

динаміці загальної кількості зареєстрованих злочинів по роках за даними Департаменту інформаційних технологій МВС України.

Виявлено, що найбільше повідомлень про резонансні злочини у 2002-2004 роках надходило в 2-х місяцях року, а саме, у квітні та у вересні-жовтні.

Список літератури:

1. Кудинов В.А., Рыбалко Т.В. Автоматизированное рабочее место дежурного дежурной части МВД-УМВД(УМВДТ): Метод. рекомендации. – К.: РИО МВД Украины, 1996. – 100 с.
2. Кудинов В.А. Проблеми функціонування автоматизованого робочого місця чергового чергової частини в органах внутрішніх справ України // Матеріали Міжвузівської науково-практичної конференції "Сучасні проблеми інформатизації органів внутрішніх справ України" (м. Київ, 15 березня 2001 р.). – К.: НАВСУ. – 2002. – С. 47-51.
3. Кудинов В.А., Рыбалко Т.В. Автоматизированная система "Заявление" // Бюллетень по обмену опытом работы МВД Украины. – 1994. – № 115. – С. 43-47.
4. Кудинов В.А. Структура бази даних автоматизованої інформаційної системи "Зведення" з обліку злочинів та надзвичайних подій, які взяті на контроль МВС України // Науково-технічний вісник "Безпека дорожнього руху України". – 2003. – № 1-2 (15). – С. 57-62.
5. Наказ МВС України від 4 жовтня 2003 року № 1155 "Про вдосконалення реагування на повідомлення про злочини, інші правопорушення і події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України".
6. Кудинов В.А. Автоматизированный контроль качества и своевременности оперативного информирования МВД Украины // Науково-технічний вісник "Безпека дорожнього руху України". – 1999. – № 3 (4). – С. 131-134.
7. Кудинов В.А. Програми контролю достовірності та попередньої обробки інформації бази даних АІС "Зведення" з обліку резонансних злочинів та інших надзвичайних подій МВС України // Науково-технічний журнал "Реєстрація, зберігання і обробка даних". – 2005. – Т. 7, № 1. – С. 80-88.
8. Кудинов В.А. Програма формування статистичної довідки про контрольні злочини та надзвичайні події Чергової частини МВС України // Науково-технічний вісник "Безпека дорожнього руху України". – 2002. – № 1 (12). – С. 103-106.
9. Кудинов В.А. Програма формування довідки про розкриття злочинів, які взяті на контроль МВС України // Науково-технічний вісник "Безпека дорожнього руху України". – 2002. – № 2 (13). – С. 125-129.
10. Наказ МВС України від 30 червня 2002 р. № 635 "Про заходи щодо організації проведення науково-дослідних робіт та впровадження їх результатів у практичну діяльність органів внутрішніх справ України".
11. Аналітичні матеріали "Стан правопорядку в Україні. Основні результати діяльності органів внутрішніх справ у 2003 році". – К.: Головний штаб МВС України. – 2004. – 31 с.
12. Аналітичні матеріали "Стан правопорядку в Україні, результати діяльності органів внутрішніх справ за 2004 рік, основні проблеми, прогноз". – К.: Головний штаб МВС України. – 2005. – 33 с.

УДК 621.317.799 297 + 681.849

О.В.Рыбальский

ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ВЫЯВЛЕНИЯ СЛЕДОВ ЦИФРОВОЙ ОБРАБОТКИ ФОНОГРАММ И ОСОБЕННОСТИ ЕЕ ПРОГРАММНОЙ И МЕТОДИЧЕСКОЙ РЕАЛИЗАЦИИ В ЭКСПЕРТИЗЕ МАТЕРИАЛОВ И СРЕДСТВ ВИДЕОЗВУКОЗАПИСИ (ЧАСТЬ 1)

Введение

В течение ряда лет в Национальной академии внутренних дел Украины (НАВДУ) разрабатывались основы теории выявления следов цифровой обработки аналоговых и цифровых фонограмм, необходимой для создания методов и средств экспертной проверки их оригинальности и подлинности. В результате проведенных исследований была разработана теоретическая база [1–6], а на ее основе – методы и средства контроля фонограмм, внедренные в экспертную практику [7–9]. Созданные способы и аппаратура для проведения экспертиз уникальны, они защищены долгосрочными патентами на изобретения и авторскими свидетельствами [10–14].

