одной итерации составляет 81 нс. В случае конвейерной обработки среднее время Ш/Д одного блока определим за формулой

$$T_{сер} = (n \cdot T + 2 \cdot T_{mux} + (N-1)T) / N,$$

где n – количество ступеней конвейера; T – время шифрования для одной итерации, T_{mux} – время переключения MUX; N – количество блоков Ш/Д данных.

Например, для сообщения размером 1 мбайт $T_{ср}$ составило 0,11 мкс, при этом продуктивность КрВ составляет 91 мбайт/с. Для Ш/Д БД большей длинны, например $N \to \infty$, $T_{ср}$ будет приближаться к T. В этом случае граничная продуктивность Ш/Д для этого типа КрВ приближается к 175 мбайт/с. Скорость шифрации 1 гигабайта информации составила порядка 100 мбайт/с, что в 5 раз превышает скоростные показатели [5]. В случае больших объемов информации скорость шифрации превышает показатели аналогов [5] даже более чем 5 раз. Такой прирост скорости был достигнут за счет использования систолической организации вычислителя для реализации криптографического алгоритма.

Список литературы

1. *Корченко А. Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А. Г. – К. : «МК-Пресс», 2006. – 207-214 с.

2. *Панасенко С. П.* Аппаратные шифраторы / С. П. Панасенко, В. В. Ракитин. – Мир ПК, 2002. - № 8 – 77-83 с.

3. *Онучин С.* Устройства защиты информации. Критерии выбора / С. Онучин. – Мир связи: Connect!, 1998. - №9 –104 с.

4. *ДСТУ ГОСТ 28147-89* Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. –[Действительный от 01.01.89].

5. Сравнение аппаратных шифраторов [электронный ресурс]: http://www.s-terra.com/CSP/RU/products/itsec_table.htm.

Поступила 16.03.2010

УДК 621.31 **Рыбальский О.В., Белозеров Е.В., Соловьев В.И., Белозерова Я.А.**

МЕТОДОЛОГИЯ ПРОВЕРКИ ПОДЛИННОСТИ СИГНАЛОГРАММ ВЫДЕЛЕНИЕМ САМОПОДОБНЫХ СТРУКТУР

В работе [1] было показано, что цифровой сигнал, записанный на аппаратуре цифровой записи аналоговых сигналов (АЦЗАС), имеет фрактальную структуру, изменяющуюся при монтажных операциях с этим сигналом.

Дальнейшее изучение этого явления подтвердило, что цифровой сигнал, записанный на каждом конкретном аппарате, имеет свою индивидуальную структуру [2]. Потому это физическое явление может быть использовано, для проведения идентификации АЦЗАС при проведении экспертиз. А учитывая то, что, выявление оригинальности сигналограммы основано на идентификации аппаратуры записи, это явление полностью годно для проведения экспертизы оригинальности сигналограмм [3].

Задачей исследования является создание методологии оценки подлинности сигналограмм на основе сравнения фрактальных характеристик сигналов на различных участках сигналограммы.

Будем рассматривать цифровые данные записи звукового файла, как временной ряд отсчетов амплитуды звуковой волны, которые являются результатом взаимодействия двух составляющих - записываемой мелодии, речи и второй составляющей – аппаратурных помех. В общем случае это не обязательно сумма. Если бы статистические характеристики

этих двух составляющих были примерно одинаковы, постановка большинства задач разделения сигнала и помех была бы безсмысленна. Однако, известно, что в большинстве важных случаев, частотные характеристики сигнала и помехи разнесены. Мощность аппаратурных помех локализуется в основном в высокочастотной области по сравнению с сигналом. С точки зрения современных концепций мультифракталов (самоподобных образований), звуковой сигнал на любом произвольном отрезке представляет собой совокупность различных мультифракталов, как на уровне исходной мелодии, так и на уровне помех. Возможно предположить, что самоподобные структуры характеризующие мелодию, речь будут изменчивы на протяжении достаточно представительных участков звукового файла. В то же время, из физических соображений очевидно, что мультифрактальные образования ответственные за характеристики аппаратуры звукозаписи должны обладать более устойчивыми характеристиками на протяжении достаточно длительных фрагментов звукового файла.

Кроме того, эквивалентная частота мультифракталов порождаемых каналом звукозаписи должна быть выше (либо существенно разнесена) по сравнению с эквивалентной частотой мелодий.

