{s}_j)\cdot H(s/\tilde{s}_j) =$$
$$= \sum_{j=1}^{N} P(\tilde{s}_j)\cdot\left\{-\sum_i P(s_i/\tilde{s}_j)\cdot\log\left[P(s_i/\tilde{s}_j)\right]\right\} =$$
$$= -\sum_{i=1}^{N}\sum_{j=1}^{N} P(s_i,\tilde{s}_j)\cdot\log\left[P(s_i/\tilde{s}_j)\right], \qquad (26)$$

где $P(\tilde{s}_i)$ — распределение вероятностей скремблированного сигнала; $P(s_i/\tilde{s}_j)$ — условное распределение вероятностей сигнала s_i при известном скремблированном значении $\tilde{s}_i$; $P(s_i,\tilde{s}_j)$ — совместное распределение вероятностей исходного и скремблированного сигналов; $H(s_i/\tilde{s}_j)$ — условная энтропия сигнала s_i при известном скремблированном значении $\tilde{s}_j$.

Оценка остаточной информации в скремблированном сигнале $I(s,\tilde{s})$ может быть выражена и на основе соотношения (27), отражающего взаимосвязь совместной, условной и частной энтропий:

$$H(s\,|\,\tilde{s}) = H(s,\tilde{s}) - H(\tilde{s}). \qquad (27)$$

Преобразование (27) приводит к удобной форме для информации:

$$I(s,\tilde{s}) = H(s) - H(s\,|\,\tilde{s}) =$$
$$= H(s) - H(s,\tilde{s}) + H(\tilde{s}), \qquad (28)$$

$$I(s,\tilde{s}) = \sum\sum[-p(s,\tilde{s})\log p(s) +$$
$$+ p(s,\tilde{s})\log p(s,\tilde{s}) - p(s,\tilde{s})\log p(\tilde{s})] =$$
$$= \sum\sum\left[p(s,\tilde{s})\log\frac{p(s,\tilde{s})}{p(s)p(\tilde{s})}\right]. \qquad (29)$$

В качестве первого приближения использована нормальная аппроксимация для плотностей распределения сигнала, скремблированного сигнала, совместной и условной плотности сигнала и скремблированного сигнала:

$$P(s) = \frac{1}{\sqrt{2\pi}\cdot\sigma_s}\cdot\exp\left(-\frac{s^2}{\sigma_s^2}\right),$$
$$P(\tilde{s}) = \frac{1}{\sqrt{2\pi}\cdot\sigma_{\tilde{s}}}\cdot\exp\left(-\frac{\tilde{s}^2}{\sigma_{\tilde{s}}^2}\right); \qquad (30)$$

$$P(s,\tilde{s}) = \frac{1}{2\pi\sigma_s\sigma_{\tilde{s}}\sqrt{1-r^2}}\times$$
$$\times\exp\left[-\frac{1}{2(1-r^2)}\cdot\left(\frac{s^2}{\sigma_s^2}+\frac{\tilde{s}^2}{\sigma_{\tilde{s}}^2}-\frac{2r\cdot s\cdot\tilde{s}}{\sigma_s\sigma_{\tilde{s}}}\right)\right]; \qquad (31)$$

$$P(s/\tilde{s}) = \frac{P(s,\tilde{s})}{P(\tilde{s})} =$$

$$= \frac{1}{\sqrt{2\pi}\cdot\sigma_s\sqrt{1-r^2}}\cdot\exp\left[-\frac{1}{2(1-r^2)}\cdot\left(\frac{s^2}{\sigma_s^2}+\frac{\tilde{s}^2\cdot(2r^2-1)}{\sigma_{\tilde{s}}^2}-\frac{2r\cdot s\cdot\tilde{s}}{\sigma_s\sigma_{\tilde{s}}}\right)\right], \quad (32)$$

где σ_s и $\sigma_{\tilde{s}}$ — среднеквадратические отклонения сигнала s и скремблированного сигнала $\tilde{s}$; r — коэффициент корреляции между ними.

В этом случае выражение для количества информации о сигнале в его скремблированной форме приобретает вид

$$I(s,\tilde{s}) = \sum_{i=1}^{N}\sum_{j=1}^{N}\left\{\frac{1}{2\pi\sigma_s\sigma_{\tilde{s}}\sqrt{1-r^2}}\cdot\exp\left[-\frac{1}{2(1-r^2)}\cdot\left(\frac{s_i^2}{\sigma_s^2}+\frac{\tilde{s}_j^2}{\sigma_{\tilde{s}}^2}-\frac{2r\cdot s_i\tilde{s}_j}{\sigma_s\sigma_{\tilde{s}}}\right)\right]\times\right.$$

$$\left.\times\log\left[\frac{1}{\sqrt{1-r^2}\cdot\exp\left[-\left(s_i^2/\sigma_s^2+\tilde{s}_j^2/\sigma_{\tilde{s}}^2\right)\right]}\cdot\exp\left[-\frac{1}{2(1-r^2)}\cdot\left(\frac{s_i^2}{\sigma_s^2}+\frac{\tilde{s}_j^2\cdot}{\sigma_{\tilde{s}}^2}-\frac{2r\cdot s_i\tilde{s}_j}{\sigma_s\sigma_{\tilde{s}}}\right)\right]\right]\right\}. \quad (33)$$

