Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Комп'ютерних наук
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)
магістр
(освітньо-кваліфікаційний рівень))

на тему: **Математичне та програмне забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації**

Виконав: студент (ка) 6 курсу, групи САм-61
спеціальності (напряму підготовки)
124 «Системний аналіз»
(шифр і назва спеціальності (напряму підготовки))

		Телев'як П.А.
	(підпис)	(прізвище та ініціали)
Керівник		Матійчук Л. П.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Мацюк О. В.
	(підпис)	(прізвище та ініціали)
Рецензент		Тиш Є. В.
	(підпис)	(прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Математичне та програмне забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації // Дипломна робота освітнього рівня "Магістр" // Телев'як Павло Анатолійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група САм-61 // Тернопіль, 2019 // С.–124, рис. – 25, табл. – 7, додат. – 2, бібліогр. джерел –57.

Методи дослідження базуються на принципах системного аналізу, апараті обчислювальної математики, методах логічного проектування і процедурної алгоритмізації, прийомах об'єктно-орієнтованого та логічного програмування.

Мета дослідження – розробка математичного та програмного забезпечення для виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації..

Дістав подальший розвиток алгоритм виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі з втратою інформації .

Вперше запропоновано за результатами обчислювального експерименту в якості порогового значення для відділення частини цифрового аудіо, що містить фальсифікацію від оригінальних частин, використовувати визначене значення 40.

Об'єктом дослідження є процес виявлення та локалізації фальсифікації цифрового аудіо-сигналу.

Предметом дослідження є методи та засоби вирішення задачі процесу виявлення фальсифікації цифрового аудіо-сигналу

Ключові слова: цифровий аудіо-сигнал, фальсифікація, локалізація, MATLAB.

ANNOTATION

Mathematical and software detection and localization of falsification of digital audio signal saved in the format with loss of information // Diploma work of educational level "Master" // Televyak Pavlo Anatolyevich // Ternopil National Technical University named after Ivan Pulyuy of Information Systems and Software Engineering, Department of Computer Science, Sam-61 group // Ternopil, 2019 // C. – 124, fig. - 25, tab. - 7, add. - 2, bibliography. sources –57.

Research methods are based on the principles of system analysis, the apparatus of computational mathematics, methods of logical design and procedural algorithmization, techniques of object-oriented and logical programming.

The purpose of the study is to develop mathematical and software for the detection and localization of falsification of digital audio signal stored in a lossy format.

The algorithm for detection and localization of falsification of digital audio signal saved in the format with loss of information was further developed.

For the first time, it was proposed to use the predetermined value of 40 as a threshold for separating a portion of digital audio containing falsification from the original parts.

The object of the study is the process of detecting and localizing digital audio tampering.

The subject of the research are methods and means of solving the problem of the process of detection of digital audio signal tampering

Keywords: digital audio, falsification, localization, MATLAB.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АЧХ - амплітудно-частотна характеристика

ЦА – цифрове аудіо

ЦЗ – цифрове зображення

ДКП – дискретне косинусне перетворення

ПБС – підблок сигналу

МПЗІ – методи пасивного захисту інформації

ЗМІСТ

ВСТУП

Розвиток сучасних технологій характеризується постійним зростом значення інформації, тому сьогодні не залишається сумнівів у необхідності забезпечення інформаційної безпеки. Необхідність збереження різних видів таємниць, забезпечення безпеки електронних документів та безпека самих працівників організації безпосередньо пов'язані з рівнем інформаційної безпеки.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності [5].

Початковий етап розвитку комп'ютерної безпеки тісно пов'язаний з криптографією. Зараз головні умови безпеки інформації – її доступність і цілісність. Іншими словами, користувач може в будь-який час зажадати необхідний йому набір сервісних послуг, а система безпеки повинна гарантувати при цьому його правильну роботу.

Будь-який файл або ресурс системи, при дотриманні прав доступу, повинен бути доступний користувачеві в будь-який час. Якщо якийсь ресурс недоступний, то він марний. Інше завдання захисту інформації – забезпечити незмінність інформації під час її зберігання або передачі. Це так звана умова цілісності.

Актуальність теми.

В сучасних умовах створення, зберігання та передачі інформації в електронному вигляді виникає можливість несанкціонованого доступу або модифікації цифрових сигналів, у тому числі цифрових аудіо (ЦА).

Це обумовлено бурхливим розвитком програмних засобів для редагування цифрових сигналів, які дають можливість змінювати цифрові аудіо, тим самим не лише порушуючи цілісність, але і фальсифікуючи його.

Під фальсифікацією будемо розуміти навмисне порушення цілісності цифрового аудіо-сигналу [7].

З відкритих джерел відомі деякі методи виявлення фальсифікації ЦА. Більшість з них заснована на аналізі особливостей технічного пристрою, на якому сигнал було створено, та відносяться до програмно-технічних методів пасивного захисту інформації.

Проте відомо, що переважними для використання є програмні методи пасивного захисту, які не потребують додаткової інформації для проведення перевірки цілісності сигналу.

Відомі також методи виявлення фальсифікації ЦА, що базуються на аналізі матриці нульових сингулярних чисел блоків (МНСЧБ), двовимірного горизонтального представлення цифрового аудіо сигналу.

До області застосування цих методів відносяться аудіо сигнали, що збережені у форматі без втрат інформації.

У зв'язку з цим задача виявлення фальсифікації цифрового аудіо, збереженого у форматі із втратою інформації, є актуальною, але невирішеною в повному обсязі, проблемою.

Зв'язок роботи з науковими програмами, планами, темами

Напрямок виконаних досліджень безпосередньо пов'язаний з науково-дослідним напрямком кафедри комп’ютерних наук Тернопільського національного технічного університету імені Івана Пулюя.

Мета і задачі дослідження

Метою дипломної роботи є удосконалення методики та практичних навиків виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

— провести аналіз існуючих методів перевірки цілісності цифрового аудіо-сигналу;

— провести адаптацію для цифрового аудіо-сигналу методу виявлення та локалізації фальсифікації цифрового зображення, заснованого на аналізі функції

середньоквадратичного відхилення значень коефіцієнтів дискретного косинусного перетворення (ДКП) матриці цифрового зображення від їх повторно відквантованих значень з різними коефіцієнтами квантування;

— визначити параметр, який може бути використаний для відділення частини цифрового аудіо, що містить фальсифікацію, від оригінальних частин;

— програмно реалізувати автоматизовану систему виявлення та локалізації фальсифікації для цифрового аудіо, збереженого у форматі із втратою інформації.

Об'єкт дослідження – процес виявлення та локалізації фальсифікації цифрового аудіо-сигналу

Предмет дослідження – математичне та програмне забезпечення процесу виявлення фальсифікації цифрового аудіо-сигналу

Методи дослідження – теоретичний аналіз і систематизація науково-теоретичних джерел, методи криптографії та захисту інформації, обробки сигналів та теорії чисел, мови програмування MATLAB.

Наукова новизна одержаних результатів.

Дістав подальший розвиток алгоритм виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі з втратою інформації .

Вперше запропоновано за результатами обчислювального експерименту в якості порогового значення для відділення частини цифрового аудіо, що містить фальсифікацію від оригінальних частин, використовувати визначене значення 40.

Практичне значення одержаних результатів.

Результати роботи можуть бути використані для вдосконалення комплексної системи захисту інформації на комерційному або державному підприємстві.

РОЗДІЛ І
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ФАЛЬСИФІКАЦІЇ ЦИФРОВИХ СИГНАЛІВ

1.1. Проблеми захисту інформації в комп'ютерних системах

У сучасних умовах масового поширення засобів електронної обчислювальної техніки та можливостей несанкціонованих дій над інформацією виникає необхідність захисту не тільки державної та військової, але й промислової, комерційної та фінансової таємниць. Захист інформації загалом й захист інформації в автоматизованих системах зокрема, стає усе актуальнішою й складнішою проблемою, для вирішення якої необхідна побудова загального системного комплексного підходу до захисту інформації. До недавнього часу комплексні системи захисту інформації були орієнтовані на захист інформації, що створюється, змінюється та передається безпосередньо у самій системі. Проте існування будь-якої системи неможливе без комунікації із зовнішнім середовищем та іншими системами [8,19].

Отже, захищеність інформації всередині системи залежатиме від достовірності інформації, що надходить до системи ззовні, що призводить до необхідності створення методів перевірки цілісності вхідної для системи інформації. Тому завдання виявлення фальсифікації цифрових сигналів загалом та цифрових зображень (ЦЗ) зокрема, є однією з найважливіших сьогодні завдань в області захисту інформації .

Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватися, і передаватися по каналах зв'язку. Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних.

При цьому сучасні швидкісні методи криптографічного перетворення дозволяють зберегти вихідну продуктивність автоматизованих систем.

Криптографічні перетворення даних є найбільш ефективним засобом забезпечення конфіденційності даних, їхньої цілісності і справжності. Тільки їх використання в сукупності з необхідними технічними та організаційними заходами можуть забезпечити захист від широкого спектру потенційних загроз. Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

· Перехоплення інформації - цілісність інформації зберігається, але її конфіденційність пошкоджена.

· Модифікація інформації - вихідне повідомлення змінюється або повністю замінюється іншим і відсилається адресату.

· Підміна авторства інформації. Потреби сучасної практичної інформатики привели до виникнення нетрадиційних завдань захисту електронної інформації, однією з яких є автентифікація електронної інформації в умовах, коли сторони, які обмінюються інформацією, не довіряють один одному. Ця проблема пов'язана зі створенням систем електронногоцифрового підпису. Технічною основою переходу в інформаційне суспільство є сучасні мікроелектронні технології, які забезпечують безперервне зростання якості засобів обчислювальної техніки і служать базою для збереження основних тенденцій її розвитку - мініатюризації, зниження електроспоживання, збільшення обсягу оперативної пам'яті (ОП) і місткості вбудованих накопичувачів, зростання продуктивності і надійності, розширення сфер і масштабів застосування.

Дані тенденції розвитку засобів обчислювальної техніки призвели до того, що на сучасному етапі захист комп'ютерних систем від несанкціонованого доступу характеризується зростанням ролі програмних та криптографічних механізмів захисту в порівнянні з апаратними.

Зростання ролі програмних і криптографічних засобів проявляється в тому, що виникають нові проблеми в галузі захисту обчислювальних систем від несанкціонованого доступу, які вимагають використання механізмів і протоколів з порівняно високою обчислювальною складністю і можуть бути ефективно вирішені шляхом використання ресурсів ЕОМ.

Однією з важливих соціально-етичних проблем, породжених все більш розширеним застосуванням методів криптографічного захисту інформації, є протиріччя між бажанням користувачів захистити свою інформацію і передачу повідомлень та бажанням спеціальних державних служб мати можливість доступу до інформації деяких інших організацій та окремих осіб з метою припинення незаконної діяльності [8].

Виникнення глобальних інформаційних мереж типу INTERNET є важливим досягненням комп'ютерних технологій, однак, з INTERNET пов'язана маса комп'ютерних злочинів [8,19].

Результатом досвіду застосування мережі INTERNET є виявлена слабкість традиційних механізмів захисту інформації та відставання у застосуванні сучасних методів. Криптографія надає можливість забезпечити безпеку інформації в INTERNET і зараз активно ведуться роботи із впровадження необхідних криптографічних механізмів в цю мережу. Не відмова від прогресу в інформатизації, а використання сучасних досягнень криптографії - ось стратегічно правильне рішення. Можливість широкого використання глобальних інформаційних мереж та криптографії є досягненням і ознакою демократичного суспільства.

Форсування процесу інформатизації вимагає адекватного забезпечення споживачів засобами захисту. Відсутність на внутрішньому ринку достатньої кількості засобів захисту інформації, що циркулює в комп'ютерних системах, значний час не дозволяло в необхідних масштабах здійснювати заходи щодо захисту даних.

Однією з важливих особливостей масового використання інформаційних технологій є те, що для ефективного вирішення проблеми захисту державного інформаційного ресурсу необхідно розосередження заходів щодо захисту даних серед масових користувачів. Інформація повинна бути захищена, в першу чергу там, де вона створюється, збирається, переробляється і тими організаціями, які несуть шкоду безпосередній при несанкціонованому доступі до даних. Цей принцип раціональний і ефективний: захист інтересів окремих організацій - це складова реалізації захисту інтересів держави в цілому [19].

Для надійного захисту інформації та виявлення випадків неправомірних дій проводиться реєстрація роботи системи: створюються спеціальні щоденники і протоколи, в яких фіксуються всі дії, пов'язані із захистом інформації в системі. Фіксуються час надходження заявки, її тип, ім'я користувача і терміналу, з якого ініціалізується заявка. При відборі подій, що підлягають реєстрації, необхідно мати на увазі, що зі зростанням кількості реєстрованих подій не може перегляд щоденника і виявлення спроб подолання захисту. У цьому випадку можна застосовувати програмний аналіз і фіксувати сумнівні події. Використовуються також спеціальні програми для тестування системи захисту. Періодично або у випадково вибрані моменти часу вони перевіряють працездатність апаратних і програмних засобів захисту [8].

До окремої групи заходів щодо забезпечення збереження інформації та виявлення несанкціонованих запитів відносяться програми виявлення порушень в режимі реального часу. Програми даної групи формують спеціальний сигнал при реєстрації дій, які можуть призвести до неправомірних дій по відношенню до інформації, що захищається. Сигнал може містити інформацію про характер порушення, місці його виникнення та інші характеристики. Крім того, програми можуть заборонити доступ до інформації, що захищається або симулювати такий режим роботи (наприклад, моментальна завантаження пристроїв введення-виведення), який дозволить виявити порушника і затримати його відповідною службою [19].

Один з поширених способів захисту - явне вказівку секретності виведеної інформації. У системах, що підтримують кілька рівнів секретності, вивід на екран терміналу або друкувального пристрою будь-якої одиниці інформації (наприклад, файлу, запису і таблиці) супроводжується спеціальним грифом із зазначенням рівня секретності. Ця вимога реалізується з допомогою відповідних програмних засобів [19].

В окрему групу виділено засоби захисту від несанкціонованого використання програмного забезпечення. Вони набувають особливого значення внаслідок широкого розповсюдження ПК.

1.2. Механізми забезпечення безпеки

Криптографія.

Для забезпечення секретності застосовується шифрування, або криптографія, що дозволяє трансформувати дані в зашифровану форму, з якої витягти вихідну інформацію можна тільки при наявності ключа.

Системам шифрування стільки ж років, скільки письмовою обміну інформацією. "Криптографія" в перекладі з грецької мови означає "тайнопис", що цілком відображає її первісне призначення. Примітивні (з позицій сьогоднішнього дня) криптографічні методи відомі з найдавніших часів і дуже тривалий час вони розглядалися скоріше як деякий хитрування, ніж сувора наукова дисципліна. Класичною завданням криптографії є оборотне перетворення деякого зрозумілого вихідного тексту (відкритого тексту) в уявну випадкової послідовність деяких знаків, звану шифртекст або криптограми.

При цьому шифр-пакет може містити як нові, так і наявні у відкритому повідомленні знаки. Кількість знаків у криптограмі і в початковому тексті в загальному випадку може відрізнятися. Неодмінною вимогою є те, що, використовуючи деякі логічні заміни символів в шифртекст, можна однозначно і в повному об'ємі відновити вихідний текст. Надійність збереження інформації в таємниці визначалося в далекі часи тим, що в секреті тримався сам метод перетворення [19].

Своїм перетворенням в наукову дисципліну криптографія зобов'язана потребам практики, породженим електронної інформаційної технологією. Пробудження значного інтересу до криптографії і її розвиток почався з XIX століття, що пов'язано із зародженням електрозв'язку. У XX столітті секретні служби більшості розвинених країн стали належить до цієї дисципліни як до обов'язкового інструменту своєї діяльності. В основі шифрування лежать два основних поняття: алгоритм і ключ [19].

Алгоритм - це спосіб закодувати початковий текст, в результаті чого виходить зашифроване послання. Зашифроване послання може бути інтерпретовано тільки за допомогою ключа.

Щоб уникнути можливих слабкостей, алгоритм шифрування може бути побудований на основі добре вивчених і апробованих принципах і механізмах перетворення. Жоден серйозний сучасний користувач не буде покладатися тільки на надійність збереження в секреті свого алгоритму, оскільки вкрай складно гарантувати низьку ймовірність того, що інформація про алгоритм стане відомою зловмисникові.

Секретність інформації забезпечується введенням в алгоритми спеціальних ключів (кодів). Використання ключа для шифрування надає дві суттєві переваги. По-перше, можна використовувати один алгоритм з різними ключами для відправки послань різним адресатам. По-друге, якщо секретність ключа буде порушена, його можна легко замінити, не змінюючи при цьому алгоритм шифрування. Таким чином, безпека систем шифрування залежить від таємності використовуваного ключа, а не від секретності алгоритму шифрування.

Багато алгоритмів шифрування є загальнодоступними. Кількість можливих ключів для даного алгоритму залежить від числа біт в ключі. Наприклад, 8-бітний ключ допускає 256 (2^{8}) комбінацій ключів. Чим більше можливих комбінацій ключів, тим важче підібрати ключ, тим надійніше зашифровано послання. Так, наприклад, якщо використовувати 128-бітний ключ, то необхідно буде перебрати 2^{128} ключів, що в даний час не під силу навіть найпотужнішим комп'ютерам.

Важливо відзначити, що зростаюча продуктивність техніки призводить до зменшення часу, потрібного для розтину ключів, і систем забезпечення безпеки доводиться використовувати все більш довгі ключі, що, у свою чергу, веде до збільшення витрат на шифрування.

Оскільки таке важливе місце в системах шифрування приділяється секретності ключа, то основною проблемою подібних систем є генерація і передача ключа. Існують дві основні схеми шифрування: симетричне шифрування (його також іноді називають традиційними або шифруванням з секретним ключем) і шифрування з відкритим ключем (іноді цей тип шифрування називають асиметричним).

При симетричному шифруванні відправник та одержувач володіють одним і тим же ключем (секретним), за допомогою якого вони можуть зашифровувати і розшифровувати данние.Прі симетричному шифруванні використовуються ключі невеликої довжини, тому можна швидко шифрувати великі об'єми даних. Симетричне шифрування використовується, наприклад, деякими банками в мережах банкоматів. Однак симетричне шифрування має деякі недоліки. По-перше, дуже складно знайти безпечний механізм, за допомогою якого відправник та одержувач зможуть таємно від інших вибрати ключ. Виникає проблема безпечного розповсюдження секретних ключів.

По-друге, для кожного адресата необхідно зберігати окремий секретний ключ. По-третє, у схемі симетричного шифрування неможливо гарантувати особу відправника, оскільки два користувача володіють одним ключем.

У схемі шифрування з відкритим ключем для шифрування послання використовуються два різних ключа. За допомогою одного з них послання зашифровується, а за допомогою другого - розшифровується. Таким чином, необхідної безпеки можна добиватися, зробивши перший ключ загальнодоступним (відкритим), а другий ключ зберігати тільки в одержувача (закритий, особистий ключ). У такому випадку будь-який користувач може зашифрувати послання за допомогою відкритого ключа, але розшифрувати послання здатний тільки володар особистого ключа. При цьому немає необхідності піклуватися про безпеку передачі відкритого ключа, а для того щоб користувачі могли обмінюватися секретними повідомленнями, досить наявності у них відкритих ключів один одного.

Недоліком асиметричного шифрування є необхідність використання більш довгих, ніж при симетричному шифруванні, ключів для забезпечення еквівалентного рівня безпеки, що позначається на обчислювальних ресурсах, необхідних для організації процесу шифрування.

Електронний підпис.

Якщо послання, безпека якого ми хочемо забезпечити, належним чином зашифровано, все одно залишається можливість модифікації початкового повідомлення або підміни цього повідомлення іншим. Одним із шляхів вирішення цієї проблеми є передача користувачем одержувачу короткого представлення переданого повідомлення. Подібне короткий уявлення називають контрольною сумою, або дайджестом повідомлення.

Контрольні суми використовуються при створенні резюме фіксованої довжини для представлення довгих повідомлень. Алгоритми розрахунку контрольних сум розроблені так, щоб вони були по можливості унікальні для кожного повідомлення. Таким чином, усувається можливість підміни одного повідомлення іншим із збереженням того ж самого значення контрольної суми. Однак при використанні контрольних сум виникає проблема передачі їх одержувачу. Одним з можливих шляхів її вирішення є включення контрольної суми в так звану електронний підпис.

За допомогою електронного підпису одержувач може переконатися в тому, що отримане ним повідомлення надіслано не стороннім особою, а мають певні права відправником. Електронні підписи створюються шифруванням контрольної суми та додаткової інформації за допомогою особистого ключа відправника. Таким чином, будь-хто може розшифрувати підпис, використовуючи відкритий ключ, але коректно створити підпис може тільки власник особистого ключа. Для захисту від перехоплення та повторного використання підпис містить у собі унікальне число - порядковий номер.

Аутентифікація. Аутентифікація є одним з найважливіших компонентів організації захисту інформації в мережі. Перш ніж користувачеві буде надано право отримати той чи інший ресурс, необхідно переконатися, що він дійсно той, за кого себе видає.

При отриманні запиту на використання ресурсу від імені будь-якого користувача сервер, що надає даний ресурс, передає керування серверу аутентифікації. Після отримання позитивної відповіді сервера аутентифікації користувачеві надається запитуваний ресурс.

При аутентифікації використовується, як правило, принцип, що отримав назву "що він знає", - користувач знає деякий секретне слово, яке він посилає серверу аутентифікації у відповідь на його запит. Однією зі схем аутентифікації є використання стандартних паролів. Пароль - сукупність символів, відомих підключеного до мережі абоненту, - вводиться ним на початку сеансу взаємодії з мережею, а іноді і в кінці сеансу (в особливо відповідальних випадках пароль нормального виходу з мережі може відрізнятися від вхідного). Ця схема є найбільш вразливою з точки зору безпеки - пароль може бути перехоплений і використаний іншою особою.

Найчастіше використовуються схеми із застосуванням одноразових паролів. Навіть будучи перехопленим, цей пароль буде марний при наступній реєстрації, а отримати наступний пароль з попереднього є вкрай важким завданням.

Для генерації одноразових паролів використовуються як програмні, так і апаратні генератори, що представляють собою пристрої, що вставляються в слот комп'ютера. Знання секретного слова необхідно користувачеві для приведення цього пристрою в дію.

Однією з найбільш простих систем, що не вимагають додаткових витрат на обладнання, але в той же час забезпечують гарний рівень захисту, є S / Key, на прикладі якої можна продемонструвати порядок подання одноразових паролів.

