

Література

1. Демідов, Б. О. Системна методологія обґрунтування, формування та реалізації оперативного-тактичних і тактико-технічних вимог до зразків (комплексів, систем) озброєння та військової техніки [Текст] / Б. О. Демідов, М. І. Луханін, М. В. Науменко // Наука і оборона. – 2011. – № 1. – С. 45 – 50.
2. Гриб, Д. А. Методологічний підхід до формування технічного обрисів перспективних зразків озброєння та військової техніки [Текст] / Д. А. Гриб, Б. О. Демідов, М. В. Науменко // Наука і оборона. – 2009. – № 4. – С. 30 – 34.
3. Василенко, А. В. Методические аспекты формирования общих технических требований при разработке вооружения и военной техники [Текст] / А. В. Василенко, П. А. Лукьянов, Л. М. Зотова, В. В. Сотник // Артиллерийское и стрелковое вооружение. – 2007. – № 2. – С. 56 – 59.
4. Коломийцев, А. В. Определение параметров траектории движения пули калибра 9 мм с вогнутой оживальной головной частью с учётом изменения её коэффициента силы лобового сопротивления [Текст] / А. В. Коломийцев // Вопросы проектирования и производства конструкций летательных аппаратов. Сб. науч. трудов Гос. ун-та им. Н.Е. Жуковского "ХАИ". Вып. 19(2). – Х: ДАКУ "ХАИ", 2000. – С. 48 – 52.
5. Біленко, О. І. Визначення оптимальних параметрів елементів боєприпасів для забезпечення заданої ефективності стрільби [Текст] / О. І. Біленко, В. В. Афанасьєв // Збірник наукових праць ХУПС. – Х.: ХУПС – 2008. – Вип. 1. – С. 16 – 20.
6. Біленко, О. І. Розробка тактико-технічних вимог до кінетичної зброї не смертельної дії [Текст] / О. І. Біленко, В. В. Пашенко // Збірник наукових праць ХУПС. – Х.: ХУПС, 2012. – вип. 1 (30). – С. 2 – 5.
7. Пашенко, В. В. Дослідження впливу температури заряду на дульну швидкість поразяючих елементів кінетичної зброї не смертельної дії [Текст] / В. В. Пашенко // Збірник наукових праць ХУПС. – Х.: ХУПС, 2011. – вип. 1 (6) – С. 12 – 15.
8. Бабах, Ф. К. Основы стрелкового оружия [Текст] / Ф. К. Бабах. – СПб.: ООО "Полигон", 2003. – 253 с.
9. Кирилов, В. М. Основания устройства и проектирования стрелкового оружия [Текст] / В. М. Кирилов. – Пенза: 1963. – 343 с.
10. Теория и расчёт автоматического оружия [Текст] / А. К. Голомбовский и др. – Пенза: ПВАИУ, 1973. – 493 с.

Запропоновано методи сегментації сигналів підземних трубопроводів на основі вейвлет-нейронних мереж і дискретного вейвлет-перетворення. Сегментація є етапом, який передує етапам аналізу і класифікації сигналів з метою виявлення витоків, і служить для виділення фрагментів сигналу, які не містять зовнішніх техногенних шумів. Проведено дослідження ефективності запропонованих методів сегментації

Ключові слова: сегментація, вейвлет-перетворення, витоків трубопроводів

Предложены методы сегментации сигналов подземных трубопроводов на основе вейвлет-нейронных сетей и дискретного вейвлет-преобразования. Сегментация является этапом, предшествующим этапам анализа и классификации сигналов с целью обнаружения утечек, и служит для выделения участков сигнала, не содержащих внешних техногенных шумов. Проведены исследования эффективности предложенных методов сегментации

Ключевые слова: сегментация, вейвлет-преобразование, утечки трубопроводов

УДК 004.891.3

СЕГМЕНТАЦИЯ СИГНАЛОВ ПОДЗЕМНЫХ ТРУБОПРОВОДОВ НА ОСНОВЕ ВЕЙВЛЕТ-АНАЛИЗА

В. А. Строганов

Кафедра информационных систем
Севастопольский национальный технический университетул. Университетская, 33, г. Севастополь,
Украина, 99053