В такой же последовательности получена остаточная информация для экспоненциально-степенного распределения, которое более полно описывает статистику речевых сигналов [8]. Для плотности сигнала использовано выражение

$$p(s) = \frac{\alpha}{2\lambda\sigma\Gamma(1/\alpha)}\exp\left(-\left|\frac{s}{\lambda\sigma}\right|^{\alpha}\right), \quad (34)$$

а для совместной плотности сигнала и его скремблированной формы (с учетом возможной корреляции) — выражение

$$p(s,\tilde{s}) = \frac{\alpha^2\sqrt{1-r^2}}{4(\lambda_s\sigma_s)(\lambda_{\tilde{s}}\sigma_{\tilde{s}})[\Gamma(1/\alpha)]^2}\times$$

$$\times\exp\left(-\left|\frac{s^2}{\lambda_s^2\sigma_s^2}+\frac{2rs\tilde{s}}{\lambda_s\sigma_s\lambda_{\tilde{s}}\sigma_{\tilde{s}}}+\frac{\tilde{s}^2}{(\lambda_{\tilde{s}}\sigma_{\tilde{s}})^2}\right|^{\alpha}\right). \quad (35)$$

Количество остаточной информации $I(s,\tilde{s})$, которое для обеспечения безопасности должно быть как можно меньше, зависит от коэффициента корреляции r между исходным и скремблированным сигналами. Для сегментов гласных фонем (фрагментов речевого сигнала, наиболее трудных для закрытия информации) получены оценки коэффициентов корреляции. Корреляционное поле для сегмента сигнала показывает, что корреляция практически отсутствует (рис. 4).

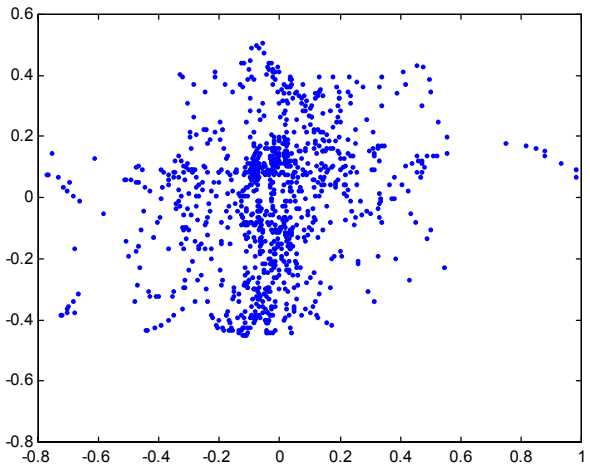

Рис. 4. Корреляционное поле исходного сигнала и скремблированного сигнала

Оценки коэффициентов корреляции между исходным и скремблированным сигналами, полученные для разных гласных фонем, находятся в диапазоне –0.24 … 0.3 со средним значением коэффициента корреляции 0.06 (табл. 3).

Теоретическая статистика указывает на довольно широкие доверительные пределы коэффициента корреляции. Например, при N = 400 и доверительной вероятности 0.99 экспериментальной оценке коэффициента 0.1 может соответствовать интервал (–0.03 … +0.2). В связи с этим

Табл. 3. Значения коэффициентов корреляции r между скремблированным и исходным сигналами

Фонема	r
[i]	–0.10 0.30
[o]	–0.24 0.08
[a]	0.07 0.08
[u]	0.027 0.17
[e]	–0.05 0.27

для остаточной информации скремблированной формы относительно основного сигнала рассчитан критерий взаимной информации для коэффициента корреляции до 0.25. Использовано как нормальное приближение, так и экспоненциально-степенной закон для распределения двух форм сигнала. Результаты показывают, что относительная остаточная информация при нормальной аппроксимации не превышает 0.8 %, а для экспоненциально-степенного распределения с различным значением параметра формы [8] имеет верхнюю границу 0.6 – 1 %.

Таким образом, корреляционный анализ показывает, что между исходным и скремблированным сигналами практически отсутствует корреляция, и это обеспечивает малую остаточную информативность скремблированного сигнала. Информационный критерий подтверждает высокую защищенность речевого сигнала при предложенном методе скремблирования на основе вейвлет-преобразования и матриц Адамара.