Эти два тезиса являются на данном этапе исследования “гипотезами здравого смысла”. Их подтверждение возможно только при условии создания математической модели (в указанном выше смысле), которая позволит решать поставленные задачи (на основе физических концепций этих гипотез). Не существует на сегоняшний день эффективного механизма выделения всех мультифрактальных образований в звуковом файле. Более того, очевидно, что помеха и полезные сигналы могут взаимодействовать на уровне мультифракталов. На основе вышеизложенного сделаем следующее предположение, которое определяет основную физическую (и математическую) концепцию разработки:

Предположим, что найден метод разделения исходного звукового сигнала на определенном отрезке на совокупность сосчтавляющих фракталов, При этом фрактальные образования в высокочастотной области устойчиво повторяются по характеристикам на протяжении фрагмента (или всего файла данных). Мы будем идентифицировать устойчивые высокочастотные самоподобные структуры с аппаратурой звукозаписи (или ее существенным влиянием на эти структуры).

Статистический анализ этих структур (при условии их выявления) для различных звуковых файлов (фрагментов файла) в принципе позволяет решить поставленные задачи.

Многочисленные исследования, посвященные выделению мультифрактальных структур в звуковых файлах показали следующие недостатки (и как следствие низкую эффективность) “прямого” применения вейвлет-анализа на основе различных базисов.

Первое – в практике вейвлет-анализа используется сравнительно небольшое количество различных базисов, в принциппе достаточных для решения практических задач. Однако, большинство исследований при разложении использует ортогональные базисы. Но природа сигналов вовсе не обязана следовать ортогональности. Как следствие при разложении по определенному ортогональному базису исходного звукового сигнала, хуже всего описываются маломощные высокочастотные составляющие. Но они для нас как раз наиболее интересны. Для повышения эффективности описания, можно использовать неортогональные базисы. Однако в этом случае вычислительные трудности при анализе отрезков данных свыше 1000 точек становятся практически непреодолимыми. Кроме того, неизвестно в каждой конкретной задаче возможно ли получить более точное решение с неортогональным базисом.

Отдельного рассмотрения требует задача анализа мультифрактальных структур в младшем бите звуковых файлов. При прочих равных условиях в рамках рассматриваемых задач может встретиться ситуация, когда повторяющиеся самоподобные структуры являются

следствием шумов АЦП. И только на этом уровне выделение повторяющихся характеристик шумов АЦП на различных участках звукового файла может решить поставленную задачу.

Известно, что, несмотря на влияние звукового сигнала на процесс оцифровки, значения младшего бита во многих случаях определяются в основном собственными характеристиками АЦП.

В качестве физической иллюстрации характера возможного влияния характеристик сигнала подлежащего оцифровке на младший бит приведен рис.1. Это фрагмент изменения младшего бита звукового файла, созданного искусственно и является чистой синусоидой.

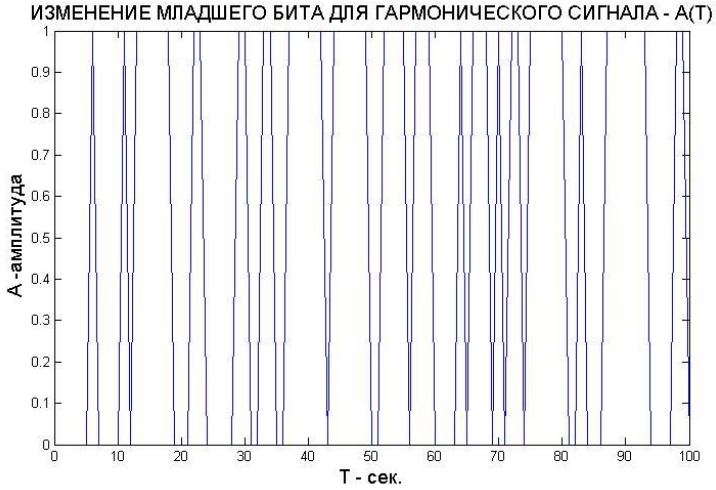

Рис. 1. Характер изменения младшего бита для гармонического сигнала

В младшем бите “остаются следы от синусоиды” в виде повторяющихся с частотой синусоиды пакетов с изменяющейся частотой. На относительно коротких отрезках битовых последовательностей (по сравнению с частотами сигнала) подобное поведение характерно и для суммы любых частот.