Целью статьи является ознакомление широкого круга специалистов в области защиты информации, криминалистической науки и экспертной практики с особенностями использования новых методов и средств проверки аутентичности сигналограмм. Эти методы и оборудование отвечают существующему уровню угроз целостности информации, содержащейся в сигналограммах, производимых посредством внешних вмешательств с использованием цифровых технологий.

Основная часть

Теория выявления следов цифровой обработки фонограмм первоначально содержала аналитически доказанные и экспериментально проверенные следующие положения:

Факт невозможности гарантированного выявления¹ следов цифровой обработки в фальсифицированных фонограммах известными методами, используемыми в широкой экспертной практике.

Тезис 1. Вероятность совпадения частот дискретизации устройств, участвующих в процессе цифровой обработки сигналограммы, ничтожно мала.

Тезис 2. Вероятность совпадения уровней квантования с технологическими дефектами квантователей устройств, участвующих в процессе цифровой обработки сигналограммы, ничтожно мала.

Концепция. Внешние вмешательства и модификация информации, содержащейся в цифровой сигналограмме, возможны только при условии использования не менее двух различных цифровых устройств.

Гипотеза 1. При проверке аутентичности цифровых сигналограмм следует использовать сигналы, воспроизводимые на аналоговом выходе цифровой аппаратуры записи аналоговых сигналов.

Гипотеза 2. Следы цифровой обработки стгналограммы проявляются в виде искажений формы и, следовательно, спектра аналоговых сигналов, получаемых при воспроизведении на аналоговом выходе аппаратуры записи аналоговых сигналов сигналограммы, обработанной в цифровой форме.

Гипотеза 3. В спектре обработанного в цифровой форме аналогового сигнала, при использовании для монтажа сигналограммы операции стробирования фрагментов с целью их последующей компиляции, появляются искажения, обусловленные влиянием стробирующего сигнала.

Гипотеза 4. Реализация средств гарантированного выявления искажений формы и спектра обработанных сигналов, содержащихся в фонограмме, при использовании время-частотного анализатора, построенного на классическом кратковременном преобразовании Фурье, технически невозможна.

Гипотеза 5. Реализация средства гарантированного выявления искажений формы и спектра обработанных сигналов, содержащихся в сигналограмме, обеспечивается применением микроволнового время-частотного анализа. Для построения такого анализатора целесообразно использовать комплексную функцию Морле.

Закономерность неизбежного увеличения числа искажений формы и

¹ Под гарантированным выявлением следов цифровой обработки сигналограмм мы понимаем достаточность разрешающей способности используемых для этого методов и средств

спектральних компонент, виділених із сигналів, воспроизведених з обробленої в цифровій формі сигналограми, відносно числа цих искажень і компонент, виділених із аналогових сигналів, воспроизведених з сигналограми, не піддавшійся такій обробці.

Ця закономірність прийнята в якості **інформативного признака** слідів цифрової обробки фонограмм.

Гіпотеза 6. Гарантоване виявлення слідів цифрової обробки сигналограмм забезпечується порівнянням еквівалентів спектрограмм, отриманих із вейвлет-портретів стаціонарних сигналів, виділяються із інформації, що міститься в зразковій і порівнюваних сигналограмах.

Ця гіпотеза після її експериментального підтвердження була прийнята в якості **метода** перевірки автентичності сигналограмм. Для її реалізації був розроблений спеціалізований програмний продукт – програма "Академія", що входить до складу апаратно-програмного комплексу "Теорема-1", призначеного для перевірки автентичності аналогових і цифрових фонограмм.

Після аналітичної перевірки і експериментального підтвердження тезисів, концепції, гіпотез і закономірностей, загальні положення теорії можуть бути розділені на теоретичні і практичні і викладені в наступній редакції:

Теоретичні положення:

Положення 1. Гарантоване виявлення слідів цифрової обробки в фальсифікованих фонограмах відомими методами, що використовуються в широкій експертній практиці, неможливо.