ЗАКЛЮЧЕНИЕ

Предложен и исследован метод скрытой передачи информационного сигнала речи для распределенной системы, включающей локально-сетевую структуру ЭВМ. Метод использует скремблирование на основе модифицированного вейвлет-преобразования. Алгоритм скремблирования включает преобразование матрицами Адамара вейвлет-отображения сигнала, имеет две разновидности (с конкатенацией и без конкатенации вейвлет-коэффициентов сигнала) и предлагается в двух формах: для аналоговых и цифровых каналов.

Введение двухфазного преобразования обеспечивает методу высокие показатели качества информационной безопасности по количеству ключей и минимальной величине остаточной информации в скремблированном сигнале. Для получения этих показателей применены методы теории матриц Адамара, комбинаторного, корреляционного анализа (для наиболее трудно скремблируемых элементов — фонем) и теоретико-информационный метод. Выполненные количественные оценки показывают преимущество метода двухфазного скремблирования над традиционными его формами.

СПИСОК ЛИТЕРАТУРЫ

1. *Baker H.J., Piper E.C.* Secure Speech Communication. London: Academic Press, 1997. 330 p.
2. *Jayant N.S., Cox R.V., Mc Dermont B.J.* Analog Scremblers for Speech Based on Sequential Permutationsin Time and Frequency // Bell System Technical Journal. 1983. V. 62, N 1. P. 25–46.
3. *Delic V.D., Milosevic V.S., Senk V.* Speech Scrembling Method. Analysis and Fast Algorithm // Proceedings of 8th European Signal Processing Conference EUSIPCO 96. Trieste, Italy, 1996. P. 1705–1708.
4. *Меркушева А.В.* Скремблер на основе преобразований вейвлет и Адамара // Проблемы информационной безопасности. 2000. № 1. С. 86–92.
5. *Меркушева А.В, Малыхина Г.Ф.* Скремблирование на основе вейвлет-преобразования // Сб. "Информационные и бизнес-технологии 21-го века", Труды научно-технической конференции. СПбГТУ, 1999. С. 19–20.
6. *Исмаилов Ш.Ю., Меркушева А.В.* Нейросетевой алгоритм на вейвлет-преобразовании нестационарного сигнала в ИИС // Сб. докладов Международной конференции по мягким вычислениям и измерениям SCM-2002. СПб., 2001. Т. 1. С. 251–256.
7. *Малыхина Г.Ф., Меркушева А.В.* Детектирование речевого сигнала и фильтрация с адаптивным порогом // Микропроцессорные средства измерений: Сборник трудов факультета технической кибернетики СПбГТУ. СПб., 2001. Вып. 2. С. 26–35.
8. *Меркушева А.В.* Фильтрация нестационарного сигнала (речи) в вейвлет-области с адаптацией к виду и динамике шума // Научное приборостроение. 2003. Т. 13, № 2. С. 73–87.
9. *Daubechies I.* Orthogonal Basis and Wavelets // SIAM Journal of Mathematical Analysis. 1993. V. 24, N. 2. P. 499–516.
10. *Daubechies I.* Orthogonal Basis of Compactly Supported Wavelets // Communications in Pure

and Applied Mathematics. 1988. V. 41, N 7. P. 909–996.
11. *Colomb S.W., Banmert I.D.* The Search of Hadamard Matrices // American Mathematics Monthly. 1983. V. 70. P. 12–17.
12. *Vallis W.D., Street A.P., Wallis J.S.* Combinatorics: Rom Squares, Sum Free Sets, Hadamard Matrices. N.Y., 1972. 240 p.
13. *Sohn I., Kim N.S., Sung W.*A. Statistical Model-Based Voice Activity Detection // IEEE Signal Processing Letters. 1999. V. 6, N 1. P. 1–3.
14. *Кульбак С.* Теория информации и статистика. М.: Наука, 1976. 408 с.
15. *Айвазян С.А., Енюков И.С., Мешалкин Л.Д.* Прикладная статистика. Исследование зависимостей. М., 1985. 487 с.

Санкт-Петербург

Материал поступил в редакцию 31.03.2003.

HIDDEN TRANSMISSION OF INFORMATIONAL SIGNALS BY MEANS OF MODIFIED WAVELET TRANSFORMATION

A. V. Merkusheva

Saint-Petersburg

A method is investigated for hidden transmission of informational signals (speech) by means of scrambling on the basis of double transformation: wavelet-mapping modification with H-equivalent matrices. Two algorithm structures for scrambling are given and analyzed. They are specialized for analog and digital channels. The number of keys is determined. The residual information in a scrambled signal is estimated on the basis of two methods (correlation and information-theoretic).