На эти частоты в младшем бите накладываются шумы АЦП, которые могут существенно доминировать над составляющими сигнала. В нашей задаче интерес представляют характеристики младшего бита, которые являются большей частью следствием шумов АЦП. Интуитивно ясно, что эффективно разделить данные в младшем бите на рассматриваемые две составляющие вряд ли возможно.

Но возможна несколько модифицированная постановка задачи. А именно. Будем считать, что шумы АЦП наиболее сильно проявляются в высокочастотной области (более 10 КГц. В это случае возможно на определенном отрезке записи в младшем бите построить частотный спектр сигнала по какому-либо рациональному базису, выделить часть спектра, эквивалентную высоким частотам, и сравнивать различные отрезки младшего бита по высокочастотной составляющей спектра с целью определения стабильности или изменчивости характеристик этого участка спектра. Высокочастотные составляющие любого спектра, как правило, весьма изменчивы. Если мы обнаружим устойчивость этих характеристик на достаточно большой последовательности временного ряда младшего бита, то эти характеристики возможно использовать для идентификации аппаратуры звукозаписи.

Выделение самоподобных структур, являющихся следствием характеристик младшего бита звукового файла, на основе стандартных методов вейвлет-преобразований не является достаточно эффективным.

Для дальнейшего еще раз подчеркнем, что нас будут интересовать лишь высокочастотные паттерны, самоподобные структуры в младшем бите звукового файла.

На Рис.2., Рис.3. приведены характерные фрагменты изменения величин в младших битах 16-ти разрядных звуковых файлов формата wav.

Рис. 2. Фрагмент изменения величины младшего (16-го) бита звукового файла

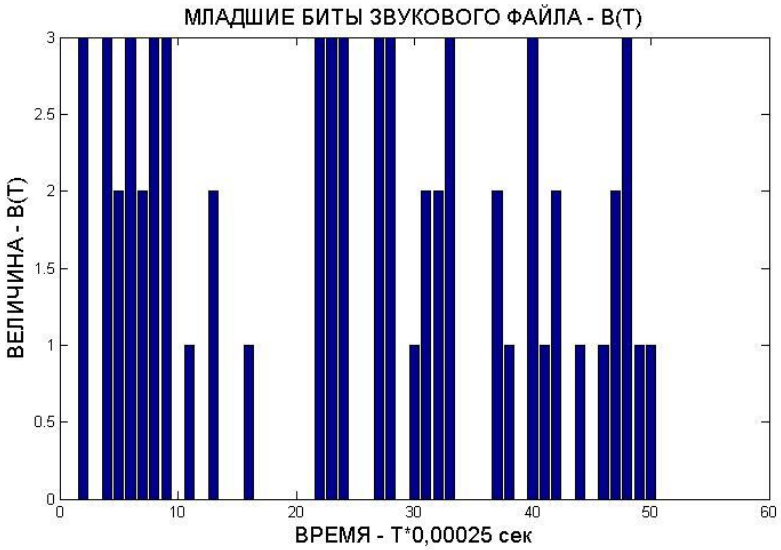

Рис. 3. Фрагмент изменения величины двух младших (15+16-й) бит звукового файла.

Сложность постановки задачи состоит, кроме прочих причин, также в том, что визуально наблюдаемые паттерны бит (сгустки и разрежения на графике) могут оказаться вовсе и не повторяющимися устойчивыми самоподобными структурами и закономерностями. Это могут быть чисто случайные последовательности бит. Таким образом, априори неизвестно ни факт наличия подобных закономерностей, ни их характер. Необходимо применение рациональной математической модели для описания и выявления этих мультифрактальных образований. Что собственно, при наличии достаточной статистики на большом фактическом материале и может служить доказательством их существования в младших битах цифровых звуковых файлов.

Специфика величин в младших битах звуковых файлов – это целые числа малой величины, существенно усложняет прямое применение вейвлет-анализа. Практика показывает, что описание чередующихся нулей и единиц на основе, существующих вейвлетных базисов, малоэффективно. Так, на рис.4. приведен характерный вейвлет-портрет

для фрагмента младшего бита звукового файла (wav. формат). Для анализа использовался базис Хаара, как базиса имеющего наибольшее сродство к подобным образованиям.