У процесі аутентифікації з використанням S / Key беруть участь дві сторони - клієнт і сервер. При реєстрації в системі, що використовує схему аутентифікації S / Key, сервер надсилає на клієнтську машину запрошення, що містить зерно, передане по мережі у відкритому вигляді, поточне значення лічильника ітерацій і запит на введення одноразового пароля, який повинен відповідати поточним значенням лічильника ітерації. Отримавши відповідь, сервер перевіряє його і передає керування серверу необхідного користувачеві сервісу.

Захист мереж. Останнім часом корпоративні мережі все частіше включаються в Інтернет або навіть використовують його в якості своєї основи. Зважаючи на те, якої шкоди може принести незаконне вторгнення в корпоративну мережу, необхідно виробити методи захисту. Для захисту корпоративних інформаційних мереж використовуються брандмауери.

Брандмауери - це система або комбінація систем, що дозволяють розділити мережу на дві або більше частин і реалізувати набір правил, що визначають умови проходження пакетів з однієї частини в іншу. Як правило, ця межа проводиться між локальною мережею підприємства і INTERNETOM, хоча її можна провести і всередині. Однак захищати окремі комп'ютери невигідно, тому зазвичай захищають всю мережу. Брандмауер пропускає через себе весь трафік і для кожного проходить пакету приймає рішення - пропускати його або відкинути. Для того щоб брандмауер міг приймати ці рішення, для нього визначається набір правил.

Брандмауер може бути реалізований як апаратними засобами (тобто як окрема фізична пристрій), так і у вигляді спеціальної програми, запущеної на комп'ютері.

Як правило, в операційну систему, під управлінням якої працює брандмауер, вносяться зміни, мета яких - підвищення захисту самого брандмауера. Ці зміни зачіпають як ядро ОС, так і відповідні файли конфігурації. На самому брандмауері не дозволяється мати розділів користувачів, а отже, і потенційних дірок - тільки розділ адміністратора.

Деякі брандмауери працюють тільки в режимі одного, а багато хто має систему перевірки цілісності програмних кодів.

Брандмауер зазвичай складається з декількох різних компонентів, включаючи фільтри або екрани, які блокують передачу частини трафіку. Всі брандмауери можна розділити на два типи:

· Пакетні фільтри, які здійснюють фільтрацію IP-пакетів засобами фільтруючих маршрутизаторів;

· Сервери прикладного рівня, які блокують доступ до певних сервісів в мережі.

Таким чином, брандмауер можна визначити як набір компонентів або систему, яка розташовується між двома мережами і володіє наступними властивостями:

· Весь трафік з внутрішньої мережі в зовнішню і з зовнішньої мережі у внутрішню повинен пройти через цю систему;

· Тільки трафік, певний локальної стратегією захисту, може пройти через цю систему;

· Система надійно захищена від проникнення.

1.3. Аналіз сучасних методів захисту інформації та їх класифікація

Для організації успішного бізнесу все більшого значення набуває використання інформаційних технологій. Адже за допомогою своєї інформаційної системи (ІС) кожна компанія організовує всі внутрішні процеси,

взаємодіє із зовнішніми партнерами, контрагентами, державними органами. Забезпечення безпеки й постійної працездатності інформаційної системи є одним із пріоритетних завдань будь-якого підприємства.

Створення сучасних комп'ютерних систем і поява глобальних комп'ютерних мереж радикально змінили характер і діапазон проблем захисту інформації. У широко комп'ютеризованому й інформатизованому сучасному суспільстві володіння реальними цінностями, керування ними, передача цінностей або доступ до них часто побудовані на інформації, існування якої не обов'язково пов'язується з яким-небудь записом на фізичному носії. Тому досить важливо створювати й застосовувати ефективні засоби для реалізації всіх необхідних функцій, пов'язаних із забезпеченням конфіденційності й цілісності електронної інформації.

Методи захисту інформації можна класифікувати по меті їх використання на методи активного та пасивного захисту. Метою методів активного захисту інформації є збереження всіх категорій інформації. Методи пасивного захисту інформації (МПЗІ) націлені на те, щоб дати відповідь, чи було зроблено навмисне порушення якоїсь категорії інформації. МПЗІ за способом їх реалізації можна розділити на методи експертної оцінки, програмно-технічні й програмні [2].

Методи експертної оцінки використовують візуальне або акустичне оцінювання інформації фахівцем. Головним недоліком методів експертної оцінки є наявність людського фактору [2].

Програмно-технічні МПЗІ ґрунтуються на знанні специфічних особливостей пристроїв аудіо –, відео – або фотофіксації та (або) впливу якихось зовнішніх факторів на проведення запису. До програмно-технічних МПЗІ відносяться методи, присвячені доведенню цілісності цифрових звукозаписів, засновані на перевірці технічних засобів фіксації аудіосигналів та аналізі можливих способів фальсифікації сигналограм [15,20,21].

У процесі теоретичних досліджень були встановлені способи проведення такої обробки. Виявлено, що фонограми можуть бути оброблені або способом

компіляції фрагментів в персональній електронній обчислювальній машині (ПЕОМ) за допомогою звукових редакторів, або способом синтезу необхідного тексту за заданими зразками голосів фігурантів створюваної фонограми. При цьому додатково можуть використовуватися специфічні прийоми обробки сигналів. Однак, при використанні будь-якої з цих технологій, попередньо необхідно ввести в ПЕОМ фонограми із зразками мовлення фігурантів. Такі первинні фонограми можуть бути записані на цифровій апаратурі запису аналогових сигналів (ЦАЗАС) і введені в машину в цифровий або аналоговій формі (залежно від типу використовуваної апаратури запису). Таким же чином вони можуть бути виведені з комп'ютера при перезапису обробленої фонограми на ЦАЗАС. Можливий ще варіант перезапису обробленої фонограми по акустичному каналу. Крім того, у процесі створення обробленої фонограми завжди використовується операція стробування і вирізання фрагментів, оскільки, навіть при використанні способу синтезу, оброблена фонограма повинна містити діалог як мінімум двох осіб. Застосування всіх цих операцій при обробці фонограм призводить до неминучого утворення їх слідів у вигляді спотворень форми оброблюваних сигналів і, як наслідок, спотворень їх спектрального складу.

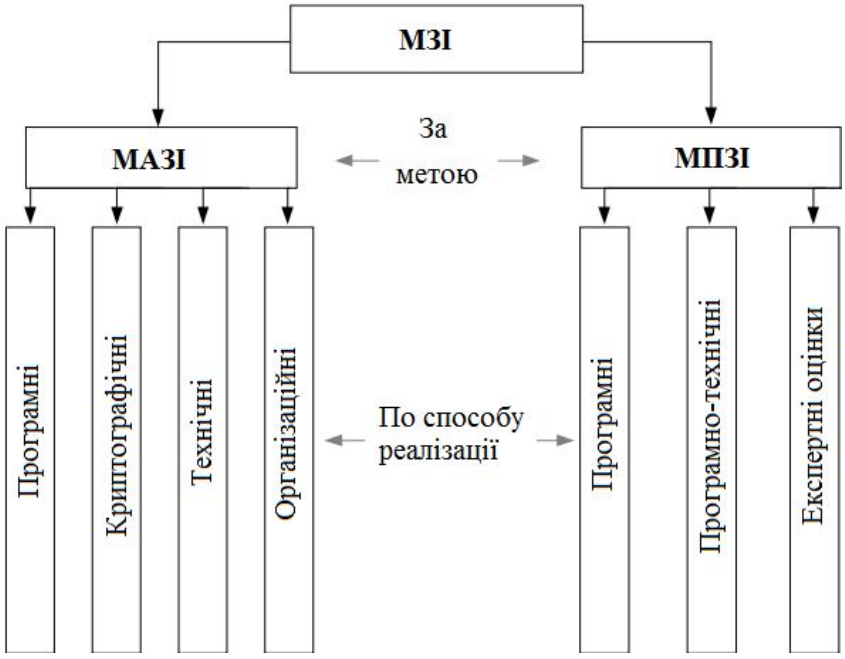


Рисунок 1.1- Класифікація методів захисту інформації

Таким чином, у роботі розглядається нова класифікація МЗІ, яка більш повно відображає існуючі на сьогоднішній день методи захисту інформації, дає системне уявлення про способи їх реалізації та дозволяє визначити місце методів перевірки цілісності цифрових сигналів серед всіх інших методів.

Запропонована класифікація може бути корисна при вивченні існуючих і розробці нових методів і засобів захисту інформації.

1.4. Постановка задачі дослідження

До основних недоліків існуючих у відкритих джерелах методів виявлення фальсифікації ЦЗ можна віднести значну обчислювальну складність та необхідність додаткової інформації для проведення аналізу ЦЗ (як правило, характеристик технічних приладів, на яких ЦЗ було створено). Більшість сучасних цифрових фотокамер використовують для збереження ЦЗ формат JPEG з втратами інформації, що ґрунтується на дискретному косинусному перетворенні (ДКП) або вейвлет-перетворенні. Не обмежуючи спільності міркувань, для визначеності розглядається формат JPEG, що ґрунтується на ДКП. Більшість несанкціонованих змін фотографії зводиться до заміщення 224 деякої її області в область іншого ЦЗ, що могло бути також отримане після попереднього стиснення JPEG, або зберігалося у форматі без втрат інформації. Після такої фальсифікації отримане зображення зберігається знову у форматі JPEG або з використанням форматів без втрат інформації.

Мета магістерської роботи – розробити новий практичний підхід до виявлення та локалізації фальсифікації цифрового зображення без наявності додаткової інформації. Дослідження цифрового зображення на наявність фальсифікації – це надзвичайно важлива та актуальна проблема.

При теоретичному опрацюванні проблеми був використаний метод декомпозиції процесу обробки фонограм і на аналітичних моделях підтверджені висунуті факти, тези, гіпотези і концепція обробки фонограм, а також встановлена закономірність, властива прояву слідів цифрової обробки у фонограмах. Також була встановлена принципова придатність вейвлет-аналізу (і

непридатність класичного частотного для часу аналізу, побудованого на короткочасному перетворенні Фур'є) для проведення такої експертизи і показано, що найбільш придатними для виявлення слідів цифрової обробки є комплексні вейвлети, зокрема, вейвлет Морле, сконструйований з гауссіана. На цій базі були розроблені методи і засоби виявлення слідів цифрової обробки аналогових і цифрових фонограм (АФ і ЦФ).

Експериментальні дослідження на мовних сигналах проводилися в два етапи. На першому етапі перевірялася ефективність запропонованого методу для виявлення за вейвлет-портретів інформативних ознак цифрової обробки АФ і ЦФ при різних моделях введення / виведення інформації в апаратуру звукозапису і в ПЕОМ при різних видах обробки фонограм.

На другому етапі перевірялася можливість виявлення слідів цифрової обробки, за умови перезапису обробленої фонограми по акустичному каналу.

У процесі проведення експериментів було знято понад 300 вейвлет-портретів, перетворених у програмі Academy в графічні спектрограми. Вони були отримані при записі, обробці та перезапису мовних сигналів на різних апаратах.

У роботі були проведені дослідження і створено експериментальний зразок апаратно-програмного комплексу, що дозволяє виявляти сліди цифрової обробки аналогових і цифрових фонограм. Теоретичні та апаратні розробки даного комплексу базуються на застосуванні вейвлет–аналізу процесів, неминуче виникають при будь-якій обробці первинної фонограми: перезапису і перекодуванні.

Дослідження проводилися в два етапи. На першому – з'ясовувалася здатність виявлення та індикації за допомогою вейвлет-портретів нелінійності статичної характеристики квантувача за рівнем (СХ КР) на моделях. Ця частина експерименту побудована на моделюванні в ЕОМ сигналів з привнесеної в них немонотонністю і нелінійністю СХ та їх подальшого вейвлет-аналізу.

На другому – перевірялася придатність даного методу при проведенні експертизи на реальних апаратах цифрового звукозапису.

На першому етапі моделювання сигналів здійснювалося за допомогою програмного пакету MATLAB. Немонотонність статичної характеристики (НСХ) задавалась за допомогою таблиці рівнів, а диференційна нелінійність (ДНСХ) задавалося в рівнях відповідно з нормальним законом розподілу. Проводилася серія експериментів, і знімалися вейвлет-портрети отриманих сигналів.

На другому етапі проводився запис гармонійних сигналів на різні апарати аналогового і цифрового звукозапису, і знімалися їх вейвлет-портрети. В якості апаратів цифрового звукозапису використовувалися різні ПЕОМ з різними звуковими картами та цифрові диктофони.

Переваги такої побудови експерименту полягають у тому, що на його першому етапі можна задати частоту досліджуваного сигналу, немонотонність в будь-якому з рівнів квантування, частоту дискретизації і розрядність перетворення. При цьому забезпечується наглядність отриманих результатів, тому завжди можна порівняти форму сигналів до внесення нелінійності і після її внесення, оскільки тестові сигнали можна сформувати в ЕОМ і порівняти вейвлет-портрети, отримані для їх різних варіантів. Цим оцінювалася принципова придатність методу для виявлення таких малих стрибків у сигналі.

На другому етапі експерименту первинні записи проводилися через вбудовані мікрофони апаратів звукозапису. Записувалися сигнали від генератора звукової частоти, посилені й відтворені через звукові колонки. Отримані первинні цифрові фонограми в аналоговій формі вводилися в ПЕОМ з частотою дискретизації і оцифруванням, відповідними умовами запису в апаратурі, на якій вони записувалися. Потім з ПЕОМ сигнали перезаписувалися на апаратуру звукозапису. При цьому перезапис з комп'ютера проводився як на цифрову, так і аналогову апаратуру.

Отримані таким чином копії фонограм, що містять сліди двох дискретизацій в часі і квантування за рівнем на різних цифрових пристроях, вводилися в ЕОМ при частоті дискретизації 44,1 кГц для подальшого вейвлет-аналізу.

Так само записувалися від генератора звукової частоти і сигнали на аналоговий диктофон, а отриманий первинний запис вводився в комп'ютер на частоті дискретизації 16 кГц і 44,1 кГц. Перезапис, проведений на частоті 16 кГц, перезаписувався на аналоговий диктофон і потім вводився в ЕОМ на частоті дискретизації 44,1 кГц для подальшого аналізу. Для введення в ПЕОМ використовувалася програма Cool.

Отримані таким чином перезаписи, що містять (а для випадку аналогового запису – не містять) сліди цифрової обробки на частотах дискретизації нижче, ніж частота введення сигналів для вейвлет–аналізу, аналізувалися і порівнювалися їх вейвлет-портрети.

У процесі порівняння відбиралися типи вейвлетів та режими завдання коефіцієнтів для проведення аналізу. У разі виявлення відмінності між портретами для різних сигналів, приймалося рішення про придатність вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм, тобто оцінювалася принципова придатність методу для проведення експертизи.

Для проведення експертиз найбільш доцільно використовувати вейвлети з високою вибірковістю, наприклад, вейвлет Морле. При використанні таких вейвлетів застосування високих значень параметрів кроку забезпечує велику наочність матеріалу, що вкрай важливо при експертизі.

Висновки до розділу 1

В даному розділі проаналізовані проблеми захисту інформації в комп'ютерних системах. Досліджені механізми забезпечення безпеки, здійснено аналіз сучасних методів захисту інформації та їх класифікацію, проведено аналіз засобів ідентифікації цифрової і аналогової апаратури запису сигналів. розроблено алгоритм виявлення і локалізації фальсифікації цифрового аудіо-зображення.,описано метод перевірки цілісності цифрового аудіо-сигналу.

РОЗДІЛ 2
МЕТОД ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО АУДІО-СИГНАЛУ, ЗБЕРЕЖЕНОГО У ФОРМАТІ ІЗ ВТРАТОЮ ІНФОРМАЦІЇ

2.1. Алгоритм виявлення і локалізації фальсифікації цифрового аудіо-зображення

У магістерській роботі представлений алгоритм виявлення і локалізації фальсифікації цифрового зображення,заснований на використанні ефекту подвійного квантування коефіцієнтів дискретного косинусного перетворення матриці зображення.

Для розроблення цього методу були вирішені наступні задачі:

- визначення достатньої умови прояви DQ-ефекту;
- дослідження особливості прояву DQ-ефекту при наявності шуму округлення;
- розробка способу віртуального збільшення внеску області фальсифікації в сукупне зображення;
- проведення обчислювального експерименту на основі побудованих алгоритмів.

Фальсифікація і перевірка на наявність фальсифікації проводилися за наступним алгоритмом:

а) завантажувалася матриця зображення розміром 1024x1024 пікселів;

б) проводилося перше квантування з відновленням матриці зображення:

1) матриця зображення розбивалася на блоки 8x8 пікселів і обчислювалися коефіцієнти ДКП для кожного з блоків;

2) квантувалися коефіцієнти ДКП за допомогою матриці квантування з кроком $q^{(1)}$;

3) відновлювалися коефіцієнти ДКП, проводилося зворотне ДКП і приводилася матриця зображення до формату uint8;

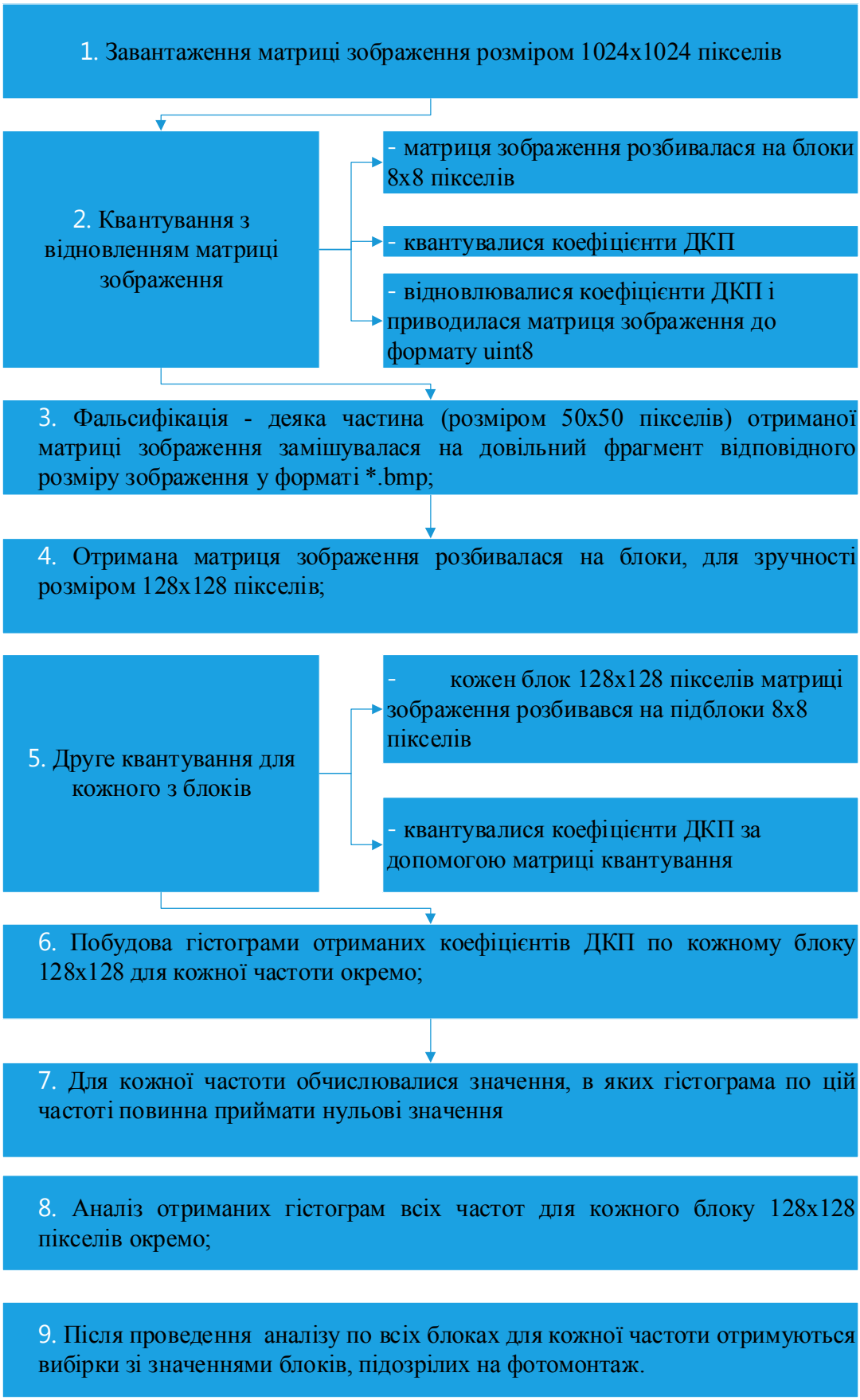


Рисунок 2.1 - Алгоритм встановлення та локалізації фальсифікації цифрового аудіо-зображення

в) фальсифікація. Деяка частина (розміром 50х50 пікселів) отриманої матриці зображення заміщувалася на довільний фрагмент відповідного розміру зображення у форматі *.bmp;

г) отримана матриця зображення розбивалася на блоки, для зручності розміром 128х128 пікселів;

ґ) проводилося друге квантування для кожного з блоків:

1) кожен блок 128х128 пікселів матриці зображення розбивався на підблоки 8х8 пікселів і обчислювалися коефіцієнти ДКП для кожного з під блоків;

2) квантувалися коефіцієнти ДКП за допомогою матриці квантування з кроком $q^{(2)}$. При цьому $q^{(2)} < q^{(1)}$;

д) будувалися гістограми отриманих коефіцієнтів ДКП по кожному блоку 128х128 для кожної частоти окремо;

е) за відомими значеннями кроків квантування і для кожної частоти обчислювалися значення, в яких гістограма по цій частоті повинна приймати нульові значення (називалися такі значення «нулями» гістограми);

є) проводився аналіз отриманих гістограм всіх частот для кожного блоку 128х128 пікселів окремо:

1) обиралися всі гістограми відповідної частоти по всіх блоках;

2) для кожної частоти кожного блоку підраховувалася кількість «нулів» гістограми, в яких гістограма прийняла ненульові значення. Отримане значення назвали кількістю вильотів. Наявність таких вильотів свідчила про наявність або фотомонтажу в даному блоці, або про високу похибку округлення при переході матриці зображення до формату uint8 після першого квантування;

3) якщо для частоти блоку 128х128 пікселів кількість вильотів більше деякого порогового значення p, запам'ятовувався номер цього блоку. Таким чином, номер блоку записувався стільки разів, по скільком частотам кількість вильотів перевищувало порогове значення;

ж) після проведення такого аналізу по всіх блоках для кожної частоти отримували вибірку зі значеннями блоків, підозрілих на фотомонтаж.