Положення 2. Вероятність збігу частот дискретизації пристроїв, що беруть участь у процесі цифрової обробки сигналограмм, незначально мала.

Положення 3. Вероятність збігу рівнів квантування з технологічними дефектами квантувачів пристроїв, що беруть участь у процесі цифрової обробки сигналограмм, незначально мала.

Положення 4. Зовнішні втручання і модифікація інформації, що міститься в цифровій сигналограмі, можливі тільки за умови використання не менше двох різних цифрових пристроїв.

Положення 5. Слідів цифрової обробки сигналограмм проявляються у вигляді искажень форми і, відповідно, спектра аналогових сигналів, що отримуються при воспроизведенні на аналоговому виході апаратури запису аналогових сигналів сигналограмм, оброблених в цифровій формі.

Положення 6. У спектрі обробленого в цифровій формі аналогового сигналу, при використанні для монтажу сигналограмм операції стробування фрагментів з метою їх наступної компіляції, виникають искаження, що обумовлені впливом стробуючого сигналу.

Положення 7. Реалізація засобів гарантованого виявлення искажень форми і спектра оброблених сигналів, що містяться в фонограмі, при використанні час-частотного аналізатора, побудованого на класическому кратковременному перетворенні Фур'є, технічно неможливо.

Положення 8. Реалізація засобів гарантованого виявлення искажень форми і спектра оброблених сигналів, що містяться в сигналограмі, забезпечується застосуванням мікрохвильового час-частотного аналізу. Для побудови такого аналізатора цілесообразно використовувати комплексну функцію Морле.

Положення 9. Джерелами виникнення искажень форми і спектра сигналів при цифровій обробці фонограмм є:

– невідповідність розміщення на статическій характеристиці квантувачів рівня аналого-цифрових і цифро-аналогових перетворювачів (АЦП і ЦАП відповідно) різних пристроїв, що беруть участь у процесі обробки, рівнів квантування з технологічними дефектами;

– расхождение истинных значений частот тактовых генераторов устройств, участвующих в процессе обработки;

– использование операции стробирования для вырезания фрагментов фонограммы при монтаже методом компиляции нового целого из вырезанных фрагментов ("сшивки") в ПЭВМ;

– возникновением информационных потерь при преобразовании форматов представления информации, используемых при обработке сигналов в ПЭВМ и их записи на цифровую аппаратуру записи аналоговых сигналов [1–9].

Правила для практического применения теории при проведении экспертизы аутентичности фонограмм:

Правило 1. При проверке аутентичности цифровых сигналограмм следует использовать сигналы, воспроизводимые на аналоговом выходе цифровой аппаратуры записи аналоговых сигналов.

Правило 2. Информативным признаком следов цифровой обработки фонограмм является **закономерность** неизбежного увеличения числа искажений формы и спектральных компонент, выделенных из сигналов, воспроизведенных с обработанной в цифровой форме сигналограммы, относительно числа этих искажений и компонент, выделенных из аналогичных сигналов, воспроизведенных с сигналограммы, не подвергавшейся такой обработке.

Правило 3. Методом гарантированного выявления следов цифровой обработки фонограмм является метод сравнения эквивалентов спектрограмм, полученных из вейвлет-портретов стационарных сигналов, выделяемых из информации, содержащейся в образцовой и проверяемой сигналограммах.

Применение данного метода позволяет обойти необходимость сравнения двух нестационарных процессов, и, таким образом уйти от вероятностной формы получения результатов экспертизы.

В НАВДУ была отработана первоначальная методика проведения экспертиз с использованием программы "Академия". В процессе проведения ряда экспертиз программа и методика совершенствовались.

Программа "Академия" построена на вейвлет-анализе сигналов. В ней используется комплексная неортогональная вейвлет-функция Морле. Выбор этого вейвлета обусловлен рядом факторов, имеющих для выявления следов цифровой обработки фонограмм важное значение.