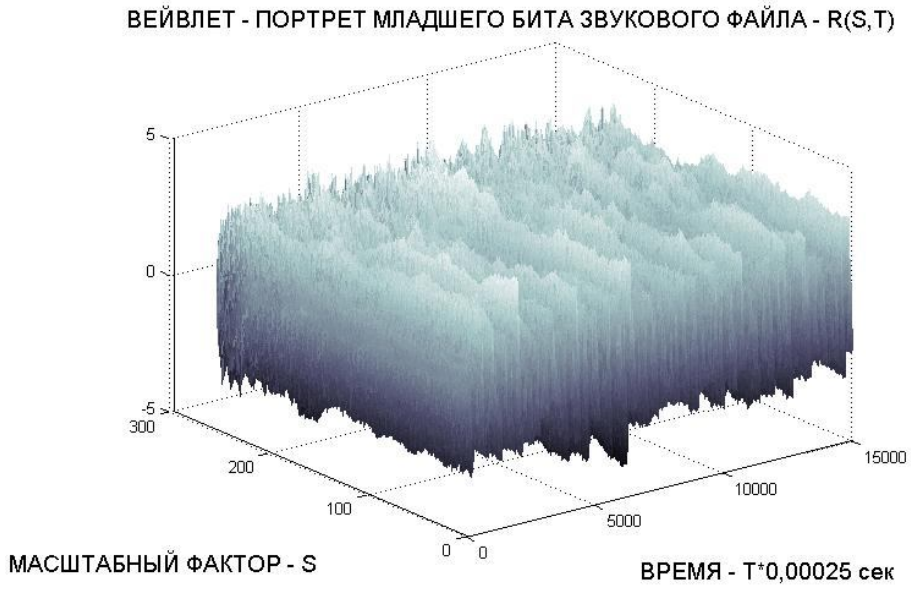

Рис. 4. Вевлет-портрет младшего бита звукового файла. (базис Хаара)

Спектр (в высокочастотной области) практически равномерно распределен различными масштабными составляющими. Однако, это ни в коей мере не говорит, как будет показано далее, об отсутствии мультифрактальных образований. Возможность применения для анализа и выделения самоподобных структур иных вейвлетных базисов дает аналогичные результаты. И все же устойчивые высокочастотные самоподобные структуры в младших битах звуковых файлов существуют. Выделим ряд произвольных структур битовых последовательности, например, одного младшего бита вида:

1 0 0 1 1 1 0 0 1 0 1 1

Это совершенно случайная последовательность бит в 16-ом разряде звукового файла, но подобранная специальным образом.

Легко подсчитать, какова вероятность встретить такую последовательность в случайном нормально распределенном стохастическом процессе – это 2 в степени 12. Если выбрать достаточно представительный фрагмент звукового файла, то легко подсчитать математическое ожидание выявления определенного количества таких фрагментов на данном интервале. На Рис.5. представлены графики зависимостей количества таких разных специально подобранных случайных последовательностей бит от номера фрагмента для случайного нормально распределенного идеального процесса типа белого шума и реального фрагмента звукового файла. Номера случайных последовательностей характеризуют последовательности расположенные в порядке возрастания числа бит. Выбор специальных последовательностей бит является предметом отдельной математической модели.

Как показывают статистические оценки отличие этих кривых статистически значимо. Массовые исследования показывают, что подобная ситуация характерна для 95% звуковых файлов. При этом для более чем 90% таких файлов характер приведенных кривых для отдельно выбранного файла близок друг к другу и существенно отличается от теоретической кривой случайных нормально распределенных последовательностей..

Массовые исследования 16-ти разрядных звуковых файлов wav – формата показывают наличие существенного количества высокочастотных битовых структур “специального вида”, количество которых в различных фрагментах одного и того же файла существенно отличается от случайного. При этом наблюдаются устойчивые закономерности в распределении таких структур по одному и тому же звуковому файлу. Этот факт является свидетельством наличия самоподобных мультифрактальных образований в младшем бите звуковых файлов. Эти образования возможно соотнести со статистическими характеристиками младших бит, которые являются следствием скрытых статистических закономерностей в АЦП.