Коефіцієнт K_i того, що і-й блок у вибірці містить фотомонтаж, обчислювався як відношення кількості появи відповідного блоку у вибірці до загального числа значень вибірки:

$$K_i = \frac{n_i}{\sum_{j=1}^{m} n_j}, \tag{2.1}$$

де n_i – кількість появ і-го блоку у вибірці, m – кількість блоків, на які розбивалася матриця зображення, $\sum_{j=1}^{m} n_j$ – кількість значень у вибірці.

Для перевірки оригінальних зображень без фальсифікації на її наявність у вищевказаному алгоритмі опускався крок 3.

2.2. Метод перевірки цілісності цифрового аудіо-сигналу

Розроблений метод перевірки цілісності цифрового аудіо-сигналу, заснований на ефекті подвійного квантування [2], ефективно використовувався для цифрових зображень та відео, збережених у форматі із втратою інформації на основі квантування складових сигналу.

Обґрунтована можливість використання зазначеного методу і для ЦА. Проте для можливості використання методу перевірки цілісності цифрового сигналу, заснованого на ефекті подвійного квантування, необхідно передбачати два можливі варіанти прояву зазначеного ефекту, що призводить до ускладнення аналізу цифрового сигналу, хоча і не зменшує його ефективність.

Серед найбільш поширених методів пасивного захисту інформації зважаючи на свою простоту перевагу надаємо методу виявлення і локалізації фальсифікації цифрового зображення (ЦЗ), збереженого у форматі із втратою інформації, створений на основі функції (1,1) квадрату середньоквадратичного відхилення значень коефіцієнтів дискретного косинусного перетворення (ДКП) від значень повторно відквантованних коефіцієнтів ДКП матриці ЦЗ з різними кроками квантування [9,10].

Для виявлення фальсифікації пропонувалося аналізувати функцію:

$$F(q) = \sum_{i=1}^{n} (f_i - f_i^q)^2 , \qquad (2.2)$$

де n – кількість коефіцієнтів ДКП, які відповідають заданій частоті;

f_i – коефіцієнт ДКП;

f_i^q – визначається за формулою (2.2):

$$f^{\cdot} = \left[\frac{f}{q} \right] q , \; q \in (1,30] \qquad (2.3)$$

Метод використовувався для цифрових зображень, збережених у форматі із втратою інформації.

Основною перевагою даного методу на нашу думку є:

- аналізування цифрового зображення відбувається без додаткової інформації щодо технічних та програмних характеристик фотоапарату за допомогою якого створено цифрове зображення;

- встановлення факту фальсифікації у визначеному підблоці сигналу в одночасно встановлює ймовірність локалізацію у самому зображенні;

- метод є досить ефективним при встановлені шумів округлення значення яскравостей пікселів матриці цифрового зображення, отже широко реалізується практично;

- за умови дотримання розкладання цифрового зображення на окремі підблоки сигналу та використовуючи запропоновану методику встановлюється фальсифікація для значних (до 50% розмірів зображення), а також незначних розмірів (порядку 20х20 пікселів).

До основних недоліків цього методу можна віднести необхідність візуального аналізу результатів роботи методу, тобто відсутність автоматизованого процесу виявлення фальсифікованого підблоку сигналу.

На основі проведеного аналізу існуючих методів перевірки цілісності цифрового аудіо можна зробити наступні висновки:

- при проведенні перевірки цілісності цифрових сигналів програмні методи пасивного захисту інформації є переважаючими;

- реалізація програмного продукту для виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації, є актуальною та на сьогодні невирішеною задачею;

- існують ефективні методи виявлення та локалізації фальсифікації цифрових сигналів, які можуть бути адаптовані для аналізу цифрового аудіо-сигналу, збереженого у форматі із втратою інформації.

2.3. Адаптація для цифрового аудіо методу виявлення та локалізації фальсифікації цифрового зображення

Метод ґрунтується на можливості визначення ознак квантування коефіцієнтів ДКП ЦЗ за допомогою різних таблиць квантування, які можуть вказувати на стиснення деяких частин одного і того ж ЦЗ з різною якістю. Це свідчить про те, що ЦЗ було стиснено з якістю α, потім в нього була вставлена частина іншого ЦЗ, яка була стиснена з якістю β, а після змінене (сукупне) зображення було ще раз стиснене з якістю γ (рисунок 2.2).

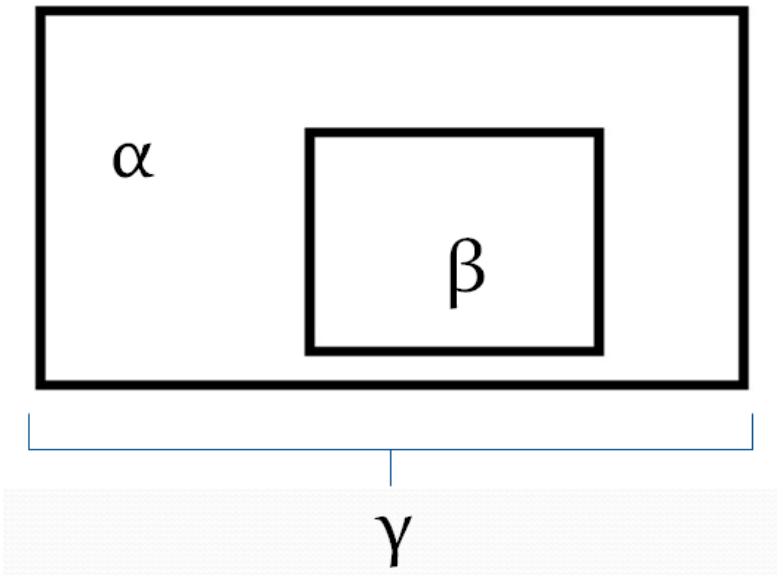
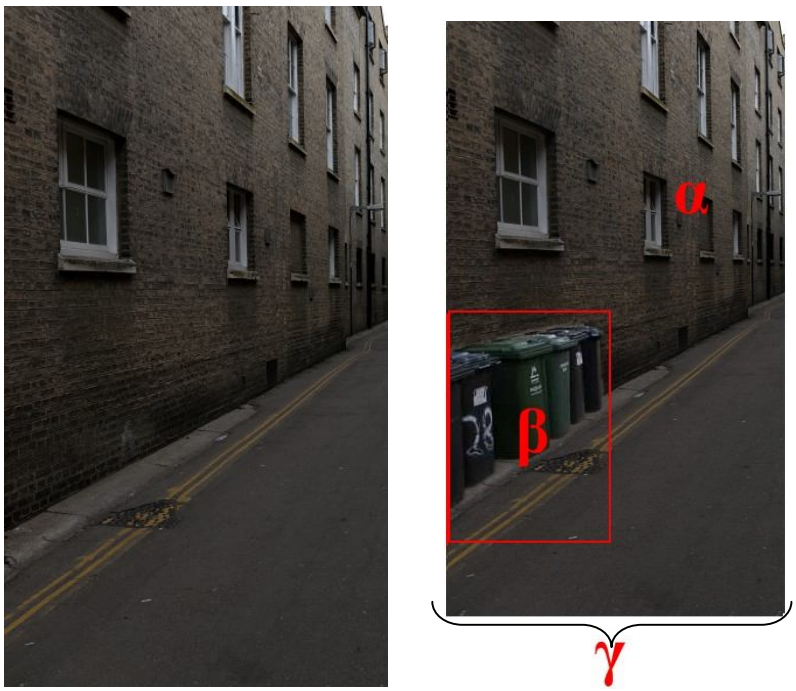


Рисунок 2.2 - Схема фальсифікації ЦЗ :оригінальне ЦЗ, збережене з якістю α, область фальсифікації, збережене з якістю β; фальсифіковане ЦЗ, збережене з якістю γ

Для наочності методу наведені приклади оригінального та фальсифікованого цифрових зображень, частини яких стиснені з різною якістю (рисунок 2.3).



а б

Рисунок 2.3 - Цифрові зображення, а – оригінальне цифрове зображення; б – фальсифіковане цифрове зображення

На практиці при проведенні фальсифікації можуть бути використані різні формати цифрових зображень.

В роботі пропонується наступна класифікація умов проведення фальсифікації в залежності від значень α, β і γ [29,30]:

а) фальсифікація 1-го типа, що характеризується відсутністю кроку квантування α;

б) фальсифікація 2-го типа, що характеризується відсутністю кроку квантування γ;

в) фальсифікація 3-го типа характеризується наявністю всіх трьох кроків квантування.

Представлена класифікація може бути застосована і для ЦА, оскільки не залежить від форми представлення сигналу та не суперечить процесу фальсифікації аудіо сигналів.

Цифрове зображення, представлене у вигляді матриці значень яскравості пікселів, розбивається на рівні частини - так звані підблоки сигналу (ПБС), не порушуючи стандартну сітку розбиття на блоки 8х8 пікселів (рисунок 2.4). Після розбиття аналізується вже не вся матриця ЦЗ, а кожен ПБС окремо згідно з алгоритмом, що наведений нижче.

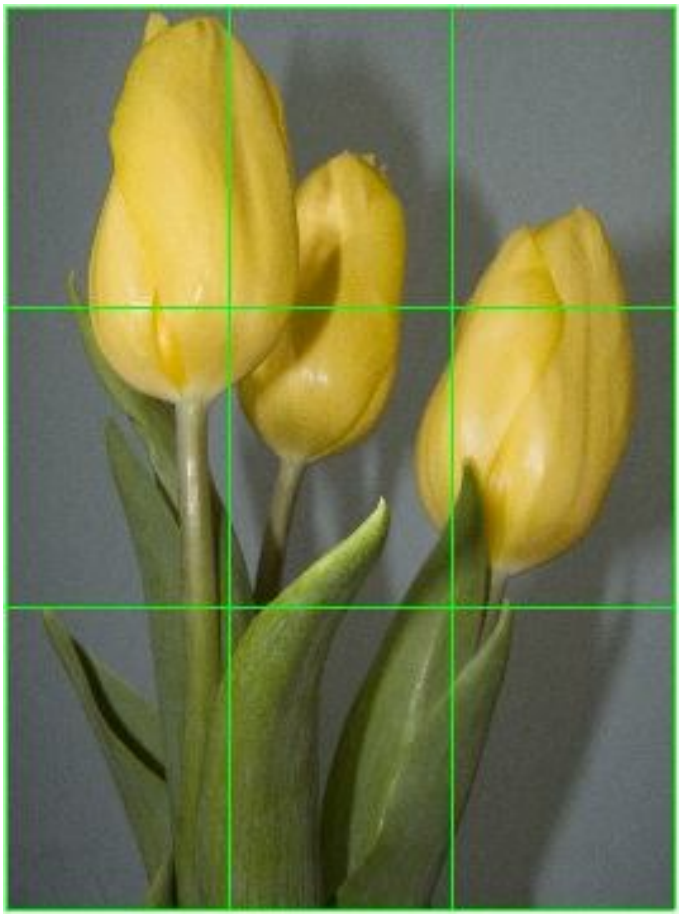


Рисунок 2.4 - Оригінальне ЦЗ розбите на 9 ПБС не порушуючи розбиття на блоки 8х8 пікселів

Алгоритм встановлення та локалізації фальсифікації цифрового зображення

Цей алгоритм формується за наступними кроками :

а) розробляється матриця ЦЗ на m ПБС;

б) для і-го ПБС, $i = 1, m$:

1) сформувати матрицю коефіцієнтів ДКП;

2) для всіх коефіцієнтів ДКП, відповідної частоти, побудувати функцію $\mathrm{F}_i(q)$ по формулі (1);

3) апроксимувати отриману функцію (1) методом найменших квадратів $\overline{\mathrm{F}_i(q)}$;

в) пряме середньо квадратичного відхилення $\overline{\mathrm{F}_i(q)}$, $i = 1, m$, відповідне фальсифікованому ПБС візуально віддільно від прямих інших підблоків. Для фальсифікації 1-го типа графік функції $\overline{\mathrm{F}_i(q)}$ фальсифікованого ПБС знаходиться нижче за інших. Для фальсифікації 2-го і 3-го типів графік функції $\overline{\mathrm{F}_i(q)}$ фальсифікованого ПБС знаходиться вище за інших.

Адаптації методу для дослідження ЦА можлива тільки для тих сигналів, формат стиснення яких також заснований на квантуванні коефіцієнтів ДКП. Найбільш поширеним форматом стиснення ЦА є стандарт MPEG, який буде розглянутий нижче.

Аудіостандарт MPEG [31] має нормативний та описовий розділи. Нормативний розділ містить специфікації стандарту. Описовий розділ ілюструє вибрані концепції, пояснює причини вибору того чи іншого підходу, містить необхідні базові відомості.

Прикладом нормативного розділу є таблиці з різними параметрами і з кодами Хаффмана, які використовуються в стандарті MPEG. А прикладом описового розділу служить алгоритм, що задає психоакустичну модель. MPEG не дає конкретного алгоритму, і кодер MPEG вільний у виборі методу реалізації моделі.

Починається аудіостандарт нормативним описом формату стисненого файлу для кожного з трьох шарів.

Потім слідує нормативний опис декодера. Опис кодера (він різний для всіх верств), а також двох психоакустичних моделей міститься в описовому розділі; будь який кодер, здатний згенерувати коректно стислий файл, може вважатися допустимим кодером MPEG.

Аудіостандарт MPEG–1 описує три методи стиснення, звані шарами (layer), які позначаються римськими числами I, II і III. Всі три шари входять в стандарт MPEG–1. При стисненні відеофільмів використовується тільки один шар, який позначається в заголовку стисненого файлу. Будь-який з цих шарів можна незалежно використовувати для стиснення звуку без відео.

Функціональні модулі молодших шарів можуть бути використані старшими шарами, але більш високі шари використовують додаткові можливості для кращого стиснення. Цікавою особливістю шарів є їхня ієрархічна структура, тобто, декодер шару III може декодувати файли стиснені шарами I і II. Важливою властивістю MPEG аудіо є можливість завдання користувачем коефіцієнта стиснення.

Структура запропонованого кодера для зжимання аудіо-даних з втратою інформації:

- вихідний цифрований звуковий сигнал розкладається на певні частотні піддіапазони а потім сегментується впродовж певного часу в блоці тимчасової і частотної сегментації;
- довжина кодованих вибірок прямо залежна від форм тимчасової функції звукового сигналу. При не фіксації змін по амплитуді доцільно використовувати довгу вибірку, при якій забезпечується досить високий дозвіл по частотах. У випадку різких коливань амплитуди сигналу відповідно довжина кодованих вибірок різко скорочується, що дає відповідно більший дозвіл за часом. Усі рішення щодо зміни довжин кодованих вибірок приймається блоком психоакустичного

аналізування, на підставі обчислння значення психоакустичної ентропії сигналу;

- Коли завершилась сегментація сигналу частотних піддіапазонів вона відповідно повинна нормуватись, квантуватись та закодовуватись. Інколи найбільш ефективні алгоритми компресії для кодування беруть не сам відлік вибірок звукових сигналів, а визначений коефіцієнт модифікованого дискретно-косинусного перетворення;
- закономірності слухових звукових сигналів зберігаються в блоці психоакустичний аналіз. В цьому блоці за розробленою процедурою для кожного окремого частотного піддіапазону визначається максимальний рівень спотворення (шумів) квантування;
- для блоку динамічного розподілу біт згідно вимог зазначеної психоакустичної моделі усім піддіапазонам кодування пропонується така мінімально можлива їх кількість, при якій рівень спотворень, викликаних квантуванням, не повинен перевищувати поріг їх чутності, розрахований за допомогою психоакустичної моделі.
- За допомогою матрицювання стерео-додавання та віднімання відповідно лівого чи правого каналу уникається повторення інформації;
- За допомогою запропонованих спеціальних процедур ітераційних циклів, вирішується задачі управління величиною енергії спотворень квантування в піддіапазонах при недостатньому числі доступних для кодування біт;
- І відповідно за допомогою техніки згладжування перехідних шумів в тимчасовій області (Temporal Noise Shaping - TNS), є змога управління мікроструктурними спотвореннями квантування всередині кожного піддіапазону кодування.

На практиці існують різноманітні прийоми які служать способом скорочення обсягів даних звукової інформації. Зокрема цього можна досягти простим звуженням смуг частот сигналів разом із зменшенням динамічного діапазону що призведе до стиснення відповідної звукової інформації. В

узагальненому вигляді структуру кодера звукового сигналу з компресією цифрових аудіо даних подано на рисунку 2.5.

Розглянувши алгоритм MPEG який орієнтовано для вирішення задач кодування високоякісного стерео-звуку і за допомогою якого можна вирішити значну кількість допоміжних властивостей.

Стиснення стерео-звуку в форматі MPEG забезпечують принципи квантування. Але, квантована величина береться не з звукового симплу, а з чисел, які виділені з частотних областей звуку. Визначений коефіцієнт стиснення (іноді бітові швидкості) який розпізнає кодер, у відповідний момент часу, він зазначає скільки жсаме біт можна призначувати квантованому сигналу. Виходячи з наведеного одною з основних частин кодера є адаптивний алгоритм призначення бітів.

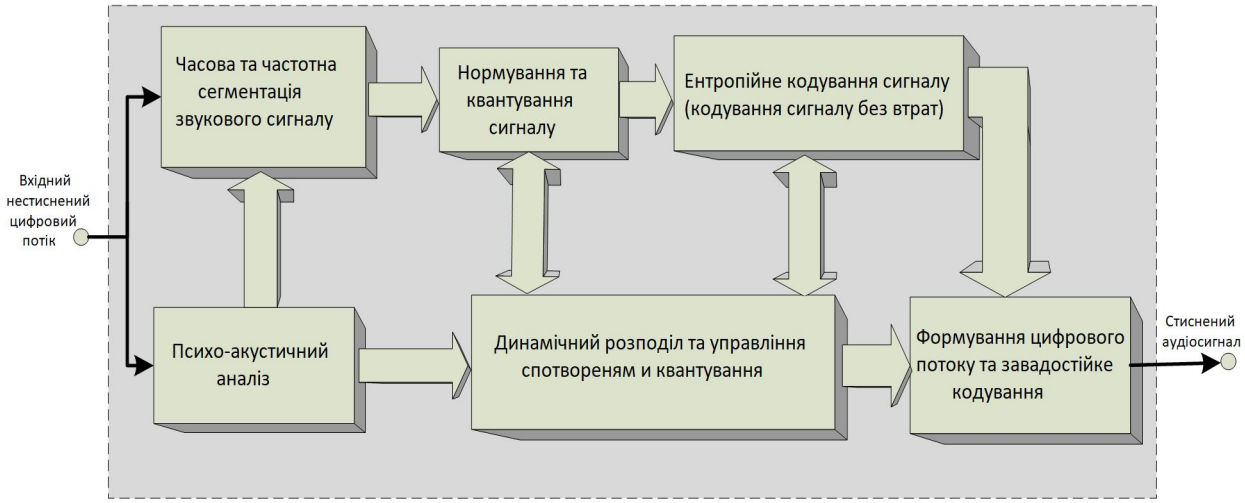


Рисунок 2.5- Структура кодера звукового сигналу з компресією цифрових аудіоданих

За допомогою наведено алгоритму у якому застосовується бітова швидкість а також частотний спектр самих останніх аудіо-симплів для визначення розміру квантування сигналу так, щоб шум квантування (різниця між вихідним сигналом і його квантованим варіантом) був нечутний (тобто, він має знаходитися нижче порога маскування).

Зокрема стандарт MPEG передбачає квантування через розрахунок коефіцієнтів ДКП. Саме тому розглянутий вище метод виявлення та локалізації фальсифікації ЦЗ доцільно адаптовати для аналізу ЦА, що зберігаються у форматі з втратою інформації.

Запропонований алгоритм виявлення та локалізації фальсифікації цифрового аудіо:

а) запропонувати вектор ЦА на *m* ПБС;

б) для і–го ПБС, $i = 1, m$:

1) Визначити вектор коефіцієнтів ДКП;

2) для всіх коефіцієнтів ДКП, відповідної частоти, побудувати функцію $\mathrm{F}_i(q)$ по формулі (1);

3) апроксимувати отриману функцію (1) методом найменших квадратів $\overline{\mathrm{F}_i(q)}$;

в) пряма середньо квадратичного відхилення $\overline{\mathrm{F}_i(q)}$, $i = 1, m$, відповідна фальсифікованому ПБС візуально віддільна від прямих інших підблоків.

2.4. Визначення параметру для відділення фальсифікованої частини аудіо сигналу від оригінальних частин

Використовуючи вище наведений метод аналізу виявлення фальсифікації у окремій частині ЦЗ здійснювався візуально, що призвело до неможливості автоматизувати роботу програми. Тому, виникає необхідність визначити параметр для виокремлення фальсифікованої частини аудіо сигналу від оригінальної частини.

Тому пропонується для визначення параметр максимально допустиме значення величини відхилення 1 похідної кожної апроксимуючої прямої від інших у ПБС. Отже абсолютне значення такого параметру для всіх підблоків може відрізнятися від сигналу до сигналу. Для реалізації проєкту пропонуємо

використати відносне значення цього параметру, яке для кожного ПБС розраховується за наступним алгоритмом:

а) обчислюємо відповідно суму значень відхилення 1 похідної кожної прямої відносно інших прямих:

$$\begin{aligned} S_1 &= |y_1 - y_2| + |y_1 - y_3| + ... + |y_1 - y_n| \\ S_2 &= |y_2 - y_1| + |y_2 - y_3| + ... + |y_2 - y_n| \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S_n &= |y_n - y_1| + |y_n - y_2| + ... + |y_n - y_{n-1}| \end{aligned}, \quad (2.4)$$

де y_i – буде 1 похідна i -ї прямої.

б) визначем суму S всіх значень S_i:

$$S = \sum_{i=1}^{n} S_i ; \quad (2.5)$$

в) визначаємо за допомогою формули (2.6) відносне значення параметру:

$$E_i = \frac{S_i}{S} \times 100\% \quad (2.6)$$

Здійснено випробувальний експеримент. Встановлено максимально допустиме значення величини E_n як для оригінальних, так і фальсифіковані аудіо сигналів. Аудіо сигнали свідомо фальсифікувались за допомогою аудіо редактору Free Audio Editor, шляхом підміни частини одного аудіо на окрему частину іншого аудіо сигналу.

Для реалізації експерименту відібрано випадковим чином 200 аудіо, це були як оригінальні, так і фальсифіковані аудіо сигнали. Основні результати проведеного експерименту подані нижче (рисунок 2.6, 2.7).