Во-первых, этот вейвлет сконструирован из колокольного импульса (гауссиана) и, в соответствии с известным принципом неопределенности Гейзенберга, имеет наилучшее произведение эффективной ширины импульса на эффективную ширину спектра. Действительно, вейвлет-функция Морле во временной области записывается как

$$\psi(t) = \pi^{-\frac{1}{4}} \left(e^{j\xi_0 t} - e^{-\frac{\xi_0^2}{2}} \right) e^{-\beta^2 t^2} = \pi^{-\frac{1}{4}} \left(e^{j\omega_c t} - e^{-\frac{\omega_c^2}{2}} \right) e^{-\frac{t^2}{2}}, \quad (1)$$

где

$$\beta = \frac{1}{\sqrt{2}},$$

ω_c – частота гетеродинамирования гауссиана (носитель).

Из (1) видно, что этот вейвлет содержит гауссиан. Известно [15], что эффективная ширина импульса для гауссиана

$$T_3 = \frac{1}{2\beta}, \quad (2)$$

а эффективная ширина спектра

$$P_{\vartheta} = \frac{\beta}{2\pi}. \quad (3)$$

Из принципа Гейзенберга вытекает, что для импульса любой формы

$$T_{\vartheta} \cdot P_{\vartheta} \geq \frac{1}{4\pi} \quad (\text{при размерности в герцах}) \quad (4)$$

или

$$T_{\vartheta} \cdot P_{\vartheta} \geq \frac{1}{2} \quad (\text{при размерности в рад/сек}) \quad (5)$$

Т.е. для любой формы импульса произведение эффективной ширины импульса на эффективную ширину спектра не может быть меньше величин, указанных в (4) и (5). При этом только для гауссиана это неравенство переходит в равенство.

Следовательно, для принятого в гауссиане значения $\beta = \frac{1}{\sqrt{2}}$, произведение эффективной ширины импульса на эффективную ширину спектра составит:

– для размерности в герцах

$$T_{\vartheta} \cdot P_{\vartheta} = \frac{1}{2\beta} \cdot \frac{\beta}{2\pi} = \frac{1}{4\pi}; \quad (6)$$

– для размерности в рад/сек

$$T_{\vartheta} \cdot P_{\vartheta} = \frac{2\pi}{2\beta} \cdot \frac{\beta}{2\pi} = \frac{1}{2}. \quad (7)$$

Для импульсов любой другой формы это значение будет большим, что свидетельствует о наилучшей избирательной способности вейвлета, построенного на гауссиане, как во временной, так и в частотной области.

Во-вторых, комплексность вейвлета Морле позволяет использовать вейвлет-портрет аргумента сигнала для построения эквивалента спектрограммы, сохраняющей все положительные свойства вейвлет-анализа и удобной (в отличие от вейвлет-портрета) при интерпретации и иллюстрации результатов экспертных исследований фонограмм [7–9].

Выводы

1. Подведены итоги разработки теории, методов и средств выявления следов цифровой обработки фонограмм.

2. Показана оптимальность вейвлета Морле, выбранного при построении программы "Академия", используемой в аппаратно-программном комплексе "Теорема-1", предназначенного для выявления следов цифровой обработки аналоговых и цифровых фонограмм при экспертизе их аутентичности.

Список литературы:

1. Рыбальский О.В., Жариков Ю.Ф. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе. – К.: НАВСУ, 2003. – 300 с.
2. Рибальський О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі. – К.: НАВСУ, 2004. – 167 с.
3. Рибальський О.В. До основ теорії виявлення слідів цифрової обробки фонограм // Зб. наук. пр. Військового інституту телекомунікацій та інформатизації НТУУ "КПІ". – К. –2004. – № 4. – С. 129–138.
4. Рыбальский О.В. К экспериментальной проверке достоверности положений теории выявления следов цифровой обработки фонограмм // Реєстрація, зберігання та обробка даних. – К. – 2004. – Т.6, № 3. – С. 85–98.
5. Рыбальский О.В. К основам теории выявления следов цифровой обработки

фонограмм // Защита информации. Сб. трудов НАУ. – К.: КМУЦА, 2004. – Вып. 11. – С. 50–56.

6. Рыбальский О.В. Анализ возможных цифровых и аналоговых способов подделки фонограмм и требований к анализаторам для выявления их следов // Захист інформації. – К.: КМУЦА, 2004. – Спеціальний випуск. – С. 44–48.