E-mail: vstroganov@mail.ru

1. Введение

Одним из наиболее перспективных подходов к поиску утечек подземных трубопроводов можно считать метод анализа акустических сигналов, излучаемых движущейся по трубопроводу жидкостью [1]. Акустический сигнал, излучаемый трубопроводом, преоб-

разуется в колебания грунта и может быть считан на поверхности грунта, над местом прокладки трубопровода [2]. Решение о наличии или отсутствии утечки в данной точке трубопровода может быть принято по результатам классификации полученного сигнала [3].

При использовании такого подхода возникает проблема влияния внешних шумов на сигнал трубопро-

вода. К сигналу трубопровода примешиваются шумы техногенного происхождения: звуки проходящего автотранспорта, работающих механизмов и т. п. Уровень шумов, как правило, высок, что мешает распознаванию сигналов утечек. Кроме того, шумы имеют нестационарный характер, что затрудняет использование для борьбы с ними алгоритмов фильтрации. Учитывая, что шумы имеют кратковременный характер, представляется возможным выделить для дальнейшего анализа и распознавания временные участки сигнала, не содержащие внешних шумов. То есть речь идет о необходимости разработки метода сегментации сигналов подземных трубопроводов.

2. Сегментация сигналов подземных трубопроводов

Пусть дан сигнал подземного трубопровода, представленный дискретными отсчетами $x[n]$. Рассматривается фрагмент сигнала, включающий N отсчетов:

$$x[n] = \{x[0], x[1], \dots, x[N - 1]\}.$$

В некоторый случайный момент времени n_1 к сигналу трубопровода добавляется внешний шум, который прекращается в момент времени $n_2 > n_1$. Разобьем сигнал $x[n]$ на L сегментов $x_0[n], x_1[n], \dots, x_{L-1}[n]$ длиной K отсчетов каждый:

$$x_i[n] = \{x[2^*i], x[2^*i + 1], \dots, x[2^*i + K - 1]\}.$$

Тогда задачу сегментации сигнала подземного трубопровода $x[n]$ можно сформулировать следующим образом: необходимо определить множество номеров сегментов сигнала без внешнего шума $L_{\text{чист}} = \{l_{\text{чист},i}\}$, таких, что

$$2^*l_{\text{чист},i} + K - 1 < n_1 \quad || \quad 2^*l_{\text{чист},i} > n_2. \quad (1)$$

2.1. Модель сигнала и техногенного шума

Для исследований предложена модель сигнала утечки подземного трубопровода и фонового шума. Результирующий сигнал $x(t)$ при этом определяется выражением

$$x(t) = \sum_{q=1}^Q c_q \sin(2\pi(f_q + \Delta f_q)t + \phi) + \sum_{r=1}^R d_r \sin(2\pi(f_r + \Delta f_r)t + \phi) + n,$$

где c_q – амплитуды гармонических составляющих сигнала утечки с частотами f_q ; d_r – амплитуды гармонических составляющих фонового сигнала с частотами f_r ; ϕ – случайная начальная фаза сигналов, равномерно распределённая на интервале от 0 до 2π ; n – гауссовский шум с заданной дисперсией. Дополнительно вводится Δf – случайное приращение частоты гармонических составляющих как основного, так и фонового сигналов, с заданной дисперсией.

Полученный сигнал $x(t)$ оцифровывается с частотой дискретизации f_{sample} , в результате получаем сигнал $x[n]$, состоящий из N отсчетов.

Внешний шум $s[n]$ моделируется как случайный процесс с равномерным законом распределения. Уро-

вень шума задается в процентах относительно уровня чистого сигнала.

На рис. 1 показаны графики чистого сигнала трубопровода и сигнала с кратковременным внешним шумом. Уровень шума при этом составляет 50% от максимального уровня сигнала.