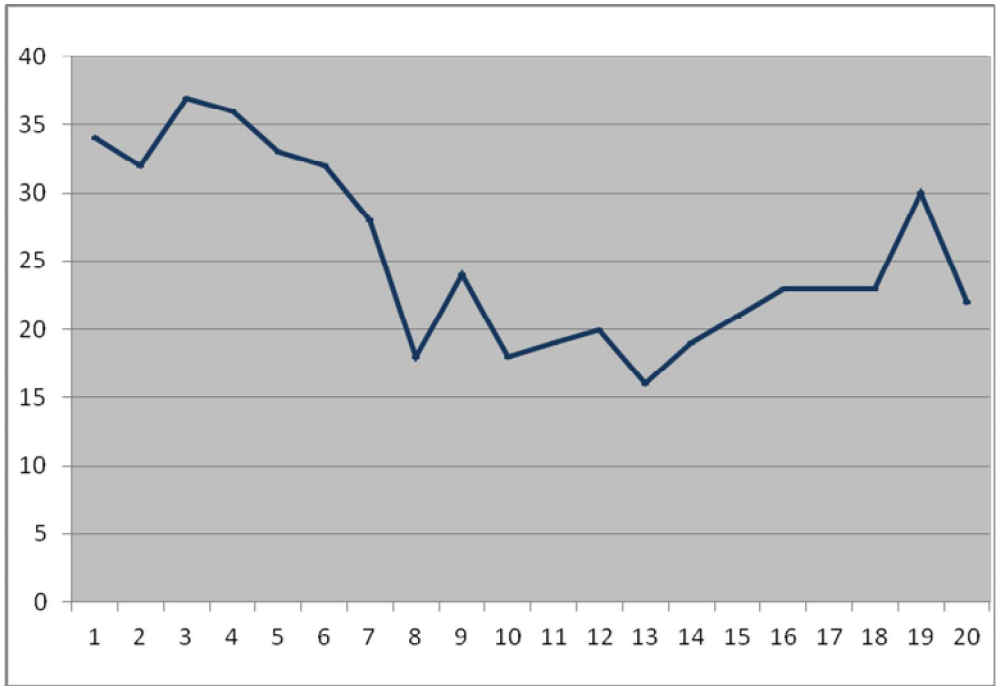


Рисунок 2.6 – Максимально допустиме значення величини E_n в блоці аудіо без фальсифікації

Згідно з результатами проведено експерименту, визначено пирогове значення для величини E_n запропоновано використати його значення 40.

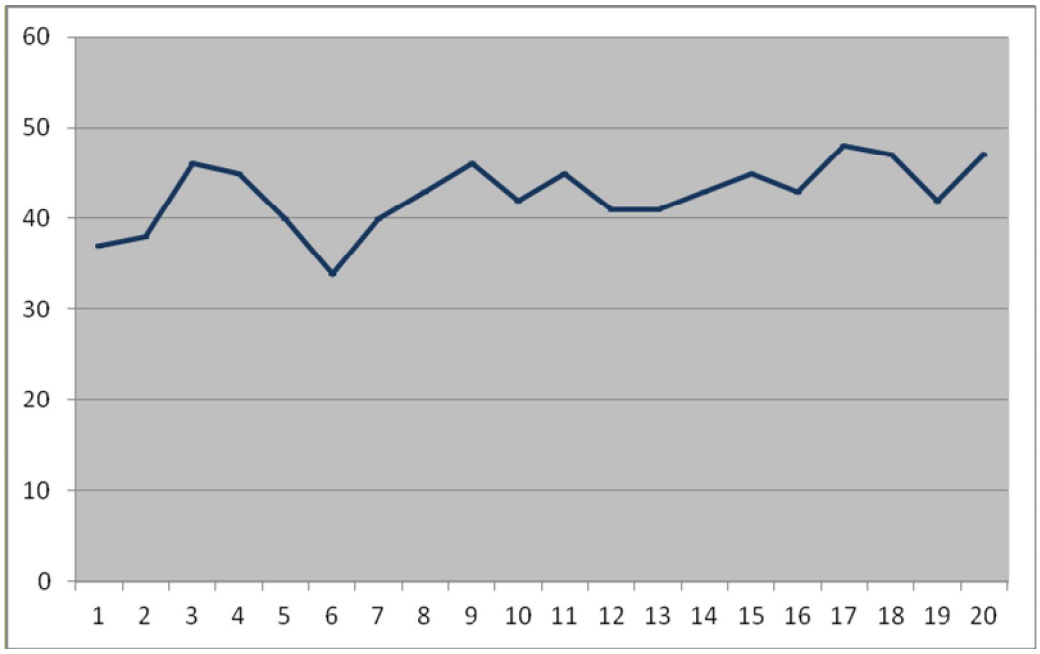


Рисунок 2.7- Максимально допустиме значення величини E_n в блоці аудіо з фальсифікацією

Отже використавши зазначену концептуальну схему (схема можливих варіантів для використання), продемонструємо акторів (особа, яка має доступ до функції наведеної програми) а також функції запропонованого програмного продукту (рисунок 2.8).

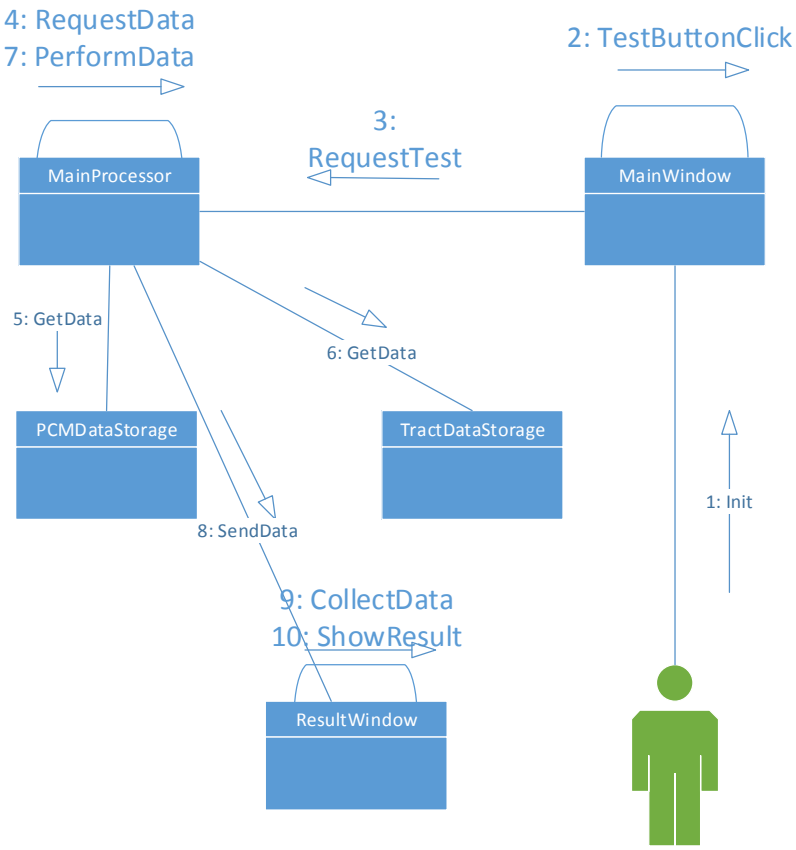


Рисунок 2.8.-Діаграма варіантів використання

Діаграма класів системи тестування цифрового аудіо-сигналу зображена на рисунку 2.9

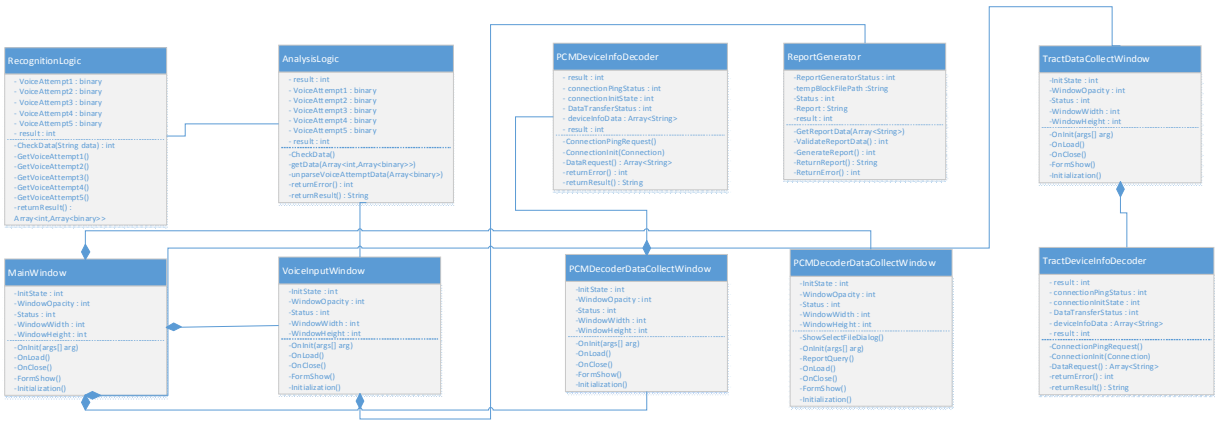


Рисунок 2.9 – Діаграма класів системи тестування цифрового аудіо-сигналу

Діаграма станів та переходів системи тестування цифрового аудіо-сигналу зображена на рисунку 2.10.

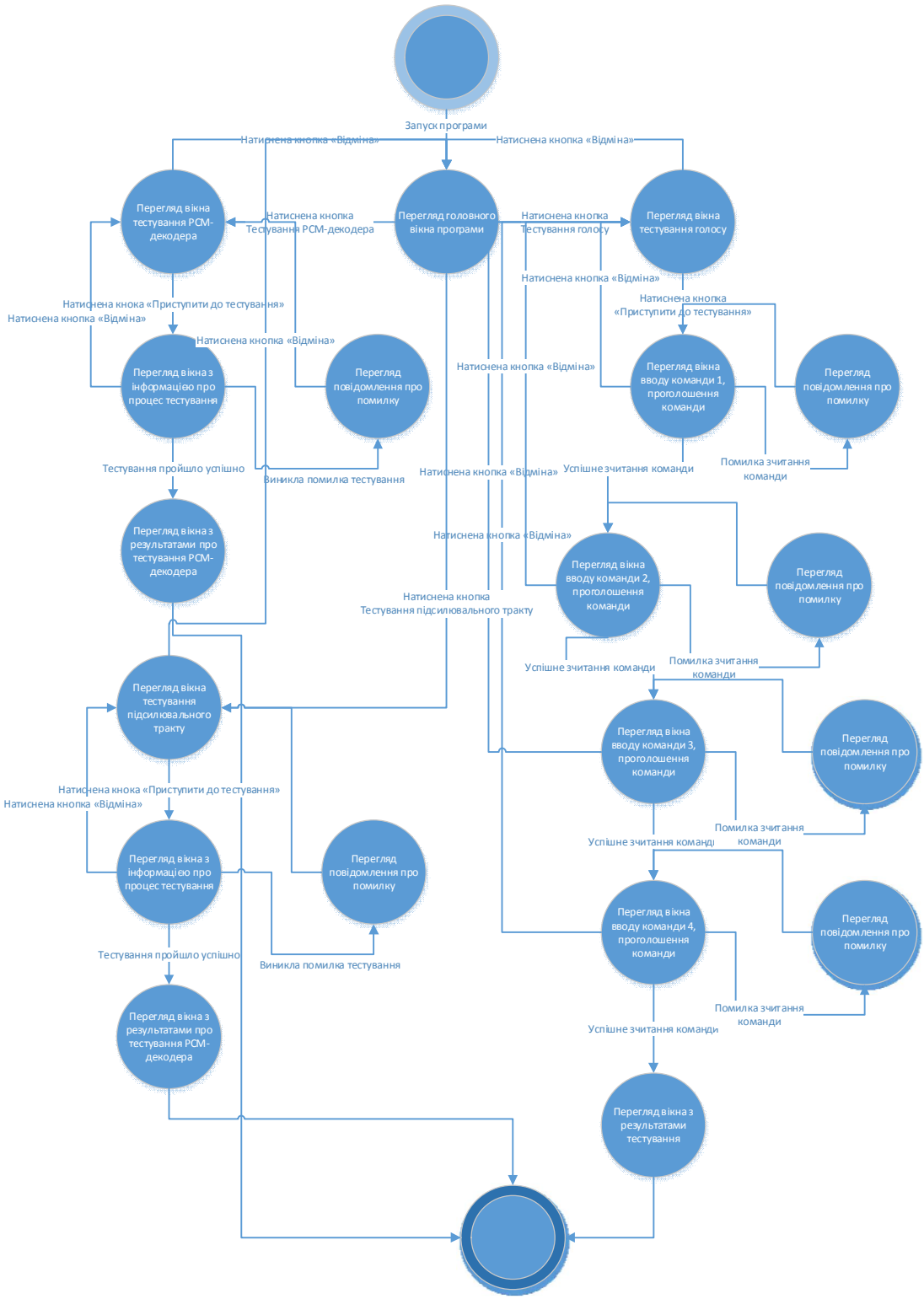


Рисунок 2.10 – Діаграма станів та переходів системи тестування цифрового аудіо-сигналу

Висновки до розділу 2

У розділі 2 була проведена адаптація для цифрового аудіо методу виявлення та локалізації фальсифікації цифрового зображення, заснованого на аналізі дослідження функції середньоквадратичного відхилення значень коефіцієнтів ДКП матриці цифрового зображення від їх повторно відквантованих значень з різними коефіцієнтами квантування, а також було визначено параметр, який використовується для відділення частини цифрового аудіо, що містить фальсифікацію від оригінальних частин.

РОЗДІЛ 3
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО АУДІО СИГНАЛУ, ЗБЕРЕЖЕНОГО У ФОРМАТІ ІЗ ВТРАТОЮ ІНФОРМАЦІЇ

3.1. Опис мови програмування та інтерфейс програмного продукту

Для реалізації програмного продукту було обрано пакет прикладних програм MATLAB, який використовується для рішення задач технічних обчислень, містить в собі засновані на матрицях структури даних, широкий спектр функцій та інтегроване середовище розробки.

Система MATLAB - це мова програмування високого рівня, що допускає роботу в режимі командного інтерпретатора, головним призначенням якого є виконання матричних обчислень.

Система MATLAB була створена компанією MathWorks в 1984 році як інтерактивна оболонка над пакетами підпрограм, написаних на мові FORTRAN, для вирішення лінійних систем (LINPACK) і дослідження проблеми власних значень (EISPACK). Надалі до MATLAB були додані пакети підпрограм для вирішення інших завдань обчислювальної математики, а також численні графічні інструкції, що відкривають перед користувачем широкі можливості для створення високоякісних двовимірної і тривимірної графіки.

Вхідна мова програмування MATLAB близька по синтаксису до сучасних систем програмування на базі універсальних алгоритмічних мов таких як FORTRAN, C або Java. І хоча MATLAB поступається цим мовам у швидкодії, унікальні бібліотеки чисельних методів і засобів візуалізації результатів обчислень, які в ньому містяться часто дозволяють користувачеві отримати кінцевий результат швидше, ніж при використанні традиційних мов програмування.

Система MATLAB має можливості як процедурної, так і об'єктно-орієнтованої мови програмування. Крім того, вона володіє засобами

інтерактивної розробки графічних інтерфейсів, в яких можуть бути присутні такі стандартні елементи, як меню, кнопки, перемикачі, лінійки прокрутки і.т.п.

На базі ядра MATLAB створені численні розширення, орієнтовані на вирішення завдань у спеціальних галузях науки і техніки. Ось лише деякі з них:

- Communications Toolbox - пакет, призначений для розробки цифрових і аналогових пристроїв передачі інформації.
- Data Acquisition Toolbox - пакет, що забезпечує взаємодію системи MATLAB в режимі реального часу з зовнішніми пристроями введення / виведення, такими як вимірювальні прилади, інтерфейсні плати і датчики.
- Filter Design Toolbox - пакет інструментів для побудови та аналізу цифрових фільтрів.
- Image Processing Toolbox - пакет, призначений для цифрової обробки растрових зображень.
- Optimization Toolbox - пакет підпрограм для вирішення лінійних і нелінійних задач оптимізації з великою кількістю невідомих.
- Partial Differential Equation Toolbox - пакет, призначений для чисельного розв'язання задач математичної фізики методом кінцевих елементів.

Основні характеристики:

- розробка високого рівня чисельних обчислень, візуалізації та розробка додатків;
- інтерактивне середовище для ітераційної розробки та вирішення графічних проблем;
- математичні функції лінійної алгебри, статистики, аналіз Фур'є, фільтрація, оптимізація, чисельне інтегрування, рішення звичайних диференціальних рівнянь;
- вбудована графіка для візуалізації даних та інструменти для створення користувацьких ділянок;
- розвиток інструментів для поліпшення якості коду і максимальної продуктивності;

- інструменти для створення додатків з призначеним для користувача графічним інтерфейсом;
- функції MATLAB для інтеграції на основі алгоритмів із зовнішніми програмами і такі мови, як C, Java,. NET і Microsoft Excel.

MATLAB для користувача надає значну кількість функціоналу для аналізування даних, що охоплює практично весь математичний арсенал.

MATLAB дозволяє вам отримувати доступ до даних з файлів, інших додатків, баз даних та зовнішніх пристроїв. Ви маєте можливість зчитувати дані з файлів таких основних форматів, як Microsoft Excel, текстових або двійкових файлів, зображень, аудіо і відеофайлів, наукових форматів (netCDF і HDF). Функції вводу-виводу дозволяють працювати практично з будь-яким форматом.

Використовуючи розширення MATLAB можна отримувати дані з різних пристроїв, таких як послідовний порт комп'ютера або звукова карта, а також потокові дані в реальному часі з вимірювальних пристроїв безпосередньо в MATLAB для аналізу та візуалізації.

MATLAB має можливості створювати спеціальні набори інструментів, що розширюють його функціональність.

Набори інструментарію є збіркою функцій, написаними мовою MATLAB що дає можливість вирішити задачі певного класу. Компанія Mathworks забезпечує інструментарій, що має прикладне значення в багатьох областях, зокрема: цифрове оброблення сигналів, зображень та даних; систем керування; фінансова аналітика; аналіз і синтез географічних карт; можливість збору та аналізу експериментальних даних; засоби розробки; візуалізація та уявлення даних; взаємодія із зовнішніми програмними продуктами; бази даних; наукові та математичні пакети; нейронні мережі; нечітка логіка; символьні обчислення.

Завдяки своїм особливостям MATLAB є найкращим вибором для вирішення нашого завдання.

Результатом проведеної роботи став програмний продукт «TestAudio», реалізований у середовищі MATLAB.

3.2. Аналіз засобів ідентифікації цифрової і аналогової апаратури запису сигналів.

На основі теорії криміналістичної ідентифікації були розглянуті шляхи створення засобів ідентифікації цифрової і аналогової апаратури запису із застосуванням мультимасштабного аналізу [14].

Апаратура запису сигналів (ідентифікований об'єкт) може бути ідентифікована за своїм паразитним параметрам, зокрема, по регулярним спектральним компонентам, що містяться у власних шумах записаних на цій апаратурі сигналограм (ідентифікуючі об'єкти). Але при цьому ідентифікуючими ознаками є місця розташування даних компонент на осі частот, а самі спектральні компоненти, що виділяються із спектру власних шумів сигналограми, є ідентифікованими ознаками.

Відомо, що опис фізичної побудови практично всіх об'єктів матеріальної природи носить фрактальний характер. І при цьому фрактали, що лежать в основі опису графічної побудови будь–якого об'єкта, індивідуальні. Ця властивість фракталів дозволяє застосувати їх в різних галузях науки, наприклад, в медичних дослідженнях. А апарат дослідження фрактальної структури базується на мультимасштабному аналізі.

У роботі показано, що і цифровий сигнал, записаний у сигналограмах, може бути виражений індивідуальною фрактальною структурою, що несе в собі індивідуальні ознаки апаратури, на якій вона записувалася і відтворювалася; показана змінність цієї структури при перезапису сигналограми з одного апарату на інший.

Для розвитку цієї ідеї було розроблено спеціалізоване програмне забезпечення "Фрактал", призначене для ідентифікації апаратури цифрового і аналогового запису (ідентифікація останньої реалізувалася при введенні аналогових сигналограмм в ЕОМ для аналізу).

Програма побудована на застосуванні вейвлетних базисів в мультимасштабному аналізі. В основу її побудови закладено принципи

виявлення та аналізу самоподібних структур, що виділялися з сигналограм на основі використання вейвлет–перетворення, і подальшого їх аналізу. При цьому в звуковому файлі спочатку виділялися паузи. Для цього використовувався багатопрохідний складний алгоритм з автоматичною корекцією порогу виділення. На виділених ділянках обчислювався вейвлет–спектр. Для цього застосовувалася операція згортки цих сигналів з вейвлетом Морлі, використовуваного в якості базису.

Виділення спектру проводилися з накопиченням. Аналізувався вейвлет–спектр виділених ділянок. За результатами аналізу будувалася вейвлет–спектрограма (скейлограма), як залежність квадрата коефіцієнтів вейвлет–перетворення від масштабного фактора (еквівалент частоти сигналу для вейвлет–спектрограми).

З скейлограми виділялися коефіцієнти вейвлет–перетворення, відповідні високочастотній області сигналу. При цій операції нижня частота сигналів в області виділення визначалася значенням частоти дискретизації вихідного звукового сигналу і максимальною частотою мовного сигналу. Виділена частина спектру представлялася у вигляді функції щільності розподілу ймовірностей (шляхом спеціального нормування). Отримана функція в системі іменується "Ідентифікатором апаратури запису". Дві такі функції, отримані, наприклад, з файлів зразкових (експериментальних) і досліджуваних записів, порівнювалися між собою за критерієм $\chi 2$. Результати порівняння виводилися у вигляді рішення про прийняття або відкидання гіпотези про ідентичність щільностей розподілу ймовірності.

При такій реалізації програми виникає проблема із недостатністю статистичного матеріалу, одержуваного з порівнюваних ділянок і необхідного для прийняття достовірного рішення. Особливо яскраво недолік такого підходу проявився при дослідженнях сигналограм з частотами дискретизації 8 і 11,025 кГц.

При виявленні точок монтажу можна підігнати всі види аналізу розподілу різних сигналів під один критерій. Це випливає з аналізу апроксимувати кривих

щільності ймовірності для сигналів з великою і малою частотою дискретизації. Так, для частот дискретизації нижче 16 кГц в більшості випадків нормальність розподілів не спостерігалася. У той же час, починаючи з частоти дискретизації 16 кГц і вище, досліджувані розподілення близькі або підпорядковуються нормальному закону.