7. Рыбальский О.В. Метод получения графиков текущих спектров сигналов из их вейвлет-портретов // Захист інформації. – К.: КМУЦА. – 2004. – № 1. – С. 51–56.

8. Рыбальский О.В. Выбор направлений разработки методов и средств выявления следов цифровой обработки фонограмм // Захист інформації. – К.: КМУЦА. – 2004. – № 2. – С. 51–54.

9. Рыбальский О.В. Программа для выявления следов цифровой обработки аналоговых и цифровых фонограмм при проведении судебно-акустической экспертизы // Реєстрація, зберігання і обробка даних. – К. – 2003. – Т. 5, № 3. – С. 50–56.

10. Пат. 60403 України, МКВ G 11 b 27/00, 27/36. Спосіб перевірки автентичності цифрових сигналів: Пат. 60403 України, МКВ G 11 b 27/00, 27/36 Рыбальський О. В., Жаріков Ю.Ф. (Україна); НАВСУ. – № 2002031835; Заявл. 05.03.02; Опубл. 15.10.03, Бюл. № 10.

11. Пат. 54627 України, МКВ G 11 b 27/00, 27/36. Спосіб ідентифікації цифрової апаратури запису аналогових сигналів та перевірки автентичності цифрових сигналів: Пат. 54627 України, МКВ G 11 b 27/00, 27/36 Рыбальський О.В., Жаріков Ю.Ф., Орлов Ю.Ю., Геранін В.О., Писаренко Л.Д., Мовчан Т.В., Кирюша Б.А. (Україна); НАВСУ. – № 2001129156; Заявл. 28.12.01; Опубл. 17.03.03, Бюл. № 3.

12. Пат. 27207 України, МКВ G 11 b 27/00, 27/36. Спосіб перевірки оригінальності та автентичності магнітних фонограм: Пат. 27207 України, МКВ G 11 b 27/00, 27/36 Рыбальський О.В., Жаріков Ю.Ф., Орлов Ю.Ю. (Україна); НАВСУ. – № 99084533; Заявл. 09.08.99; Опубл. 15.08.00, Бюл. № 3.

13. Пат. 73631 України, МКВ G 11 b 27/00, 27/36. Спосіб виявлення слідів цифрової обробки аналогових і цифрових сигналів: Пат. 73631 України, МКВ G 11 b 27/00, 27/36 Рыбальський О.В., Геранін В.О., Жаріков Ю.Ф., Орлов Ю.Ю., Волкович С.Л., Струк І.О. (Україна); НАВСУ. – № 2003076921; Заявл. 22.07.03; Опубл. 15.08.05, Бюл. № 8.

14. Свідоцтво № 11088 про реєстрацію авторського права на твір. Комп'ютерна програма "Академія". Рыбальський О.В., Волкович С.Л. (Україна); Рыбальський О.В. – № 10986; Заявл. 26.07.2004; Опубл. 17.09.2004.

15. Добеши И. Десять лекций по вейвлетам. – М.- Ижевск: Dynamica, 2001. – 463 с.

УДК 535.39

В.В. Козловский

АНАЛИЗ ЦЕПИ УТЕЧКИ ИНФОРМАЦИИ С ПЛАНАРНОГО ОПТОВОЛОКНА

В настоящее время в связи с интенсивным развитием волоконно-оптических линий связи (ВОЛС) существенно возрос интерес к вопросам защиты информации, передаваемой по оптоволокну. На сегодняшний день для анализа каналов утечки информации используется классическая модель диэлектрического волновода [1-3]. Анализ работ по волоконной оптике [4-7] и методам защиты информации [1,3] свидетельствует о том, что основными причинами утечки информации в оптическом диапазоне являются места ввода света в волновод (стыки), в результате чего в оптоволокну возникают моды излучения. Излучение света в местах стыка вызвано несовпадением геометрических (профиль поперечного сечения) и распределённых параметров (диэлектрическая и магнитная проницаемость) соединяемых волокон. Моды излучения представляют собой незатухающие в поперечном сечении или слабозатухающие колебания, которые существуют вне волокна. Моды излучения, как и направляемые моды, являются решениями уравнений Максвелла, имеющих непрерывный спектр собственных