Возникает естественный вопрос – почему вейвлет-преобразования для различных рациональных базисов не выявляют эти структуры. Причина кроется в сочетании нескольких факторов и свойств существующих вейвлетных базисов, которые негативно сказываются на эффективности выявления мультифракталов битовых структур.

Первое – мультифрактальные образования в младших битах звуковых файлов представляют собой последовательность малых целых чисел, которые имеют “слабое сродство” практически с любым вейвлетным базисом.

Второе – необходимая ортогональность вейвлет базисов, которая позволяет разложить сигнал на независимые в физическом смысле образования различной размерности. Характер высокочастотных самоподобных структур в младших битах звуковых файлов в сочетании с малостью целых чисел плохо укладывается в концепцию ортогональности. Это “маленькие островки - патерны” между которыми “пустыня”, в которой нет ничего интересного с точки зрения рассматриваемых задач. Естественно выделить эти “особенности”, используя вейвлет – преобразование, чрезвычайно тяжело.

Необходимая совокупность базовых обьектов, которая эффективно выявляет высокочастотные мультифрактальные образования в младших битах звуковых файлов должна учитывать характерные особенности последовательностей младших бит.

Предположим, что в младшем бите звукового файла с нерегулярной периодичностью генерируются “патерны” в виде близких по структуре (но не идентичных) повторяющихся нулей и единиц. Эти патерны генерируются случайным процессом (но не белым шумом). Этот процесс имеет определенные закономерности, внешним проявлением которых и являются рассматриваемые патерны. Описание этих самоподобных структур, как мультифракталов, в стандартном виде вряд ли целесообразно. Имеется в виду, то, что мультифракталы могут быть приближенно получены друг из друга путем аффинных преобразований. В данном случае – сжатий и растяжений по битовой оси, путем перемещения и изменения числа бит. Очевидно, что напрямую подобный механизм самопообия вряд ли может быть полезен для математических расчетов. Необходим какой либо базис, с большим сродством к последовательности бит. Этот базис должен позволить решить две задачи.

Первая – классификация патерн по какому-то признаку с целью построения статистических кривых для анализа возможных закономерностей отклонения от случайности.

Вторая – соответствовать нашим физическим представлениям о характере самоподобных структур-паттерн.

При выявлении битовых сочетаний накладывать определенные требования в рамках рассматриваемых задач на взаимнообратное разложение последовательности бит по этому базису или требования ортогональности не имеет смысла (да и вряд ли возможно в рамках сравнительно простых математических абстракций).

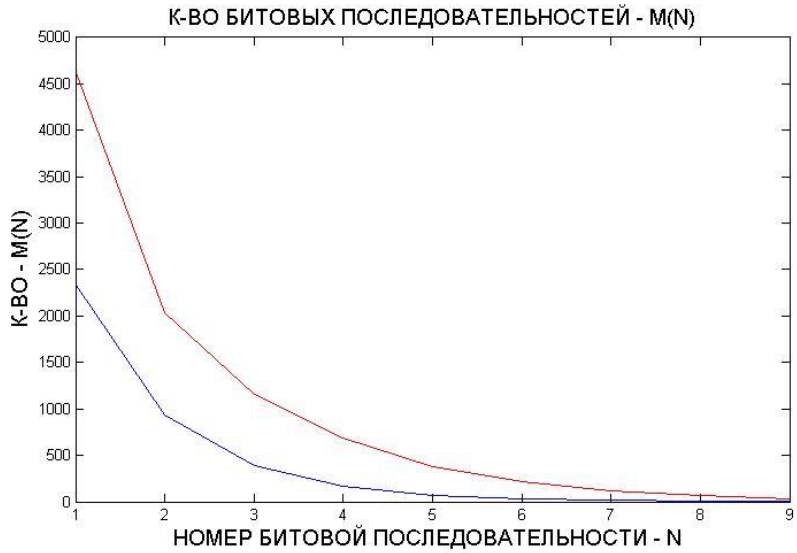

Рис. 5. Распределение битовых последовательностей
(верхняя кривая соответствует фрагменту звукового файла, нижняя –
теоретическая для последовательности случайно распределенных бит)

Одну из возможностей построения подобного базиса подсказывает теория симметрий и групп. Будем рассматривать паттерны, как отклонения от различных определенным образом классифицированных симметричных битовых структур. Так, например,:

1 0 0 1 (1)

1 1 0 1 1 (2)

Это симметричные относительно центра симметрии битовые образования.