Другий метод заснований на візуальному контролі експертом спеціальних сигналів, що виділяються на основі мультимасштабного аналізу по всій довжині сигналограми. Аналіз зводився до виявлення характерних візуальних "картинок", властивих місцям вставки сигналів з сигналограми. Для цього, як і при ідентифікації апаратури, з досліджуваної сигналограми по всій її довжині виділялися паузи і розраховувався спектр містивщихся в них сигналів. Але при цьому досліджувані сигнали попередньо розбиваються на базові інтервали по 512 відліків частоти дискретизації. Потім інтервали розбиваються на підінтервали по 64 відліку. На кожному з підінтервалов обчислюється вейвлет-спектр досліджуваних сигналів на базі вейвлета Морле і будується скейлограмма як вейвлет-спектр потужностей сигналів. При цьому застосовується 16 рівнів вейвлет-перетворення.

Для аналізу аудіозаписів також існують методи, що враховують додавання до записуваних сигналів шумів, утворених електричною мережею з частотою 50/60 Гц [15,21]. Ґрунтуючись на знанні технічних характеристик мікрофону, можна проводити аналіз шумів навколишнього середовища в момент проведення запису аудіо сигналу [20]. Порушення таких фонових складових може свідчити про навмисне порушення цілісності самого сигналу.

Розглянуті вище методи перевірки цілісності ЦА мають один вагомий спільний недолік, який властивий всім програмно-технічнім методам пасивного захисту інформації – жорстка прив'язаність до технічного пристрою, його властивостей або впливу оточуючих факторів на запис сигналу. Якщо не представляється можливим досліджувати пристрій фіксації, або не відомі умови, в яких проводилася зйомка або аудіо запис, то використовувати зазначені методи не можливо.

Більш широке поширення отримали програмні методи захисту інформації, які аналізують лише цифрову форму представлення самого сигналу, а тому не залежать від технічних характеристик пристроїв або людського фактору, як у програмно-технічних методах і методах експертного оцінювання.

Багато наукових досліджень присвячені аналізу цифрового аудіо (ЦА) на наявність фальсифікації за допомогою матричного аналізу [19].

В якості основного параметру, що визначає цифрове аудіо, виступали сингулярні числа блоків матриць, побудованих відповідним чином. Пропонується декілька способів двовимірного представлення цифрового аудіо з метою його аналізу на наявності фальсифікації розробленим методом.

Проводився аналіз впливу MPEG стиснення на параметри ЦА, представленого в матричному вигляді, для виділення таких характеристичних особливостей сингулярного спектру відповідної аудіо сигналу матриці, які можуть бути використані для вирішення задачі виявлення фальсифікації. Для цього автором реалізована психоакустична звукова модель, обґрунтований вибір найбільш доцільного з точки зору використовуваної звукової моделі матричного представлення ЦА, визначено характерні особливості параметрів, що визначають ЦА до і після стиснення.

В результаті на підставі встановлених властивостей власних значень блоків матриць ЦА стало можливим відрізнити сигнал, збережений без втрат інформації від частково відновленого або повністю відновленого після стиснення, що дозволило ефективно виявляти фальсифікацію в ЦА.

У відкритій пресі був запропонований метод виявлення фальсифікації «copy/paste» цифрового аудіо сигналу на основі загального матричного підходу до розв’язку задачі визначення несанкціонованого втручання в цифровий сигнал. Однак, цей метод можна використовувати лише для аудіо, збереженого у форматі без втрати інформації.

Дипломна робота заснована на дослідженні ефекту подвійного квантування і його використанні при виявленні фальсифікації цифрових зображень.

3.3 Інструкція користувача

Після запуску програмного продукту з’являється вікно, яке має з правої сторони панель кнопок , а з лівої сторони область для завантаження аудіо та області для дослідження цих аудіо.

Ліва панель містить наступні елементи:

Області для завантаження мають такі назви:

- «Audio»;

- «Image».

Права панель містить такі елементи:

- кнопки: «Open», «Graphic», «Analise» ;

- текстове поле: «Введите пороговое значение».

Інтерфейс програми є зручним і легким у використанні, максимально спрощений для користувача. Даний інтерфейс показано на рисунку 3.1.

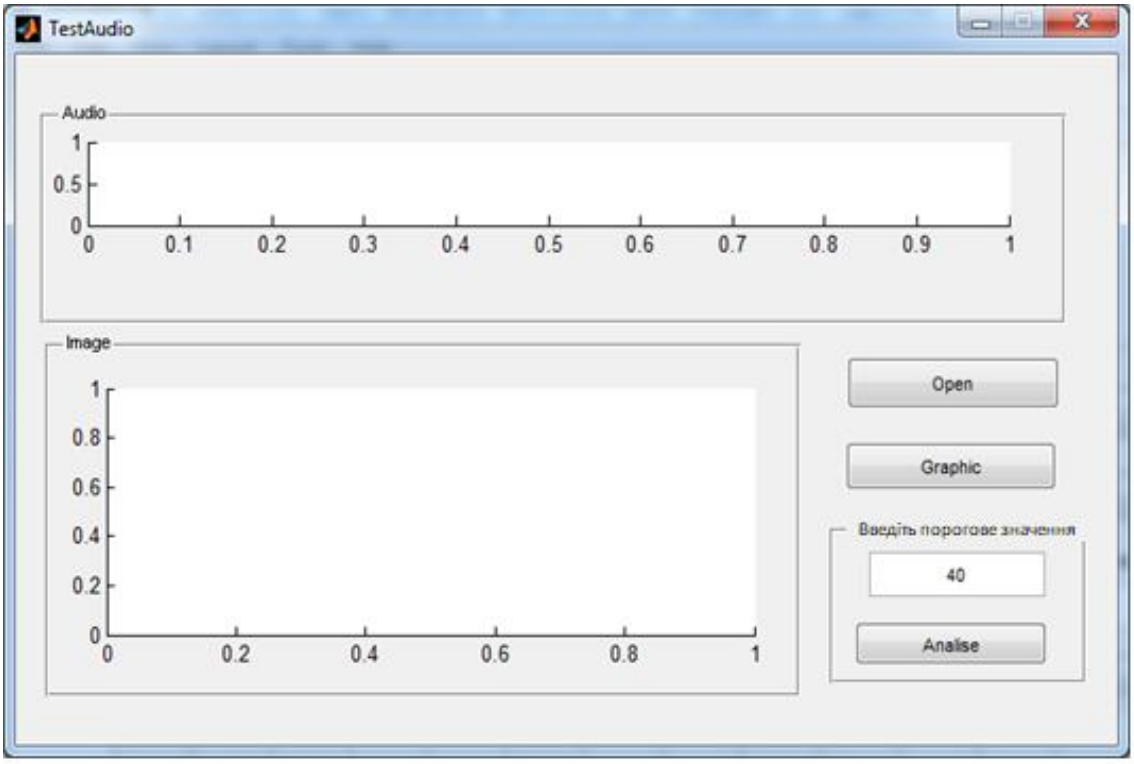


Рисунок 3.1 − Інтерфейс програмного продукту

Розглянемо далі роботу програми.

Після натиснення кнопки «Open», яка знаходиться на панелі справа, з'являється нове вікно, у якому обирається потрібний аудіо запис (рисунок 3.2). Обраний аудіо запис з'являється у верхній області для завантаження «Audio» (рисунок 3.3).

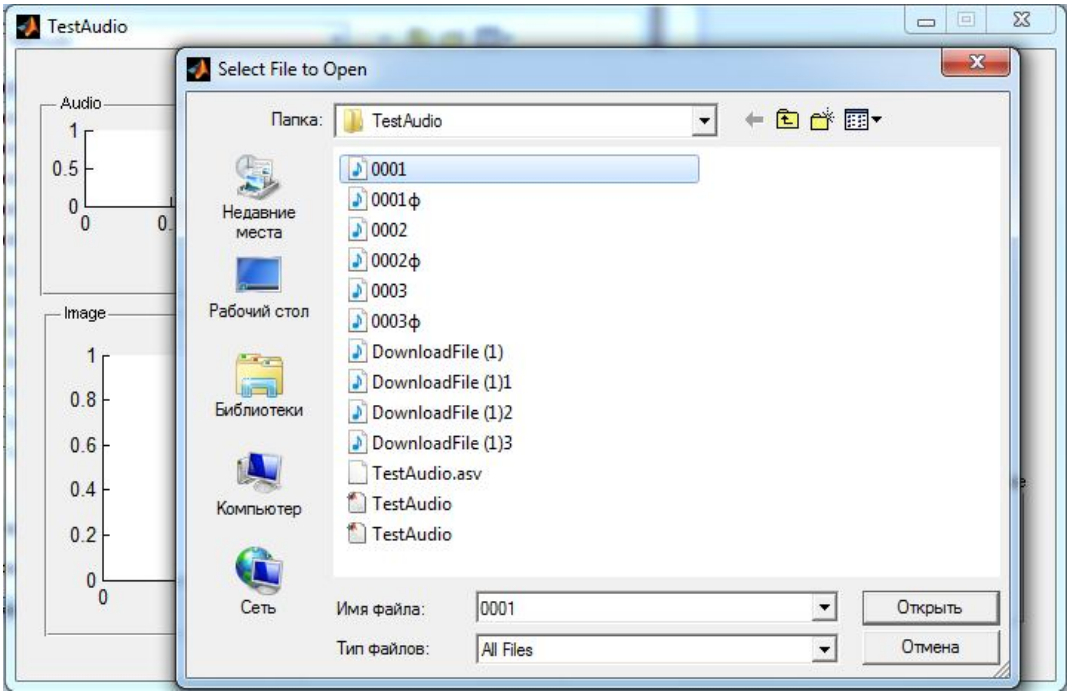


Рисунок 3.2 − Вибір аудіо

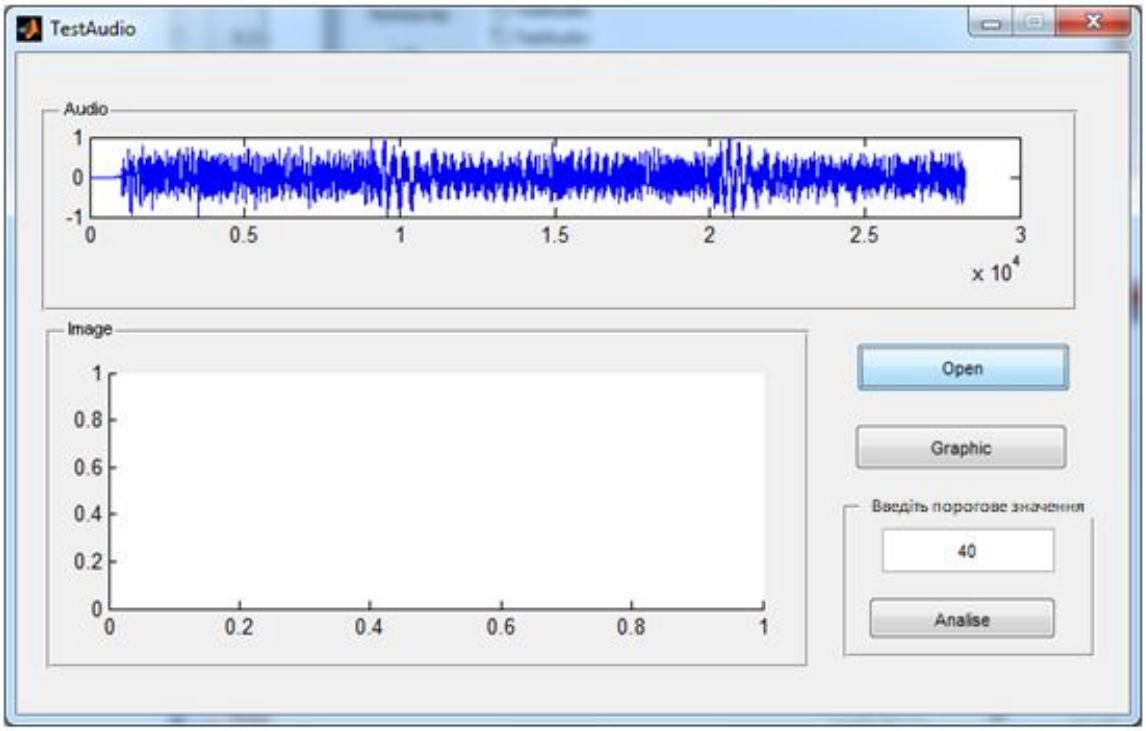


Рисунок 3.3 − Завантаження аудіо

При натисненні кнопки «Graphic» в області «Image» з'являється графік, побудований для даного аудіо запису (рисунок 3.4).

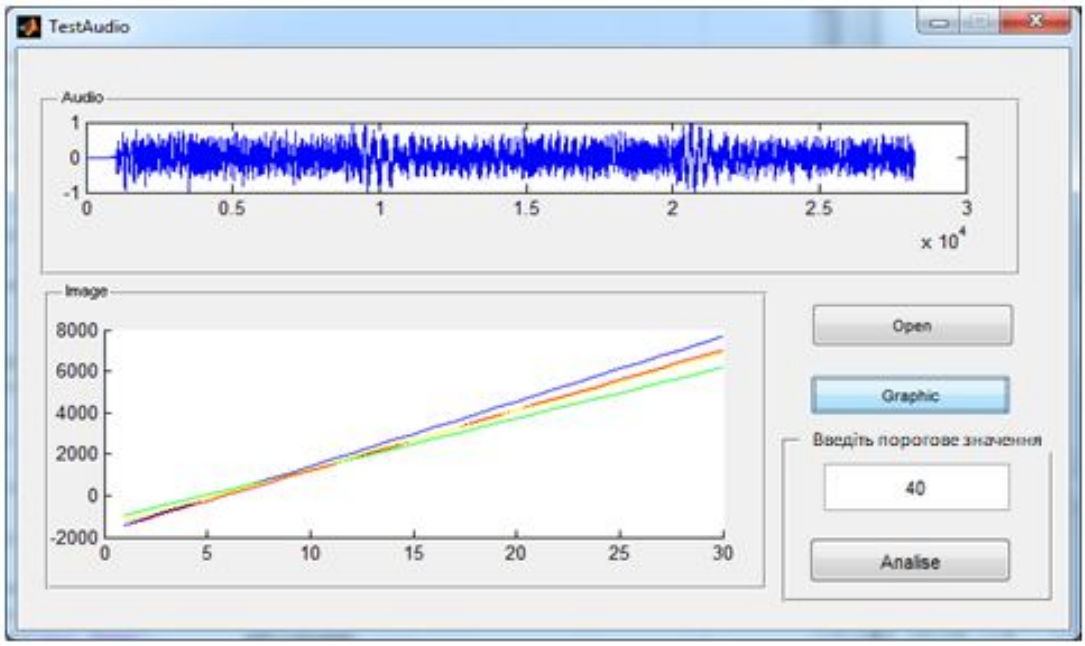


Рисунок 3.4 − Графік для аудіо без фальсифікації

При натисненні кнопки «Analise», обране аудіо аналізується на наявність фальсифікації. На рисунку 3.5 наведено приклад аудіо, яке не було сфальсифіковано.

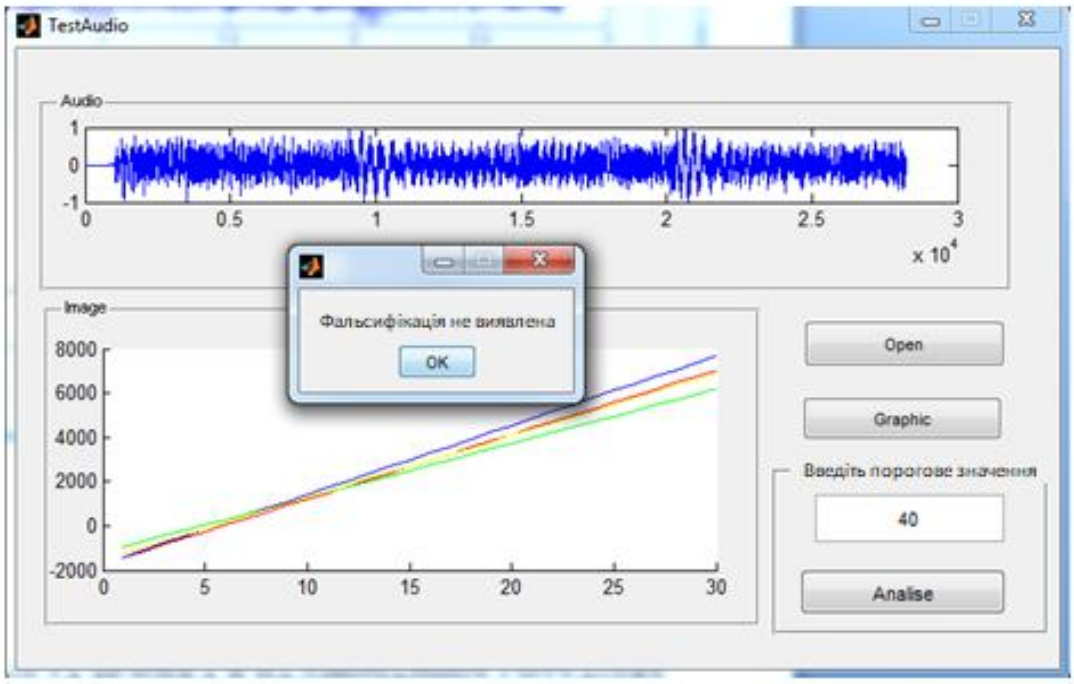


Рисунок 3.5 − Виявлення фальсифікації у аудіо

3.4. Тестування програмного продукту

Приклад роботи програми для фальсифікованого аудіо. Обирається потрібний аудіо запис (рисунок 3.6) та завантажуєтья в область «Audio» (рисунок 3.7).

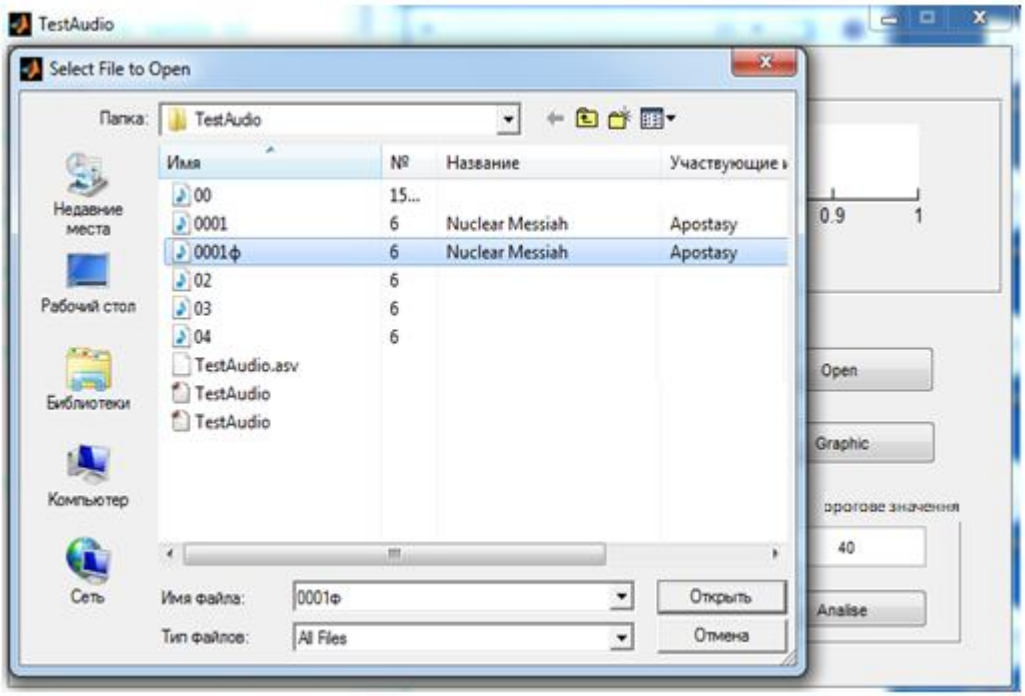


Рисунок 3.6 − Вибір аудіо

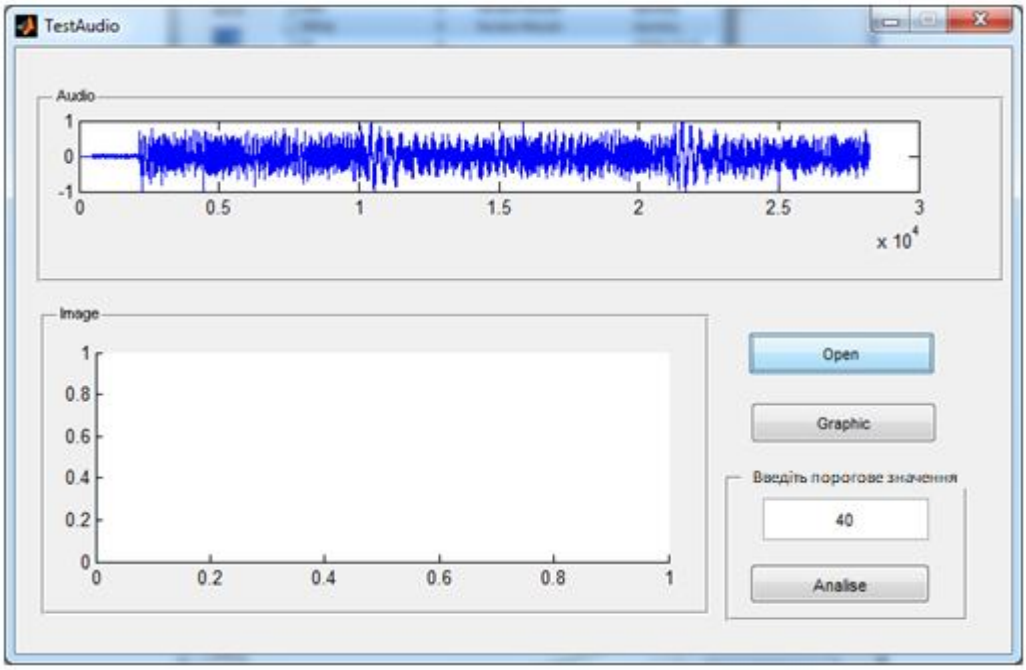


Рисунок 3.7 − Завантаження аудіо

При натиснені кнопки «Graphic» в області «Image» з'являється графік, побудований для даного аудіо запису (рисунок 3.8).