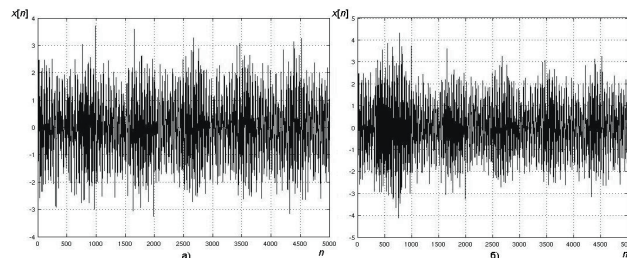


Рис. 1. Сигналы, полученные на основе моделей: а – отсчеты чистого сигнала трубопровода $x[n]$ в зависимости от номера отсчета n ; б – отсчеты сигнала трубопровода $x[n]$ с внешним шумом в зависимости от номера отсчета n

Видно, что эти сигналы визуально не различимы.

2.2. Сегментация на основе дискретного вейвлет-преобразования

Для сегментации сигналов трубопроводов и выделения сегментов, не содержащих шума, предлагается использовать дискретное вейвлет-преобразование. Дискретное вейвлет-преобразование определяется выражением [5, 9]

$$D(m,n) = 2^{-m/2} \sum x(k)\psi(2^{-m}k - n),$$

$$k, m, n \in \mathbf{Z}.$$

где $x[k]$ – исходный сигнал, $\psi[k]$ – вейвлет-функция. Как видно, вейвлет преобразование заключается в разложении сигнала $x[n]$ по базису, формируемому за счет растяжений и сдвигов вейвлет-функции $\psi[k]$: вейвлет-функция сдвигается по оси времени на целочисленные интервалы и масштабируется с коэффициентами, равными степеням числа 2.

Основная особенность вейвлет-преобразования заключается в том, что вейвлет-функции обладают временной локализацией [6], что позволяет применять вейвлет-преобразование для анализа нестационарных процессов и анализировать локальные особенности сигналов [7]. В нашем случае речь идет об анализе сигналов подземных трубопроводов, содержащих локализованные по времени внешние техногенные шумы.

В результате одного шага дискретного вейвлет-преобразования сигнала $x[n]$ получается два вектора коэффициентов разложения: a и d [8]. Вектор d содержит так называемые детализирующие коэффициенты (англ. details), характеризующие высокочастотную составляющую исходного сигнала. Вектор a соответствует низкочастотной составляющей исходного сигнала (англ. approximations) и подвергается дальнейшему разложению на следующих этапах вейвлет-преобразования.

На рис. 2 показаны результаты одного уровня вейвлет-разложения сигнала с внешним техногенным шумом.

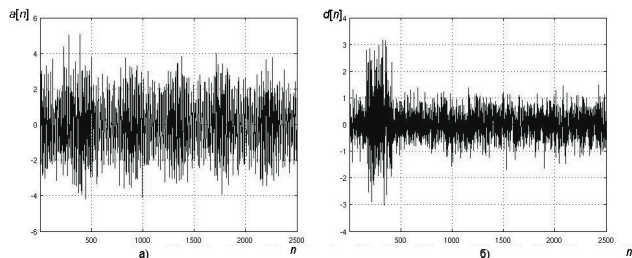


Рис. 2. Результаты вейвлет-разложения:
а — коэффициенты a ; б — коэффициенты d

Видно, что в вейвлет-области наблюдается резкий скачок амплитуды коэффициентов d на участке, соответствующем времени появления внешнего шума. Разобьем вектор d на сегменты d_l , соответствующие сегментам исходного сигнала $x[n]$, и для каждого сегмента вычислим норму $norm_l$ [10]:

$$norm_l = \sqrt{\sum d_l[n]^2}.$$

На рис. 3 показаны нормы сегментов вектора d .