В качестве этих структур возможно использовать для формального описания, например, – симметричные многочлены . Эти многочлены степени n эквивалентны битовым последовательностям с нулями и единицами.

Так, например, последовательность бит

1 0 0 1 0 0 1 (3)

эквивалентна симметричному многочлену

$$X^6 + X^3 + 1 \quad (4)$$

В качестве абстрактной модели приймем модель по которой случайный процесс генерирует симметричные структуры, добавляя к ним случайные (нессиметричные) биты.

Например,

1 0 0 1 1 0 1 (5)

Последовательность бит (5) отличается от последовательности (3) одним битом.

Выделим в одну группу самоподобные структуры для конкретного симметричного многочлена, отличающиеся на несколько бит (не более двух, трех, в зависимости от многочлена) - расстояние Хэмминга для этой группы. Далее будем выбирать последовательные во времени отрезки младшего бита и рассчитывать на определенном интервале число попаданий отрезков бит в определенную группу. Кривая распределения числа элементов в группе по номеру группы будет являться статистической характеристикой распределения паттерн в младшем бите в рамках предлагаемой модели.

Важно отметить, что при такой математической концепции с применением определенного множества симметричных полиномов с фиксированной максимальной степенью, возможно некоторое пересечение характеристик для различных симметричных полиномов. В частности, стмметричный полином может раскладываться на несколько также

симметричных полиномов. С физической точки зрения это приведет к некоторому “дублированию” подсчетов при построении статистических кривых.

С целью снижения влияния этого эффекта возможно среди симметричных полиномов выбирать неприводимые полиномы. Данный подход не является строгим математическим решением рассматриваемой задачи. Это эвристический подход. Однако, он необходим для повышения эффективности анализа статистических закономерностей, и как следствие снижения вероятности ошибок принятия решений.

Необходимо отметить также пути построения более строгой математической концепции в рамках данного анализа. Логически последовательный анализ этой задачи требует введения, например, группы Галуа, в рамках которой возможно полностью формализовать рассматриваемые выше операции. Однако, при таком уровне абстракции существенным образом теряется не только физический смысл задачи, но как показывают некоторые оценки и последующая эффективность решений.

Дело в том, что самоподобные битовые структуры в виде различных аффинных преобразований физического растяжения, сжатия бит теряются и урезаются в конечной Группе Галуа (например при умножении неприводимых полиномов). В данном случае умножение сущностей сверх необходимого нецелесообразно. Рассмотренная концепция принципиально решает задачу определения распределения самоподобных структур в младшем бите звукового файла.

На основании описанной концепции разработано программное обеспечение, которое выявляет и исследует особенности фрактального построения шумов сигналограмм, позволяющее производить идентификацию аппаратуры их формирования для оценки их оригинальности. Пример итогового отчета представлен на рис.6.