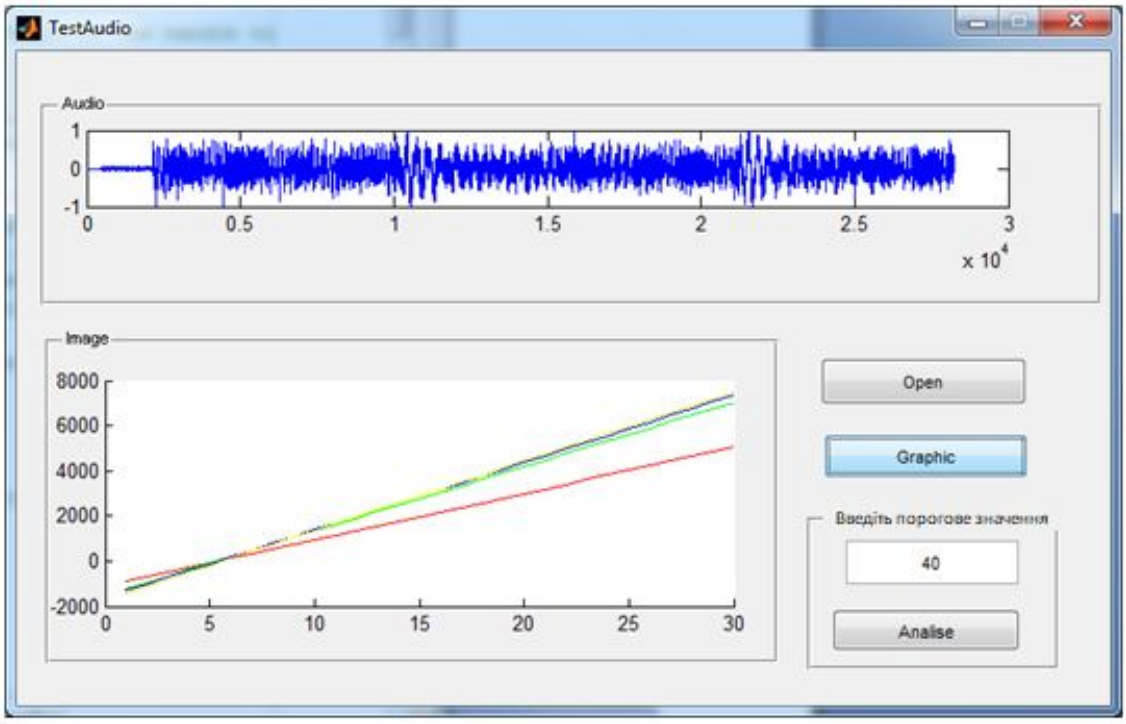


Рисунок 3.8 − Графік для аудіо з фальсифікацією

Для проведення аналізу аудіо запису є можливість самостійно вводити порогове значення у текстовому полі - «Введите пороговое значение». На рисунку 3.9 наведений приклад, коли порогове значення дорівнює 38.

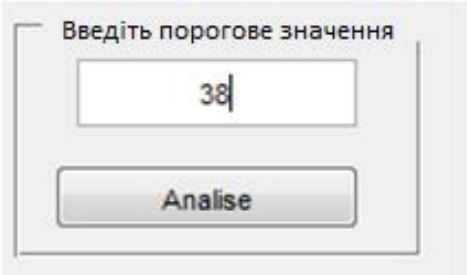


Рисунок 3.9 − Виявлення фальсифікації у аудіо

Далі перевіряємо наявність фальсифікації у аудіо, обравши порогове значення та натиснувши кнопку «Analise». На рисунку 3.10 аналізується аудіо, запис в якому фальсифікований перший ПБС, на рисунку 3.11 аналізується аудіо запис, в якому фальсифікований третій ПБС.

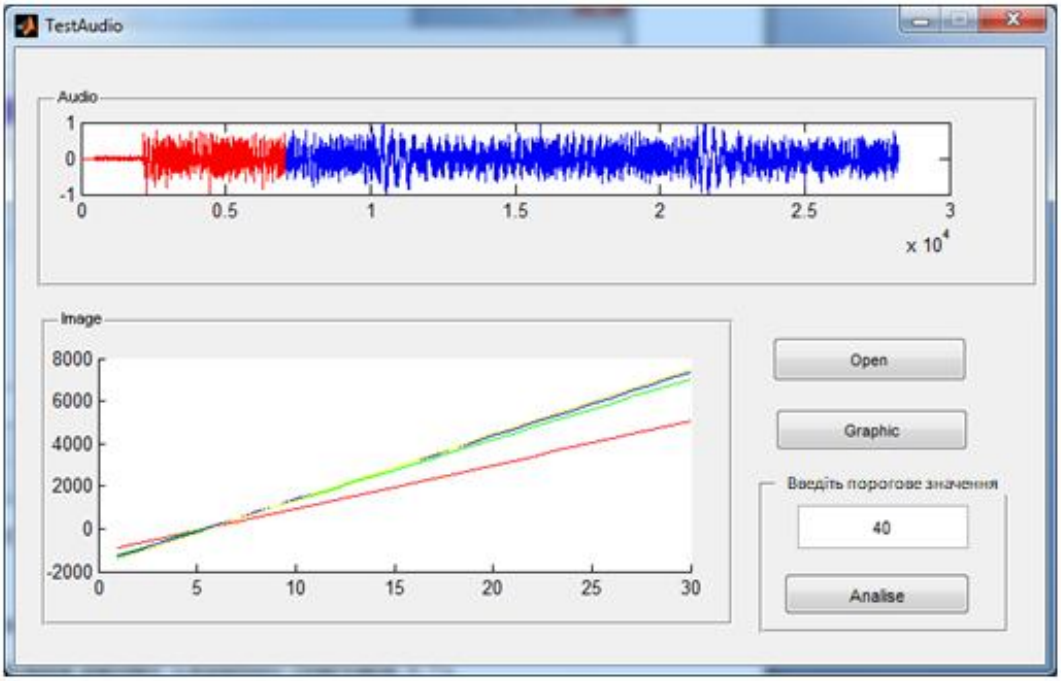


Рисунок 3.10 − Виявлення фальсифікації у аудіо

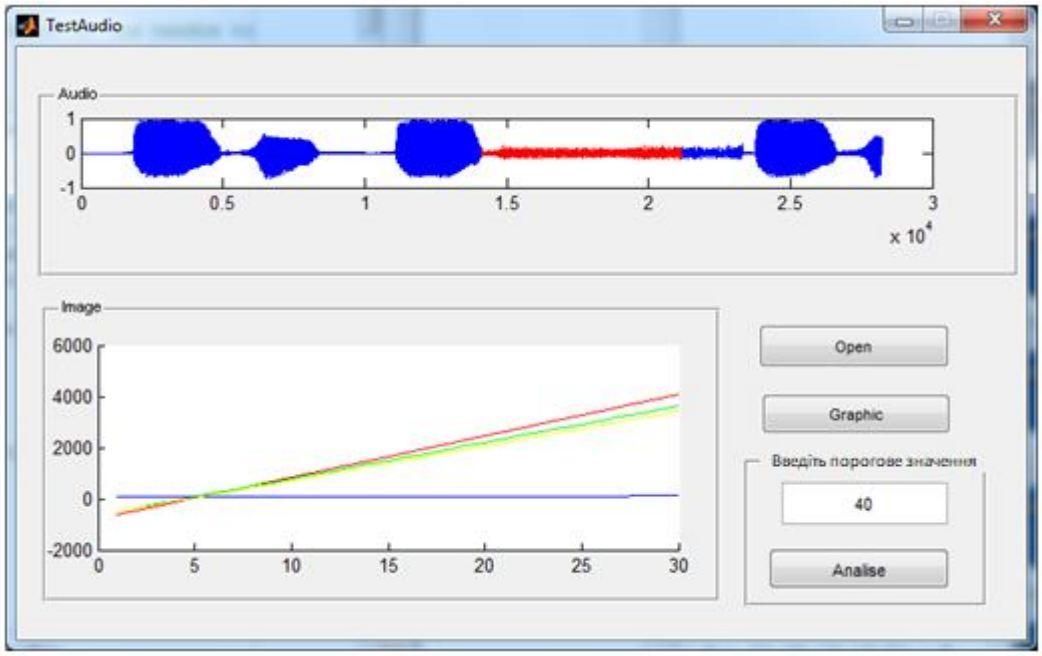


Рисунок 3.11 − Виявлення фальсифікації у аудіо

Програмний продукт TestAudio надає ефективний висновок щодо фальсифікації цифрового аудіосигналу, має зручний інтерфейс, а результати аналізу є наочними.

Значною перевагою використання розробленого програмного продукту є можливість та зручність його використання навіть недосвідченими користувачами, адже окрім наглядності подачі результату формується висновок про вміст чи відсутність фальсифікації робиться автоматично. Тобто, використання програмного продукту TestAudio на практиці для будь-якого підприємства дозволяє виявляти наявність чи відсутність фальсифікації цифрового аудіосигналу без залучення до цього процесу позаштатних висококваліфікованих фахівців, що в кінцевому підсумку призводить до заощадження коштів при збереженні достовірності результатів аналізу.

Висновки до розділу 3.

У даному розділі проведений огляд розробленого в рамках дипломної роботи програмного продукту, описано інтерфейс користувача та тестування, описана програмна реалізація процесу виявлення фальсифікації цифрового аудіо-сигналу, обґрунтовано вибір мови програмування, наведена інструкція користувача програмного продукту та описано тестування розробленого програмного продукту.

РОЗДІЛ 4
ПАСИВНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ЇХ КЛАСИФІКАЦІЯ ТА ПЕРЕВІРКА ЦІЛІСНОСТІ ЦИФРОВИХ СИГНАЛІВ ЯК МЕТОД ПАСИВНОГО ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Аналіз існуючих методів перевірки цілісності цифрових сигналів

Задачі перевірки цілісності цифрових сигналів є надзвичайно значущими та актуальними. У зв'язку із зростаючою кількістю, різноманітністю та доступністю засобів фіксації цифрових сигналів найбільш переважними для виявлення порушення цілісності цифрових сигналів виявляються програмні методи пасивного захисту інформації перед програмно-технічними методами та методами експертного оцінювання. Одним з нових і надзвичайно перспективних методів виявлення фальсифікації ЦС є метод, заснований на дослідженні особливостей проявлення DQ-ефекту на гістограмах коефіцієнтів ДКП. Більшість існуючих методів виявлення фальсифікації та доказу цілісності не мають достатнього теоретичного обґрунтування або не враховують специфічність аналізу ЦС у реальних умовах функціонування системи: при наявності шумів округлення значень ЦС або процесу друку та сканування для ЦЗ. Окрім цього жодний з методів, доступних з відкритих джерел, не має орієнтації на виявлення фальсифікації малих розмірів, коли розміри фальсифікації порівняні з розміром блоків при стандартному розбитті сигналу.

Висновком з проведеного на основі даних, отриманих з відкритих джерел, аналізу методів перевірки цілісності цифрових сигналів та їх теоретичної обґрунтованості є необхідність розробки теоретично обґрунтованого практичного методу перевірки цілісності ЦС, що давав би можливість наступної локалізації області порушення цілісності, в тому числі малих розмірів, у випадку її порушення, в реальних умовах функціонування системи для ЦЗ, ЦВ та ЦА.

Гістограма коефіцієнтів ДКП матриці ЦЗ після подвійного квантування має одну з двох можливих візуальних відмінностей проявлення DQ-ефекту: у

вигляді піків та ненульових впадин та у вигляді піків та нулів. Умови його проявлення у тому чи іншому вигляді на гістограмах коефіцієнтів ДКП ЦС є основоположними для створення практичного методу перевірки цілісності ЦС.

Після другого квантування значення коефіцієнтів ДКП визначаються за формулою

$$u^{(2)} = \left[\frac{u^{(1)} q^{(1)}}{q^{(2)}} \right] \qquad (4.1)$$

де $u^{(1)}$, $u^{(2)}$ — значення коефіцієнта ДКП u після першого та другого квантування без відновлення відповідно, $u^{(1)}, u^{(2)} \in Z$;

$q^{(1)}, q^{(2)}$— відповідні u коефіцієнти першого та другого квантування, $q^{(1)}, q^{(2)} \in Z$;

[•]— операція округлення аргументу до найближчого цілого.

Нехай H, $H^{(1)}$ та $H^{(2)}$ — гістограми коефіцієнтів ДКП ЦЗ, що відповідають обраній довільним чином частоті, до першого квантування та після першого та другого квантування без відновлення відповідно.

Замість (4.1) розглянемо функцію загального вигляду:

$$y(x) = \left[\frac{q^{(1)}}{q^{(2)}} x \right] \qquad (4.2)$$

де $x \in R$, $q^{(1)}$, $q^{(2)} \in N$.

Розглянемо особливості поведінки $y(x)$ для $x > 0$, так як для $x < 0$ властивості функції будуть аналогічними. Область значень функції $y(x)$ у цьому випадку буде підмножиною $N \cup \{0\}$.

З області визначення функції (4.2) оберемо тільки ті значення x_i, котрі задовольняються умові $x_i = i$, $i \in N$ та, обчислюючи значення функції у цих точках, отримаємо набір значень $y(1), y(2), \ldots y(x_i), \ldots$, де

$$y(x_i) = \left[\frac{q^{(1)}}{q^{(2)}} x_i \right], \; y(x_{i+1}) = \left[\frac{q^{(1)}}{q^{(2)}} x_{i+1} \right] = \left[\frac{q^{(1)}}{q^{(2)}} (x_i + 1) \right].$$

Використовуючи отриманий набір, побудуємо сплайн першого порядку $\bar{y}(x)$ для функції $y(x)$. Для побудови сплайну на кожному відрізку $[x_i, x_{i+1}]$, $i \in N$, знайдемо рівняння прямої, що проходить через точки $\left(x_i, \left[\frac{q^{(1)}}{q^{(2)}} x_i\right]\right)$ та $\left(x_{i+1}, \left[\frac{q^{(1)}}{q^{(2)}}(x_i+1)\right]\right)$:

$$\bar{y}(x) = \left(\left[\frac{q^{(1)}}{q^{(2)}}(x_i+1)\right] - \left[\frac{q^{(1)}}{q^{(2)}} x_i\right]\right)x + \left[\frac{q^{(1)}}{q^{(2)}} x_i\right] - \left(\left[\frac{q^{(1)}}{q^{(2)}}(x_i+1)\right] - \left[\frac{q^{(1)}}{q^{(2)}} x_i\right]\right)x_i$$

Введемо наступні поняття:

Визначення 1. Нехай $A \subseteq Z$, де Z — множина цілих чисел. Будемо називати множину A *суцільною цілою підмножиною(СЦП)*, якщо для будь-яких $z_1, z_2 \in A$ усі цілі значення $z \in Z$ такі, що $z_1 < z < z_2$, належать множині A, і *не суцільною цілою підмножиною (НСЦП)*, якщо існують такі $z_1, z_2 \in A$, для котрих знайдеться $z \in Z$ таке, що $z_1 < z < z_2$, але $z \notin A$.

Справедливі наступні теореми, що є критеріями проявлення DQ-ефекту.

Теорема 1. Для того, щоб область значень функції (2) була НСЦП необхідно і достатньо, щоб $q^{(1)} > q^{(2)}$.

З теореми 1 випливає, що при $q^{(1)} > q^{(2)}$ і тільки тоді, область значень функції (4.2), а значить і функції (1), є НСЦП. Нехай $u_{i-1}^{(2)} < u_i^{(2)} < u_{i+1}^{(2)}$ і при цьому значення $u_{i-1}^{(2)}$, $u_{i+1}^{(2)}$ належать області значень функції (1), а $u_i^{(2)}$ не належить. Тоді на гістограмі $H^{(2)}$ стовбець, що відповідає значенню $u_i^{(2)}$ буде нульовим, тобто з'явиться так званий нуль. А значенням, що належать області значень функції (1) на гістограмі $H^{(2)}$ буде відповідати ненульовий стовбець, так званий пік.

Теорема 2. Для того, щоб існували такі значення аргументу функції (4.2) $x_i, x_j, x_i \neq x_j$, що $y(x_i) = y(x_j)$, необхідно і достатньо, щоб $q^{(1)} < q^{(2)}$.

З теореми 2 випливає, що при $q^{(1)} < q^{(2)}$ і тільки тоді, функція (4.2), а значить і функція (1), мають повторювані значення. Нехай $u_i^{(1)}$ і $u_j^{(1)}$,

$u_i^{(1)} \neq u_j^{(1)} : u^{(2)}\left(u_i^{(1)}\right) = u^{(2)}\left(u_j^{(1)}\right) = u_i^{(2)}$. Це значить, що на гістограмі $H^{(2)}$ стовбець, що відповідає значенню $u_i^{(2)}$ буде мати всі значення з стовбців $H^{(1)}$, що відповідають значенням $u_i^{(1)}$ і $u_j^{(1)}$. Це означає, що на гістограмі $H^{(2)}$ з'явиться так званий пік, що відповідає значенню $u_i^{(2)}$, а усім іншим значенням на гістограмі будуть відповідати так звані ненульові впадини.

Зауваження 1. Доказ теорем для функції загального вигляду без прив'язки до коефіцієнтів ДКП ЦС та форми представлення ЦС, дозволяє говорити про особливості проявлення DQ-ефекту для ЦС, що зберігаються не тільки у форматі JPEG, а й у всіх інших форматах, що використовують квантування при стисненні, наприклад, у форматі для збереження цифрового аудіо.

Характер проявлення DQ-ефекту на гістограмах коефіцієнтів ДКП ЦС можна виявити незалежно від початкових значень коефіцієнтів ДКП, так як виникнення нулів та піків на гістограмах, характерне для DQ-ефекту, є саме періодичним, що не властиве для довільного ЦС.

Проведені дослідження внеску різних частот в проявлення ефекту подвійного квантування та чутливості різних частот до збурних дій показали, що у ході проведення аналізу DQ-ефекту розгляд внесків високих та деяких середніх частот у його проявлення є недоцільним. Це дозволяє значно зменшити кількість виконуваних операцій та покращити якість перевірки цілісності ЦС при роботі запропонованого нижче алгоритму, в якому замість 64 аналізуються 32 гістограми.

Проведений повний аналіз проявлення DQ-ефекту на гістограмах коефіцієнтів ДКП ЦС в реальних умовах функціонування системи з урахуванням збурних факторів: введення значень яскравості пікселів після зворотного ДКП у діапазон [3, 255] в процесі відновлення ЦС після першого квантування; високочастотного шуму, нелінійних спотворень, геометричних деформацій, які включають у себе обрізку, повороти та масштабування, що виникають в процесі друку та сканування (ПДС) ЦЗ. Виявлено, що вказані шуми для нижніх та середніх частот не перевищують деяке порогове значення, на

відміну від збурень, що виникають через фальсифікацію. В наслідок чого, при побудові метода перевірки цілісності ЦЗ, заснованого на використанні DQ-ефекту, при врахуванні наслідків ПДС та шуму округлення необхідно враховувати лише процес обрізки. Для врахування процесу обрізки запропоновано проводити перевірку цілісності ЦЗ декілька разів, поступово зрушуючи сітку розбиття на блоки.

4.2 Класифікація та перевірка цілісності цифрових сигналів як метод пасивного захисту інформації

На основі отриманих теоретичних відомостей розроблені методи перевірки цілісності та уточнення локалізації області порушення цілісності будь-якого ЦС (ЦЗ, ЦВ, ЦА), при стисненні якого використовується квантування, працюючі у реальних умовах функціонування системи.

Для визначеності далі розглядається випадок, коли перший коефіцієнт квантування коефіцієнтів ДКП матриці ЦЗ більший за другий.

На практиці сумніви щодо автентичності ЦЗ часто виникають за рахунок підозр у фальсифікації конкретної його підобласті. Враховуючи це, а також з метою посилення проявлення порушень DQ-ефекту (у випадку порушення цілісності) пропонується розбити початкове зображення на декілька областей — підблоків сигналу (ПБС) — однакового розміру та проаналізувати проявлення DQ-ефекту для кожної частини окремо.

Сформульовані основні вимоги до побудови ПБС :

1. Межі ПБС не мають порушувати початкову сітку розбиття ЦЗ на блоки 8×8;
2. Усі ПБС мають бути одного розміру (ці розміри мають певним чином співвідноситися з розмірами області, що підозріла на фальсифікацію);
3. Бажано, щоб підозріла на наявність фальсифікації область (області) локалізувалася в одному ПБС (чи щоб таких ПБС було якомога менше);

4. Обов'язково необхідно виділити більше двох ПБС, перетин яких з областю, підозрілою на фальсифікацію, порожній. Рекомендована кількість ПБС — 3-4.

Для врахування шумів округлення та ПДС з використанням більше ніж 300 ЦЗ експериментально встановлене порогове значення p (табл. 4.1). Якісна роль цього порогового значення полягає у відділенні шуму навмисного змінення від природного шуму: якщо кількість порушень – вилетів ——«ідеального» проявлення DQ-ефекту перевищує значення p, це говорить на користь навмисного порушення цілісності ЦЗ; кількість вилетів, менша чи рівна p трактується як спотворення DQ-ефекту за рахунок ненавмисних збурюючих дій.

Таблиця 4.1 – Рекомендовані значення порогового значения p в залежності від розмірів ПБС

Розмір ПБС, пікселів	Значення p в залежності від шумів:	
	округлення	округлення і ПДС
128×128	5	20
96×96	4	15-18
64×64	2	10

Алгоритм визначення максимального коефіцієнту порушення цілісності сигналу (алгоритм ВМКПЦС).

b) Розбити матрицю ЦЗ на m ПБС.

c) Створити масив $V: V(i)=0,\ i=\overline{1,\ m}$.

d) Для i-го ПБС $\left(i=\overline{1,m}\right)$:

a. Розбити на блоки 8×8 пікселів;

b. Обчислити коефіцієнти ДКП;

c. Для j-й частоти $\left(j=\overline{1,\ 32}\right)$:

1) Побудувати гістограму відповідних їй коефіцієнтів ДКП;

2) Визначити кількість ненульових значень у нулях гістограми — вилетів $v(j)$;

3) Якщо $v(j) > p$, то $V(i) = V(i) + v(j)$, (p визначається з табл. 4.1).

e) Для кожного ПБС обчислити значення коефіцієнта порушення цілісності сигналу (КПЦС) для i-го ПБС:

$$K(i) = \frac{V(i)}{\sum_{i=1}^{m} V(i)} 100\%$$

f) Визначити максимальне значення КПЦС $K_{\max}$ і номер відповідного ПБС f:

$$[K_{\max}, f] = \max_{i=1,\, m} K(i)$$

Розроблений алгоритм ВМКПЦС служить основою для алгоритмів перевірки цілісності та уточнення локалізації області порушення цілісності ЦЗ.

Обчислювальний експеримент проводився у середовищі Matlab. Для експерименту були обрані 200 зображень. Спочатку припустима область фальсифікації мала розміри 50×50. Відповідно до вимог 1-4 ЦЗ розбивалося на ПБС 128×128.