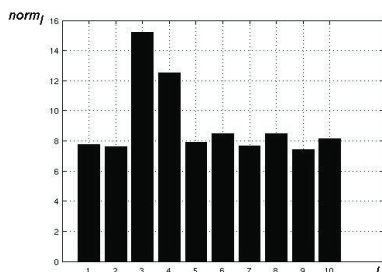


Рис. 3. Нормы $norm_l$ вейвлет-коэффициентов d в зависимости от номера сегмента l

Как показывают исследования, достаточным критерием для того, чтобы определить наличие внешнего шума в l -м сегменте сигнала, является сравнение нормы коэффициентов d_l для этого сегмента с математическим ожиданием норм коэффициентов всего сигнала.

Тогда решение задачи (1) может быть представлено в виде:

$$L_{\text{чист}} = \{l: norm_l < M[norm]\}.$$

2.3. Сегментация экспериментально полученных данных

Были проведены исследования эффективности предложенного метода сегментации применительно к экспериментально полученным сигналам утечек трубопроводов.

Методика получения экспериментальных данных и характеристики сигналов подробно описаны в [4]. К сигналам добавлялся аддитивный шум согласно модели, описанной в разделе 2.1.

Временные графики чистого сигнала трубопровода и сигнала с внешним шумом показаны на рис. 4. Уровень шума при этом составляет 50% от максимального уровня сигнала.

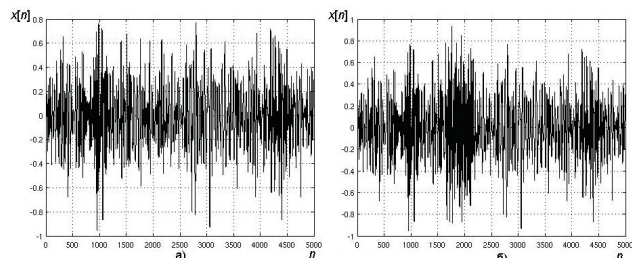


Рис. 4. Сигналы, полученные экспериментально:
а — отсчеты чистого сигнала трубопровода $x[n]$ в зависимости от номера отсчета n ; б — отсчеты сигнала трубопровода $x[n]$ с внешним шумом в зависимости от номера отсчета n

Результаты вейвлет-разложения сигнала трубопровода с кратковременным внешним шумом показаны на рис. 5.

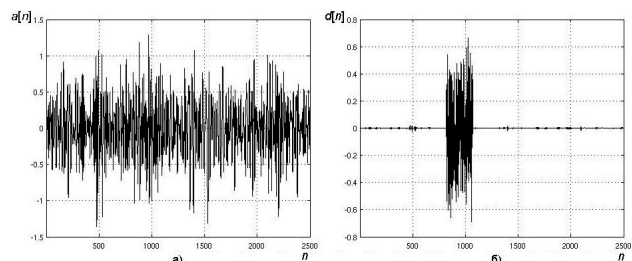


Рис. 5. Результаты вейвлет-разложения сигнала с внешним шумом: а — коэффициенты a ; б — коэффициенты d

Видно, что в вейвлет-области наблюдается резкий скачок амплитуды коэффициентов в моменты времени, соответствующие наличию внешнего шума. Нормы вейвлет-коэффициентов, соответствующих отдельным временным сегментам сигнала, показаны на рис. 6.

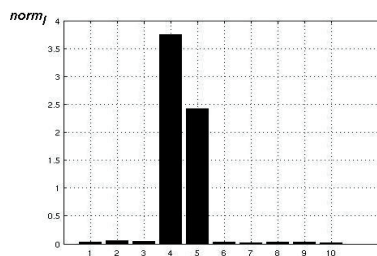


Рис. 6. Нормы $norm_l$ вейвлет-коэффициентов d в зависимости от номера сегмента l

Видно, что анализ вейвлет-коэффициентов позволяет принять решение о наличии или отсутствии внешнего шума в конкретный момент времени.

3. Заключение

По результатам проведенных исследований можно сделать следующие выводы:

- предложен метод сегментации сигналов утечек трубопроводов на основе анализа вейвлет-коэффициентов, получаемых в результате одного шага дискретного вейвлет-преобразования исходного сигнала;
- проведены исследования, подтверждающие работоспособность предложенного метода на основе модельных сигналов и на основе экспериментально полученных сигналов трубопроводов.