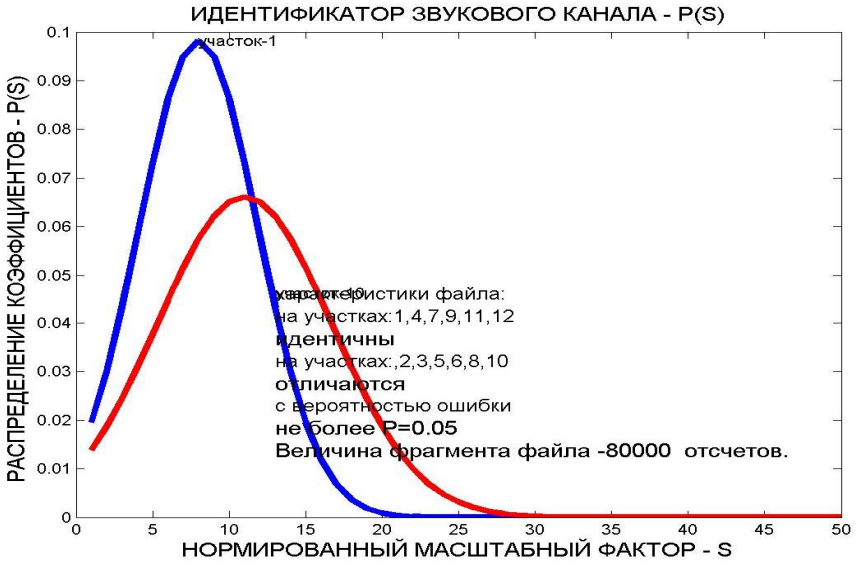

Рис. 6. Результаты анализа сигналограммы, скомпилированной из файлов записей на встроенных диктофонах мобильных телефонов Nokia-6303, Nokia-6300, LG KM330, Nokia-6275, диктофоне Panasonic RR-US360 и встроенном диктофоне мобильного телефона телефона Nokia-6303, записаных с частотою дискретизации 8 кГц, фрактальном масштабе 500, разбиты на фрагменты 80000 с вероятности ошибки P = 0,05

При проведении исследований относительно пригодности использования и апробации разработанного програмного обеспечения установлено, что использование программы позволяет выявлять следы цифровой обработки в сигналограммах.

Таким образом, разработана теоретическая концепция позволяющая призводить идентификацию подлинности сигналограм на основе анализа фрактальных структур, присутствующих в них. В качестве дальнейших исследований необходимо изучения особенностей выявленных закономерностей в оценке подлинности цифрового сигнала.

Список литературы

10. *Рыбальский О.В.* К вопросу о фрактальности аналоговых сигналов, подвергнутых цифровой обработке // Вісник Східноукраїнського національного університету ім В. Даля. – Луганськ, 2006, № 9, ч. 1. – С. 21–25.

11. Командина Т.В., Соловьев В.И. Идентификация звукового устройства по статистическим характеристикам звукового файла // Вісник Східноукраїнського національного університету ім. В. Даля. – Луганськ, № 6, ч.1, 2009. – С. 169 – 172.

12. *Кобозева А.А., Рыбальский О.В., Струк И.А., Трифонова Е.А* Комплексный подход к экспертизе подлинности материалов цифровой звукозаписи // Вісник Східноукраїнського національного університету ім. В. Даля. – Луганськ, № 6, ч.1, 2009. – С. 75 – 78.

Поступила 17.02.2010

УДК 003.26:004.056.55:621.39 **Корченко О.Г., Гнатюк С.О., Васько О.В., Козирев С.П.**

КВАНТОВО-КРИПТОГРАФІЧНА СИСТЕМА З БЕЗУМОВНОЮ СТІЙКІСТЮ

Вступ

На даному етапі розвитку інформаційного суспільства все гостріше постає питання захищеності інформаційних ресурсів. Інформаційна безпека є однією із ключових складових національної безпеки. Із розвитком інформаційних технологій невпинно розвиваються і методи захисту інформації, однак, ще стрімкіше розвиваються методи несанкціонованого доступу до інформації. Це одвічне протистояння продовжується вже багато сотень років і з подальшим розвитком науки й техніки ставатиме все гострішим. Не є секретом і те, що стійкість математичних алгоритмів шифрування інформації (таких як DES, AES, RSA) – це всього лише питання часу і, з винайденням квантового комп'ютера, дані алгоритми шифрування будуть неактуальними і неефективними [1]. Отже, можна зробити припущення, що майбутнє криптографічної науки за квантовою криптографією. На даний момент відомо два основні напрямки квантової криптографії: квантовий прямий безпечний зв'язок (КПБЗ) та квантовий розподіл ключів (КРК) [2]. У протоколах КПБЗ легітимні користувачі (Аліса і Боб) взагалі не використовують шифрування, а передають інформацію шляхом кодування повідомлення за допомогою квантових станів фотонів. Протоколи КРК призначені для розподілу ключів шифрування між легітимними користувачами по квантовому каналу зв'язку.

Аналіз останніх досліджень

Проаналізувавши останні дослідження в даній галузі, можна зробити висновок про недосконалість і невисоку криптостійкість багатьох запропонованих систем. У більшості проаналізованих наукових публікацій [3-9] вирішується проблема розподілу ключів за допомогою систем КРК. Однак, будь-яка система шифрування з використанням КРК стійка на стільки, на скільки стійкий сам ключ. У статті [5] подано чіткий аналіз квантових технологій і методів захисту інформації, а також обумовлено переваги та недоліки кожного з квантових методів. У роботі [4] йдеться про те, що існує ще ряд невирішених проблем в