З результатів обчислювального експерименту було встановлено наступне:

1. Для *фальсифікованих* ЦЗ ПБС, що містить фальсифікацію, у 98% випадків визначався зі значенням КПЦС більшим 70%;

2. Для *нефальсифікованих* ЦЗ найбільш підозрілий ПБС у 98% випадків мав значення КПЦС менше 60%.

КПЦС є числовим параметром, що характеризує ПБС ЦЗ, значення котрого дозволяє відділити фальсифіковану частину зображення від нефальсифікованої в умовах аналізу DQ-ефекту. Якщо значення КПЦС i-го ПБС $K_i > 70\%$, то ЦЗ містить фальсифікацію; якщо найбільше серед усіх значення КПЦС для ПБС $K_i < 60\%$, то ЦЗ не підлягало навмисним змінам.

Зауваження 2. Як показує обчислювальний експеримент, при зменшенні розмірів області порушення цілісності (ОПЦ) зі збереженням розмірів ПБС

КПЦС для фальсифікованого ПБС може бути значно нижчим 70%, що призводить до необхідності встановлення відповідності між розмірами припустимої ОПЦ та ПБС для забезпечення ефективної роботи запропонованого алгоритму.

В результаті перевірки цілісності 100 *нефальсифікованих* ЦЗ та 100 *фальсифікованих* ЦЗ з вбудовою ОПЦ різних розмірів при розбитті їх на ПБС 128×128, 96×96 та 64×64 пікселів виявлено (табл. 4.2), що:

1. КПЦС фальсифікованого блока приймає значення менше 70%, коли ОПЦ складає менше 5% від площі ПБС, що аналізується;

2. При проведенні перевірки цілісності нефальсифікованого ЦЗ значення КПЦС не перевищує 60% для будь-якого розміру ПБС.

В таблицях наведені найбільш характерні результаті перевірки цілісності 100 фальсифікованих та 100 оригінальних зображень.

Таблиця 2–Значення КПЦС для різних розмірів ПБС у нефальсифікованих ЦЗ.

Розмір ПБС, пікселів.	КПЦС,%									
	1	2	3	4	5	6	7	8	9	10
128×128	20	33,33	25	16,67	60	37,5	50	50	33,33	33,33
96×96	25	37,5	33,33	20	50	50	33,33	25	50	30
64×64	25	16,67	16,67	16,67	16,67	25	16,67	16,67	20	16,67

Виходячи з результатів обчислювального експерименту, площа ОПЦ має складати не менш 5% від площі ПБС. У цьому випадку значення 60% і 70% можна використовувати як порогові значення для КПЦС для визначення наявності чи відсутності фальсифікації ЦЗ.

Базовий алгоритм перевірки цілісності ЦЗ.

1. Повторити кроки алгоритму ВМКПЦС.

2. Зробити висновок про наявність чи відсутність порушення цілісності ЦЗ:

2.1. Якщо значення $K_{\max} > 70\%$, то ЦЗ містить ОПЦ в ПБС з номером f;

2.2. Якщо значення $K_{\max} < 60\%$, то цілісність ЦЗ не порушена.

Результатом роботи методу перевірки цілісності ЦЗ є висновок про наявність чи відсутність ОПЦ ЦЗ та, у випадку наявності ОПЦ, номер ПБС, що її містить. При необхідності наступним кроком перевірки цілісності ЦЗ є більш точна локалізація ОПЦ. Для вирішення проблеми більш точної локалізації ОПЦ в ПБС пропонується віртуально збільшити вклад ОПЦ в фальсифікований ПБС, що досягається за допомогою побудови так званих відображаючих матриць (ВМ).

Будувати ВМ для ПБС, що аналізується, пропонується наступним чином: не порушуючи початкову сітку розбиття на блоки 8×8 пікселів розділити матрицю ПБС по вертикалі (горизонталі) на дві, по можливості, рівні частини і симетрично відобразити спочатку праву частину наліво (1-а ВМ), а потім ліву частину вправо (2-а ВМ) (спочатку нижню частину наверх (3-а ВМ), а потім верхню частину вниз (4-а ВМ)).

В результаті отримуємо чотири матриці, в яких містяться продубльовані права, ліва, нижня та верхня частини матриці ПБС ЦЗ, і котрі мають розмір початкового фальсифікованого ПБС. Таким чином, якщо ВМ відповідають частині ПБС, що містить ОПЦ, то внесок ОПЦ в фальсифікований ПБС може збільшитися вдвічі. ВМ можна будувати не тільки дублюванням верхньої, нижньої, лівої та правої половин ПБС ЦЗ, а й чотирикратним повторенням чвертей зображення та іншими способами дублювання.

Побудова ВМ, як спосіб віртуального збільшення внеску ОПЦ у фальсифікований ПБС дозволяє: зберегти показність вибірки значень коефіцієнтів ДКП за рахунок збереження розмірів початкового ПБС; не тільки більш точно локалізувати, але й виявити ОПЦ навіть малого розміру (але як показує обчислювальний експеримент, більшу ніж 10×10 пікселів незалежно від розміру ПБС); змінюючи спосіб дублювання при побудові ВМ можна покращувати локалізацію ОПЦ. Окрім цього, при використанні ВМ розташування ОПЦ в ПБС не впливає на можливість її більш точної локалізації.

Зауваження 3. При використанні способу віртуального збільшення внеску ОПЦ в фальсифікований ПБС, що аналізується, як показує обчислювальний експеримент, значення КПЦС для фальсифікованих (нефальсифікованих) ВМ перевищує (не перевищує) 25% (10%), якщо ОПЦ міститься не більш ніж у трьох ВМ. Якщо ОПЦ міститься у всіх чотирьох ВМ (тобто розташована посередині фальсифікованого ПБС), то значення КПЦС для всіх ВМ перевищує 10%.

Для більш точної локалізації ОПЦ у зміненому ПБС ЦЗ пропонується наступний алгоритм.

Алгоритм уточнення локалізації області порушення цілісності.

1. По наявній матриці фальсифікованого ПБС ЦЗ побудувати 4 ВМ, $m = 4$.

2. Повторити кроки 2-4 алгоритму ВМКПЦС, аналізуються отримані ВМ.

3. По значеннях КПЦС для ВМ уточнити локалізацію ОПЦ в ПБС, що аналізується:

3.1. Якщо для двох чи трьох ВМ значення КПЦС більше 25%, а для інших менше 10%, то розташування ОПЦ визначається по тим ВМ, КПЦС яких більший 25%;

3.2. Якщо для усіх чотирьох ВМ значення КПЦС більше 10%, то ОПЦ знаходиться всередині ПБС, що аналізується.

При проведенні обчислювального експерименту проводилося уточнення локалізації ОПЦ для 200 зображень. У 99% випадків уточнення локалізації ОПЦ було проведене вірно.

Таким чином, розроблені методи перевірки цілісності та уточнення локалізації області порушення цілісності ЦЗ, що дозволяють ефективно детектувати наявність та локалізувати ОПЦ, в тому числі малих розмірів, в реальних умовах функціонування системи.

Для перевірки цілісності ЦВ пропонується наступна адаптація методів перевірки цілісності ЦЗ та уточнення локалізації області порушення цілісності:

1. Відео послідовність, що аналізується, представити у вигляді послідовності кадрів, виділити ключові кадри;

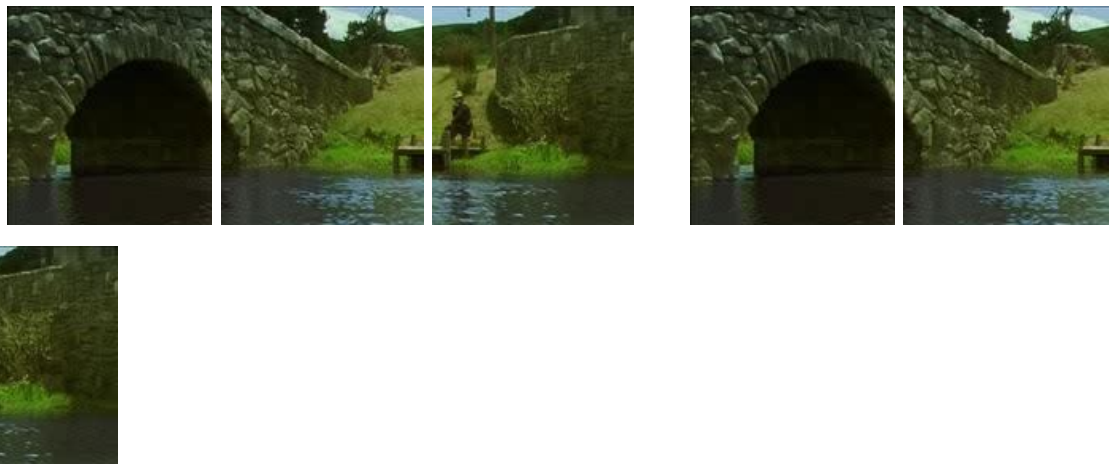
2. Кожний ключовий кадр піддати аналізу на наявність фальсифікації за допомогою базового алгоритму перевірки цілісності ЦЗ;

3. При виявленні у кадрі фальсифікованого ПБС провести більш точну локалізацію ОПЦ за допомогою алгоритму уточнення локалізації ОПЦ.

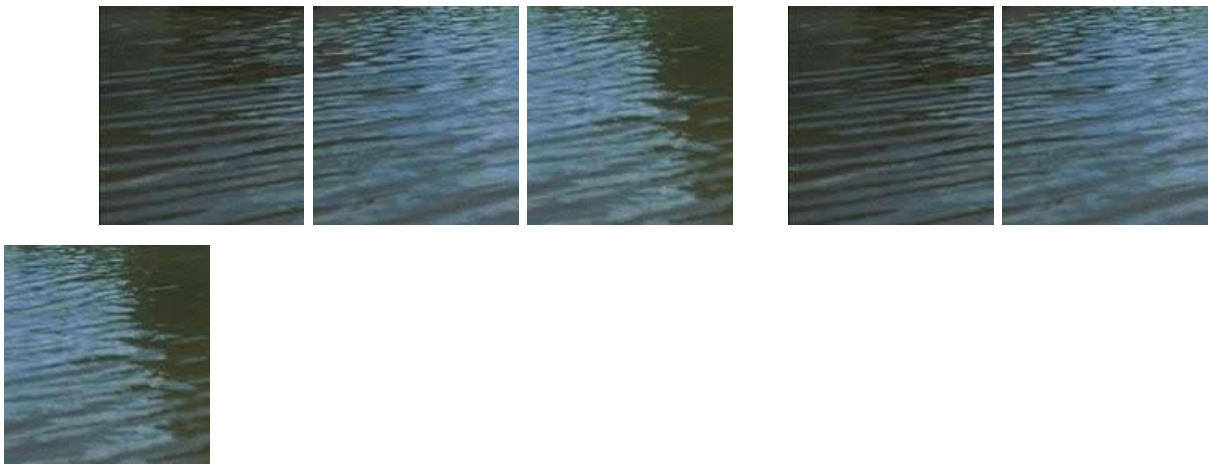
В середовищі Matlab був проведений обчислювальний експеримент перевірки цілісності відео послідовностей, що підтвердив ефективність використання розроблених методів для ЦВ. На рисунку 4.1, 2 представлений приклад роботи розроблених методів з відео послідовністю.

При проведенні перевірки цілісності ЦВ у 98% розглянутих відео послідовностей ОПЦ була виявлена та локалізована вірно.

Для можливості використання методу перевірки цілісності ЦС на основі дослідження DQ-ефекту для ЦА важливою є наявність квантування в процесі стиснення ЦА, оскільки фальсифікація та повторне збереження сигналу призведе до виникнення ефекту подвійного квантування незалежно від форми представлення ЦС.



1 2 3 1 2 3



4 5 6 4 5 6

а) б)

Рис. 1. Розбиття ключового кадру а) — нефальсифікованої, б) — фальсифікованої відео послідовності на ПБС 136×128 пікселів.

а) б) в)

Рисунок 4.2. а) – ПБС, підозрілі на наявність ОПЦ, ключового кадру нефальсифікованої відео послідовності, $K_2 = 21,28; K_3 = 21,28$, б) – ПБС, підозрілий на наявність ОПЦ, ключового кадру фальсифікованої відео послідовності, $K_3 = 81,03$; в) більш точна локалізація ОПЦ в ключовому кадрі фальсифікованої відео послідовності.

Висновки до розділу 4

Таким чином, можна зробити висновок про ефективність використання методу перевірки цілісності, заснованого на дослідженні DQ-ефекту, як для ЦЗ і ЦВ, так і для ЦА. Результати порівняльної оцінки ефективності роботи

розробленого методу та сучасних методів, що вирішують аналогічну задачу для ЦС, дозволяють стверджувати, що розроблений МПЦЦС є більш переважним як з точки зору можливості виявлення фальсифікації взагалі, так і локалізації фальсифікації малих розмірів зокрема.

Алгоритм ВМКПЦС є загальною основою для алгоритмів перевірки цілісності ЦЗ (ЦВ, ЦА) та уточнення локалізації ОПЦ. Для оцінки обчислювальної складності вказаних алгоритмів оцінена обчислювальна складність алгоритму ВМКПЦС, яка визначається розмірами вхідних даних та представляється поліномом ступеня 2, що є прийнятним для практичного алгоритму.

РОЗДІЛ 5
ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Головною метою розділу є обґрунтування економічної ефективності впровадження програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації.

Щоб виконати оцінку економічної ефективності необхідно розрахувати трудомісткість реалізації проекту, витрати на оплату праці найманим працівникам, витрати апаратного і програмного забезпечення, амортизаційні відрахування, витрати енергоресурсів та інші витрати які є основними пунктами виконання обчислень, а також показники економічної ефективності розробки проекту.

5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Реалізація проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації, складається з низки послідовних та взаємопов’язаних етапів.

Кожен із етапів реалізації проекту характеризується метою та змістом, оцінкою часу виконання, кількістю та спеціалізацією виконавців, а також приблизною оцінкою вартості.

Реалізація розробки складається із підготовчого етапу, етапу технічної пропозиції, створення технічного завдання, проектування системи, практичної реалізації, тестування, верифікації та заключного етапу.

Норми часу на виконання науково-дослідницької роботи розраховуватимуться в годинах, що наведені в таблиці 5.1 разом із інформацією про виконавців і сумарною кількості затраченого часу.

Таблиця 5.1 – Операції технологічного процесу та їх час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Підготовча стадія	Проектний менеджер	4
		Інженер-програміст	4
2	Технічна пропозиція	Проектний менеджер	8
		Інженер-програміст	8
3	Створення технічного завдання	Проектний менеджер	10
		Інженер-програміст	20
4	Проектування системи	Інженер-програміст	20
5	Практична реалізація	Інженер-програміст	69
6	Тестування системи	Тестувальник	20
7	Верифікація системи	Тестувальник	10
		Інженер-програміст	20
		Проектний менеджер	12
8	Створення документації	Інженер-програміст	20
9	Заключна стадія	Проектний менеджер	10
Разом			235

В підсумку на реалізацію проекту необхідно 235 годин, залучення трьох спеціалістів та виконання дев’яти різноманітних стадій реалізації проекту.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Визначення витрат на оплату праці та відрахувань на соціальні заходи прямо залежить від кількості витраченого працівниками часу на роботу, ставки в годину чи місяць, кількість відрахувань на соціальні заходи встановлених в законному порядку на час розрахунку.

В результаті розрахунку потрібно визначити основну та додаткову заробітну плату, витрати на соціальні заходи та на основі цих даних визначити сумарні витрати на оплату праці.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Наймані працівники для реалізація проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації, працюють згідно контракту, який в якому вказано їхню погодинну ставку. Тобто розрахунок заробітної плати працівників відбуватиметься на базі тарифної ставки та кількості відпрацьованих годин.

У штаті найманих працівників для розробки інформаційної системи залучено проектного менеджера, інженера-програміста і тестувальника.

Тарифні ставки учасників процесу розробки інформаційно-вимірювальної системи моніторингу зони покриття мобільних мереж:

– Проектний менеджер – 150 грн./год.
– Інженер-програміст – 130 грн./год.
– Тестувальник – 100 грн./год.

Основна заробітна плата розраховується за формулою 5.1:

$$З_{осн.} = Т_с \cdot К_г \, , \qquad (5.1)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує три спеціаліста, то основна заробітна плата буде розраховуватись за даною формулою 5.1;

$$З_{осн.} = 150 \cdot 44 + 130 \cdot 161 + 100 \cdot 30 \; = 30530 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати й визначається за формулою 5.2.

Коефіцієнт додаткових виплат працівникам становить 0,1.

$$З_{дод.} = З_{осн.} \cdot К_{допл.} \qquad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам

$$З_{дод} = 30530 \cdot 0,1 = 3053 \text{ грн.}$$

Звідси загальні витрати на оплату праці (фонд заробітної плати) визначаються за формулою 5.3:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (5.3)$$

$$В_{о.п.} = 30530 + 3050 = 33583 \text{ грн.}$$

З цієї суми утримуються обов'язкові відрахування на заробітну плату:

– Єдиний соціальний внесок (ЄСВ), що становить 22%;

– Військовий збір (ВЗ), що становить 1,5%;

Сума відрахувань становить 23,5% від фонду оплати праці та визначається за формулою 5.4:

$$B_{с.з.} = Ф_{оп} \cdot 0,235 \quad (5.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$B_{с.з.} = 33583 \cdot 0,235 = 7892 \text{ грн.}$$

Усі витрати обчислюються детально наведені в таблиці 5.2 та обчислюються за формулою 5.5:

$$В_{зп} = ФЗП + ФОП \quad (5.5)$$

$$В_{зп} = 33583 + 7892 = 41475 \text{ грн.}$$

Таблиця 5.2 – Розрахунки витрат на оплату праці

№ з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на плату праці, грн. (6=3+4+5)
		Тарифна ставка, грн.	Кількість відпрацьованих год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1.	Проектний менеджер	150	44	6600	660	-	-
2.	Інженер-програміст	130	161	20930	2093	-	-
3.	Тестувальник	100	30	3000	300	-	-
Разом		-	235	30530	3053	7892	41475

Згідно розрахунків, витрати на оплату праці становлять 41475 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати є невід'ємною частиною розробки для реалізація проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації та визначаються як добуток кількості витрачених матеріалів та їх ціни за формулою 5.6:

$$M_{ві} = q_{\text{і}} \cdot p_{\text{і}} , \qquad (5.6)$$

де: $q_{\text{і}}$ – кількість витраченого матеріалу і–го виду; $p_{\text{і}}$ – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 5.7:

$$З_{м.в.} = \sum M_{ві} . \qquad (5.7)$$

Результати проведених розрахунків наведено у таблиці 5.3.

Таблиця 5.3 – Результати розрахунків матеріальних витрат.

№ п/п	**Найменування матеріальних ресурсів**	**Од. виміру**	**Фактично витрачено матеріалів**	**Ціна одиниці, грн.**	**Загальна сума витрат, грн.**
1	Папір для друку А4	пачка	1	90,00	90,00
2	Заправка для принтера	шт.	1	100,00	100,00
Всього					190,90

Згідно проведених розрахунків, матеріальні витрати становлять 190,90 грн.

5.4 Розрахунок витрат на електроенергію

Однією із статей витрат є витрати на електроенергію під час проходження усіх етапів реалізації кінцевого продукту.

Затрати на електроенергію одиниці обладнання визначаються за формулою 5.8:

$$З_в = W \cdot T \cdot S, \tag{5.8}$$

де W – необхідна потужність, кВт; T – кількість годин на реалізацію розробки; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютерів для реалізації проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації – 400 Вт, кількість годин роботи обладнання згідно таблиці 5.1 – 235 годин.

Визначимо витрати на електроенергію згідно формули 5.11:

$$З_в = 0{,}4 \cdot 235 \cdot 2{,}42 = 227{,}48 \text{ грн.}$$

Згідно формули затрати на електроенергію становлять 227,48 грн.

5.5 Розрахунок суми амортизаційних відрахувань

Для будь якої діяльності характерною є властивість зношування на зниження якості властивостей інструментарію та фондів за допомогою яких ведеться діяльність.

Для вирішення проблеми із відновленням даних фондів використовується амортизація, що являє собою процес трансформації вартості основних фондів на вартість продукції, яка щойно була створена, задля повного відновлення основних фондів.

Для визначення амортизаційних відрахувань використовується формула 5.9:

$$A = \frac{Б_в \cdot Н_А}{100\,\%} \qquad (5.9)$$

де, $С_Б$ – балансова вартість обладнання, грн;

N_A – норма амортизаційних відрахувань в рік, %;

– річний робочий фонд часу, год;

– фактичний час роботи обладнання по написанню програми, год.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Річний робочий фонд становитиме 2352 годин, так як робочий день становить 8 годин, а кількість робочих днів в місяці становить 24,5 годин.

Для даної розробки засобом розробки є комп'ютер. Його сума становить 18500 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 18500 \cdot 5\% / 100\% = 925 \text{ грн.}$$

Згідно проведених обчислень амортизаційні відрахування становлять 925 грн.

5.6 Обчислення накладних витрат

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$Н_в = В_{о.п.} \cdot 0{,}2…0{,}6 \,, \qquad (5.10)$$

де $Н_в$ – накладні витрати.

Отже, накладні витрати становлять згідно формули 5.10:

$$Н_в = 33583 \cdot 0{,}2 = 6716{,}6 \text{ грн.}$$

Накладні витрати згідно розрахунку формули, становить 6716,6 грн.

5.7 Складання кошторису витрат та визначення собівартості

Результати проведених вище розрахунків наведено у таблиці 5.4.

Таблиця 5.4 – Кошторис витрат

Зміст витрат	**Сума, грн.**	**В % до загальної суми**
Витрати на оплату праці	33583	67,80
Відрахування на соціальні заходи	7892	15,93
Матеріальні витрати	190,90	0,39
Витрати на електроенергію	227,48	0,46
Амортизаційні відрахування	925	1,87
Накладні витрати	6716,6	13,56
Собівартість	49534,98	100,00

Собівартість ($С_в$) проєкту розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_в + А + Н_в \,. \qquad (5.11)$$

Отже, собівартість програмного продукту дорівнює:

Св = 33583+ 7892+ 190,90 + 227,48+ 925+ 6716,6 = 49534,98 грн.

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 49534,98 грн.