Література

1. Разработка методов повышения эффективности обнаружения и локализации мест протекания трубопроводов. Заключительный отчет госбюджетной НИР [Текст] / Руководитель НИР В.С. Чернега. – Севастополь: СевНТУ, 2004. – 145 с.
2. Brechbuehl, M. Beitrag zur akustischen Ortung von Leckstellen [Текст] / M. Brechbuehl. – Zuerich: Diss.ETH, 1988. – 182 с.
3. Строганов, В. А. Классификация сигналов утечек подземных трубопроводов с помощью искусственных нейронных сетей [Текст] / В. А. Строганов // Восточно-Европейский журнал передовых технологий, 2012.– № 6/4(60).– С. 33–36.
4. Строганов, В. А. Экспериментальное исследование сигналов утечек подземных трубопроводов [Текст] / В.А. Строганов, В. Н. Хоролич// Вестник СевНТУ. Сер. Информатика, электроника, связь: Сб. науч. тр. – Севастополь, 2010.– Вып.101.– С. 29–32.
5. Mallat, S. A wavelet tour of signal processing [Текст] / S.Mallat.– San Diego: Academic Press, 2001.– 620 с.
6. Daubechies, I. Ten lectures on wavelets [Текст] / I. Daubechies// CBMS-NSF conference series in applied mathematics. SIAM, 1992.– Том. 61.– 357 с.
7. Chui Charle, K. Wavelets: A Mathematical Tool for Signal Analysis [Текст] / Charles K. Chui // Siam Monographs on Mathematical Modeling and Computation.– 1997.–Том 1.– 210 с.
8. Mallat, S. A theory for multiresolution signal decomposition: the wavelet representation [Текст] / S. Mallat // IEEE Pattern Anal. and Machine Intell., 1989.– Том 11.– №7.– С. 674–693.
9. Chui Charles, K. An Introduction to Wavelets [Текст] / Charles K. Chui.– San Diego: Academic Press, 1992.– 264 с.
10. Бондарев, В. Н. Цифровая обработка сигналов: методы и средства [Текст] / В. Н. Бондарев, Г. Трестер, В. С. Чернега.– Севастополь: Изд-во СевГТУ, 1999.– 398 с.

В роботі проведено оцінювання криптографічної стійкості методу асиметричного шифрування інформації та методу шифрування інформації без попереднього розподілу ключів на основі математичного апарату рекурентних послідовностей. В результаті дослідження встановлено, що криптостійкість методів знаходиться на достатньому рівні, принаймні не меншому, ніж відомих аналогів

Ключові слова: захист інформації, криптографія, шифрування, розподіл ключів, криптографічна стійкість, рекурентні послідовності

В работе проведено оценивание криптографической стойкости метода асимметричного шифрования информации и метода шифрования информации без предварительного распределения ключей на основе математического аппарата рекуррентных последовательностей. В результате исследования установлено, что криптостойкость методов находится на достаточном уровне, по крайней мере не меньшем, чем известных аналогов

Ключевые слова: защита информации, криптография, шифрование, распределение ключей, криптографическая стойкость, рекуррентные последовательности

УДК 681.3.067

ОЦІНЮВАННЯ КРИПТОСТІЙКОСТІ МЕТОДІВ ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Ю. Є. Яремчук
 Кандидат технічних наук, доцент, професор кафедри, директор Центру Центр інформаційних технологій і захисту інформації
 Кафедра адміністративного та інформаційного менеджменту
 Вінницький національний технічний університет
 Хмельницьке шосе, 95, м. Вінниця, 21021, Україна
 E-mail: yurevyar@vntu.net

1. Вступ

На сьогодні криптографічні методи [1, 2] мають широке застосування. При цьому актуальним залишається вирішення проблеми спрощення обчислень

під час криптографічних перетворень, особливо в методах, що базуються на технології відкритого ключа, де використовуються великі ключі та числа великої розрядності. Виходячи з цього, певний інтерес викликає апарат на основі рекурентних послідовностей [3],