5.8 Розрахунок ціни

Ціну проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації можна визначити за формулою:

$$Ц = \frac{C_В \cdot (1 + P_{рен}) + К \cdot B_{н.і.}}{К} \cdot (1 + ПДВ), \quad (5.12)$$

де $P_{рен.}$ – рівень рентабельності, 30 %; $К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем); $B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту); *ПДВ* – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Ві.н , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_В \cdot (1 + P_{рен}) \cdot (1 + ПДВ) \quad (5.13)$$

Звідси ціна на роботу складе:

$$Ц = 49534{,}98 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 77274{,}57 \text{ грн.}$$

Загальний розрахунок проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації становить 77274,57 грн.

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці за певний проміжок часу.

Економічна ефективність (E_p) полягає у відношенні результату до затрачених ресурсів:

$$E_p = \frac{П}{C_B}, \tag{5.14}$$

де $П$ – прибуток; C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_в \ . \tag{5.15}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 77274,57 - 49534,98 = 27739,59 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_p = \frac{П}{C_B}. \tag{5.16}$$

Тоді,

$$E_p = 27739,59 / 49534,98 = 0,56.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_p = \frac{1}{E_p}, \qquad (5.17)$$

Термін окупності дорівнює:

$$T_p = 1 / 0,5 = 1,78 \text{ р.}$$

Згідно проведених розрахунків прибуток від проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації становить 27739,59 грн., економічна ефективність дорівнює 0,56, а термін окупності становить 1,78 роки що вважається доцільним та економічно вигідним.

5.10 Висновки до п’ятого розділу

В розділі обґрунтування економічної ефективності було розраховано основні техніко-економічні показники проєкту програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації (див. таблиця 5.5).

Значення економічної ефективності становить 0,56 що є достатньо високим значенням.

Період окупності повинен коливатись від 1 до 3 років, тоді реалізація проекту вважається доцільною та економічно обґрунтованою. Термін окупності даної роботи становить 1,78 років.

Таблиця 5.5 – Техніко-економічні показники

№ п/п	**Показник**	**Значення**
1.	Собівартість, грн.	49534,98
2.	Плановий прибуток, грн.	27739,59
3.	Ціна, грн.	77274,57
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,78

На основі проведених розрахунків можна зробити висновок, що створення програмного забезпечення виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі із втратою інформації є доцільним у зв’язку з невеликим терміном окупності та достатнім обсягом планового прибутку.

РОЗДІЛ 6

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1. Основні завдання та функції системи управління охороною праці на підприємстві (СУОПП).

Функціонування системи забезпечується керівником підприємства і реалізується через комплекс організаційних заходів.

Виконання управлінських рішень з питань охорони праці й забезпечення функціонування СУОП у структурних підрозділах здійснюється керівниками цих підрозділів.

Організаційно-методичне керівництво й координацію діяльності всіх структурних підрозділів підприємства в рамках СУОП здійснює служба охорони праці.

У керуванні охороною праці, крім штатних посадових осіб і структурних підрозділів беруть участь профспілковий комітет (цехові комітети) з його комісією з охорони праці й громадських інспекторів з охорони праці або інші вповноважені найманими робітниками особи з питань охорони праці, завдання й функції яких повинні бути визначені відповідними положеннями. [5].

У цілому організаційна структура управління охороною праці базується на координуючій ролі служби охорони праці, що, відповідно до діючого на підприємстві положення, наділена необхідними повноваженнями й бере участь у здійсненні всіх функцій, пов'язаних із забезпеченням безпеки праці.

Переважне право розробляти й представляти керівництву підприємства на розгляд і затвердження організаційно-розпорядницькі документи з питань охорони праці має служба охорони праці.

Якщо виникає потреба розробки таких документів іншими структурними підрозділами (службами, відділами й т.п.) вони підлягають обов'язковому узгодженню зі службою охорони праці.

Велике значення у створенні безпечних і нешкідливих умов праці має стандартизація. Вона дозволяє застосовувати дійові заходи з підвищення технічного рівня й упорядкування розробки нормативно-технічної документації з безпеки праці[4].

У нашій країні створена система стандартів з безпеки праці, що являє собою комплекс великої кількості взаємозалежних стандартів, спрямованих на забезпечення праці. Ця система встановлює загальні вимоги й норми за видами небезпечних і шкідливих виробничих факторів, загальні вимоги безпеки до виробничого устаткування й процесів, вимоги до засобів захисту працюючих, методи оцінки безпеки праці.

СУОП підприємства встановлює єдиний порядок діяльності керівників структурних підрозділів та інших посадових осіб з питань охорони праці: цільові завдання й функції підрозділів, обов'язки посадових осіб, порядок планування профілактичної роботи, систему контролю за станом охорони праці й дотриманням працюючими вимог правил, норм й інструкцій з охорони праці, а також основні положення екологічного регулювання й мотивації роботи з охорони праці на підприємстві[2].

Основні завдання управління охороною праці можна сформулювати коротко – забезпечення дотримання вимог НПАОП щодо безпеки умов праці та безпеки технологічних процесів і виробничого обладнання, а також впровадження національної концепції розвитку в сфері управління охороною праці.

Функція прогнозування та планування роботи з охорони праці**,** в основі якої лежить прогностичний аналіз, має вирішальне значення в системі управління охороною праці на виробництві. Планування роботи з охорони праці на виробництві поділяється на перспективне, поточне та оперативне.

Перспективне планування вміщує найбільш важливі, трудомісткі і довгострокові заходи, виконання яких, як правило, вимагає сумісної роботи кількох підрозділів підприємства. Можливість виконання заходів перспективного плану повинна бути підтверджена обґрунтованим розрахунком

необхідного матеріально-технічного забезпечення і фінансових витрат із зазначенням джерел фінансування. Основною формою перспективного планування роботи з охорони праці є розроблення комплексного плану щодо покращення стану охорони праці.

Поточне планування здійснюється у межах календарного року через розроблення відповідних заходів у розділі "Охорона праці" колективного договору.

Оперативне планування роботи з охорони праці здійснюється за підсумками контролю стану охорони праці в структурних підрозділах і на підприємстві в цілому. Оперативні заходи щодо усунення виявлених недоліків зазначаються безпосередньо у наказі по підприємству, який видається за підсумками контролю, або у плані заходів, як додатку до наказу.

Процес планування заходів з охорони праці, як і реалізація будь-якої іншої управлінської функції, повинен здійснюватися в три етапи:

1. – оцінка ситуації чи стану об’єкта управління (оцінка стану безпеки праці і виробничого середовища на підприємстві);

2. – пошук шляхів і способів впливу на ситуацію (визначення варіантів заходів, які можуть вплинути на стан охорони праці);

3. – вибір і обґрунтування оптимального способу дій для поліпшення ситуації (визначення раціонального переліку заходів із охорони праці для включення їх у план чи колективний договір).

Функція УОП щодо організації та координації робіт передбачає формування органів управління охороною праці на всіх рівнях управління і всіх стадіях виробничого процесу, визначення обов’язків, прав, відповідальності та порядку взаємодії осіб, що приймають участь в процесі управління, а також прийняття та реалізацію управлінських рішень.

Глибоко помилковою є думка, яку, на жаль, ще дуже часто можна почути, що робота з охорони праці є прерогативою лише служб охорони праці. Налагодження функціонування СУОП на виробництві необхідно починати перед усім із аналізу функціональних обов’язків всіх посадових осіб

підприємства і, якщо необхідно, відповідного їх коригування з метою усунення прогалин та непотрібного дублювання. Неналежне виконання своїх обов'язків, наприклад, службою постачання при закупівлі обладнання може обернутись травмою для будь-якого робітника підприємства.

Облік, аналіз та оцінка показників охорони праці спрямовані (відповідно до одержаної інформації) на розробку та прийняття управлінських рішень керівниками усіх рівнів управління (від майстра дільниці до керівника підприємства). Суть даної функції полягає у системному обліку показників стану охорони праці, в аналізі отриманих даних та узагальненні причин недотримання вимог НПАОП, а також причин невиконання планів із охорони праці з розробкою заходів, направлених на усунення виявлених недоліків. Аналізуються матеріали про нещасні випадки та професійні захворювання; результати всіх видів контролю за станом охорони праці; дані паспортів санітарно-технічного стану умов праці в цеху (на дільниці); матеріали спеціальних обстежень будівель, споруд, приміщень, обладнання тощо. В результаті обліку, аналізу та оцінки стану охорони праці вносяться доповнення та уточнення до оперативних, поточних та перспективних планів роботи з охорони праці, а також по стимулюванню діяльності окремих структурних підрозділів, служб, працівників за досягнуті показники з охорони праці[3].

Контроль за станом охорони праці та функціонуванням СУОП забезпечує дійове управління охороною праці. Будь-яка система управління може надійно функціонувати лише при наявності повної, своєчасної і достовірної інформації про стан об'єкта управління. Одержати таку інформацію про стан охорони праці, виявити можливі відхилення від норм безпеки, а також перевірити виконання планів та управлінських рішень можна тільки на підставі регулярного та об'єктивного контролю. Тому контроль стану охорони праці є найбільш відповідальною та трудомісткою функцією процесу управління.

До основних форм контролю за станом охорони праці в рамках СУОП підприємства відносяться: оперативний контроль; відомчий контроль, що проводиться службою охорони праці підприємства; адміністративно-

громадський багатоступеневий контроль. Крім цих видів контролю, існує відомчий контроль вищих господарських органів, державний нагляд та громадський контроль за охороною праці, які розглядаються окремо.

Оперативний контроль з боку керівників робіт і підрозділів підприємства проводиться згідно із затвердженими посадовими обов’язками. При цьому служба охорони праці контролює виконання вимог безпеки праці у всіх структурних підрозділах та службах підприємства.

6.2. Заходи щодо забезпечення сприятливих умов зорової роботи користувача ЕОМ.

Однією із характерних особливостей сучасного розвитку суспільства є зростання сфер діяльності людини, в яких використовуються інформаційні технології. Широке розповсюдження отримали персональні комп'ютери. Однак їх використання загострило проблеми збереження власного та суспільного здоров'я, вимагає удосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу ПК на здоров'я користувачів.

Розглянемо основні вимоги до організації роботи з ЕОМ.

Основні вимоги до організації роботи з ЕОМ [5]:

1. площа на одне робоче місце має становити не менше ніж 6,0 м, а об'єм не менше ніж 20,0 метрів кубічних;

2. природне освітлювання має забезпечувати коефіцієнт природної освітленості не нижче 1,5%. Розраховується КПО за методикою, викладеною в ДБН В.2.5–28–2006;

3. віконні прорізи приміщень для роботи з ВДТ мають бути обладнані регульованими пристроями (жалюзі, завіски, зовнішні козирки);

4. покриття підлоги повинне бути матовим з коефіцієнтом відбиття 0,3–0,5;

5. забороняється для оздоблення інтер'єру приміщень ВДТ застосовувати полімерні матеріали (деревинно – стружкові плити, шпалери, що ються,

рулонні синтетичні матеріали, шаруватий паперовий пластик тощо), що виділяють у повітря шкідливі хімічні речовини у приміщеннях з ВДТ слід щоденно робити вологе прибирання;

6. приміщенням з ВДТ мають бути обладнані побутові приміщення для відпочинку під час роботи, кімната психологічного розвантаження. В кімнаті психологічного розвантаження слід передбачити встановлення пристроїв для приготування й роздачі тонізуючих напоїв, а також місця для занять фізичною культурою[5].

Для збереження здоров'я користувачів ЕОМ, виключення професійних захворювань і підтримки працездатності варто передбачати регламентовані перерви для відпочинку протягом зміни.

При виконанні протягом дня робіт з ЕОМ, які займають не менш 50% тривалості робочої зміни, повинні передбачатися перерви:

- для відпочинку й прийому їжі (обідня перерва);

- для відпочинку й особливих потреб (відповідно до трудових норм);

- додаткові перерви, які вводяться для окремих професій з урахуванням особливості трудової діяльності[5].

В окремих випадках, при постійних скаргах на зорову втому тих, хто працює перед відеотерміналом, при дотриманні санітарно-гігієнічних вимог до режиму праці та відпочинку, а також вимог щодо застосування індивідуальних засобів локального захисту очей, допускається індивідуальний підхід до обмеження тривалості робіт перед відеотерміналом, зміни змісту роботи, чергування з іншими видами діяльності, не пов'язаними з відеотерміналом.

При виконанні робіт, що належать до різних видів трудової діяльності за основну роботу з ПК вважають роботу, що займає не менше 50% часу впродовж робочого дня.

У випадках, коли виробничі обставини не дозволяють застосовувати регламентовані перерви, тривалість безперервної роботи за ВДТ не повинна перевищувати 4 години. З метою зниження нервово-емоційного напруження, втоми зорового аналізатора, поліпшення мозкового кровообігу, подолання

несприятливих наслідків гіподинамії, запобігання втоми ДСАНПІН 3.3.2.007-98 рекомендується деякі перерви використовувати для психофізіологічного розвантаження.

Крім того, психофізіологічне розвантаження рекомендується проводити і в кінці робочого дня. Для цієї мети повинні бути спеціально обладнані приміщення – кімнати психологічного розвантаження. Деякі дослідження говорять про те, що при роботі на комп'ютері більше 5 годин в день різко зростає втомлюваність, підвищується вірогідність погіршення стану здоров'я та різко падає продуктивність праці. При цьому слід враховувати саме роботу на комп'ютері, а не періодичне кидання очима на працюючий монітор при занятті іншими справами[5].

Користувачі ПК повинні проходити обов'язкові медичні огляди: попередні – під час оформлення на роботу та періодичні – протягом трудової діяльності відповідно до наказу МОЗ України №45 від 31.03.94р. та ДСАНПІН 3.3.2.007-98. (раз у два роки комісією в складі терапевта, невропатолога й офтальмолога). Основними критеріями придатності до роботи з ПЕОМ можуть бути показники стану органів зору, і також стану організму в цілому. До роботи безпосередньо на ПК допускаються особи, які не мають медичних протипоказань. Періодичні медичні огляди повинні проводитися раз на два роки комісією в складі терапевта, невропатолога та офтальмолога.

6.3. Фактори ризику і можливі порушення здоров'я користувачів комп'ютерної мережі.

Вплив інформаційних технологій на людину з кожним роком зростає. Уже сьогодні важко уявити будь-яку діяльність без використання інформаційних технологій. Активне формування і розвиток інформаційного середовища сприяє прискоренню всіх процесів в людській діяльності. Результатом є виникнення нових вимог і певних умов життя, до яких людина повинна пристосуватися [10]. На даний час існую декілька технологій, що розвиваються стрімкими темпами.

Одна з них – це технологія квантових обчислень. ІТ-фахівці, як і будь-які інші працівники, повинні проходити навчання і перевірку знань з охорони праці або в навчальному центрі, або в самій організації.

Однак на даний момент не існує конкретних прикладів програм роботи з квантовими комп'ютерами. Це пов'язано з відсутністю досвіду і відносної прихованістю принципів роботи квантових систем.

Споживачам лише дається загальна інформація, в кінці якої говориться, що їм не потрібно купувати і встановлювати подібний комп'ютер у себе вдома, а все взаємодія відбувається за допомогою хмарних сервісів через Інтернет.

У зв'язку з цим залишається лише збирати крупиці знань з іноземних джерел та відеоекскурсій, де розповідають про взаємодію з подібного роду системами. Отже, за наявних та отриманих знань із вищезгаданих джерел варто розділити працівників на кілька груп:

1) Ті, хто не використовує квантові комп'ютери безпосередньо, а працює через віддалений комп'ютер або термінал, або звичайні користувачі [11];

2) Ті, хто займається установкою готових квантових комп'ютерів, їх налаштуванням і супроводом, тобто монтажники або обслуговуючий персонал [12];

3) Розробники квантових комп'ютерів, що створюють їх архітектуру, регламентують принцип дії, в тому числі криогенного обладнання, тобто інженери-науковці;

4) Розробники процесорів, які «вирощують» в стерильних лабораторіях. Це також інженери, науковці та математики.

Перша категорія користувачів - це звичайні люди, які не будуть безпосередньо взаємодіяти із квантовими комп'ютерами. Вони будуть використовувати термінали, віддалено, через класичний резисторний комп'ютер, тим самим делегуючи повноваження з підтримання його роботи спеціально навченому персоналу.

Як правило, компанії, які надають послуги з оренди або продажу даних комп'ютерів також надають послуги з їх обслуговування. Наприклад якась

компанія, або навіть навчальний заклад може придбати на місяць потужності квантового комп’ютера для одноразових розрахунків, після чого такий потужний комп’ютер буде не потрібен. Таким чином для цієї категорії користувачів діють ті ж самі регламентовані норми охорони безпеки, що існують зараз.

Друга і третя група людей вже буде безпосередньо взаємодіяти з квантовими комп’ютерами. Тут спеціалісти вже будуть стикатися із кріогенним обладнанням та високовольтними мережами, так як квантовий комп’ютер для своєї роботи вимагає близько 15кВт енергії [13]. Нутрощі квантового комп'ютера повинні бути максимально ізольовані від навколишнього середовища і підтримувати свій власний температурний режим. Якщо комп'ютер необхідно розібрати, щоб замінити центральний процесор потрібно його вимкнути і повернути кімнатну температуру.

На ранніх етапах були лабораторії, де вивчалися окремі складові квантових комп'ютерів. Зараз в таких лабораторіях вирощують чіпи. Даний процес схожий зі створенням кристалів процесорів сучасних комп'ютерів. Тому для четвертої групи слід зазначити, що при роботі з «голими», незахищеними схемами і чіпами необхідна абсолютна чистота приміщення, повна відсутність пилу, а працівникам необхідно одягнути спецодяг.

Тому такі лабораторії повністю ізолюють від зовнішнього світу, оснащують складними системами очищення і кондиціонування повітря, що роблять його у 10000 разів чистіше, ніж в хірургічній палаті [14].

Всі фахівці, що працюють в такій чистій кімнаті, не просто дотримують стерильність, а й носять захисні костюми з антистатичних матеріалів, маски, рукавички. І все ж, незважаючи на всі обережності, щоб зменшити ризик браку, компанії-виробники процесорів намагаються автоматизувати максимум операцій, вироблених в чистій кімнаті, поклавши їх на промислових роботів.

Іншою технологією, що поступово інтегрується в інформаційне життя є технологія віртуальної реальності. Віртуальна реальність міцно увійшла в життя сучасної людини. Тепер у нас є VR-ігри, студенти-медики вчаться за допомогою

програм віртуальної реальності, а вчені можуть створювати тривимірні VR-конструкції для своїх досліджень.

Дізнаючись про нові технології, люди поспішають скоріше зануритися у віртуальний світ, але забувають про потенційні небезпеки її використання і правилах роботи з нею. Технологія VR сьогодні доступна всім бажаючим. Досить купити спеціальний шолом і ви можете вирушати назустріч віртуальним пригод.

Але не варто забувати про техніку безпеки - щоб користуватися шоломом без шкоди для себе і оточуючих необхідно дотримуватися ряду правил. Будь-який VR-шолом (Samsung Gear VR, Oculus Rift, HTC Vive, PlayStation VR) впливає на сприйняття світу. VR-шолом занурює вас в вигадане простір, яке ваші очі сприймають, як реальне.

Важливо розуміти, що почуття запаморочення, нудоти і дезорієнтації, які виникають внаслідок використання шолома, обумовлені тим, як ваш мозок реагує на зображення. Коли ви знімаєте шолом і повертаєтеся в звичну обстановку, неприємні відчуття проходять.

Таким чином, використання новітніх інформаційно-комунікаційних технологій вимагає від фахівців ІТ-індустрії додержання певних правил та вимог з точки зору безпеки праці, її нормування з урахуванням віку працюючих та загального інформаційного навантаження, розробки та впровадження індивідуальних, щотижневих та щорічних режимів праці та відпочинку, які сприятимуть профілактиці перевтомлення і підвищенню розумової працездатності працюючих.

Особливу роль в цьому напрямі повинні відігравати ергономічні заходи стосовно створення робочих місць, оптимізації взаємодії людини в рамках системи «оператор-термінал». Всі ці вимоги повинні бути втілені у відповідних нормативно-правових актах (стандартах підприємств), що регламентують різноманітні питання охорони та психології безпеки праці фахівців ІТ-індустрії.

6.4. Вплив стихійних лих, аварій (катастроф) та їх наслідки.

Відомо понад 30 видів природних особливонебезпечних явищ, які об'єднуються в три групи:

1. Літосферні - землетруси, виверження вулканів, гірські обвали, зсуви, викиди гірських порід тощо.

2. Гідросферні - цунамі, повені, сельові потоки, снігові лавини, льодові затори, ожеледиця, обмерзання суден тощо.

3. Атмосферні - бурі, смерчі (вихори), буревії, грози, зливи та снігопади, град, ожеледь, посухи, пожежі, заморозки тощо.

До розряду надзвичайних відносяться тільки ті катастрофи, що мають хоча б одну з наведених нижче ознак-критеріїв оцінки катастроф як надзвичайних ситуацій природного характеру:

Геологічні небезпечні явища (землетруси, виверження вулканів, обвали, зсуви, просідання земної поверхні) – землетруси в 4 і більше балів; кількість потерпілих 15 осіб і більше; кількість загиблих 4 особи і більше; прямі матеріальні збитки 500 тис. грн. і більше; вплив на функціонування інших галузей господарства;

Гідрометеорологічні і геліогеофізичні небезпечні явища – кількість потерпілих 10 осіб і більше;

кількість загиблих 2 особи і більше; прямі матеріальні збитки 500 тис. грн. і більше, зокрема:

– сильний вітер (у т.ч. смерчі, шквали)

– швидкість вітру при поривах 25- 30 м/с і більше;

– сильний дощ (зливи) – більше 120 мм, а в селенебезпечних гірських районах понад 30-50 мм за 12 годин;

– крупний град – розміром більше 20 мм;

– сильний снігопад – 30 мм і більше за 12 годин;

– сильна хуртовина (снігові заноси) – вітер 20 м/с і більше протягом доби із снігопадом;

– сильна ожеледь – діаметр налипання на лініях електропередач 20 мм і більше;

– сильний мороз або спека;

– високі хвилі, вітрові нагони, дощові паводки (повені);

– заморозки – зниження температури повітря нижче 0 °С в екстремально пізні строки (весна – початок літа) і в екстремально ранні (літо – початок осені) в період активної вегетації сільгоспкультур, що може призвести до їх загибелі;

– засуха – поєднання високих температур повітря, дефіциту опадів, низької вологості повітря, малих запасів вологи в ґрунті, що призводить до загибелі врожаю польових культур; високі рівні води при дощових повенях, заторах, вітрових нагонах, що перевищують небезпечні рівні води для конкретних об’єктів;

– низькі рівні води – нижче проектних значень водозабірних споруд та навігаційних рівнів на судноплавних річках протягом місяця і більше;

– селілавини – загроза населеним пунктам, господарським об’єктам, туристичним базам тощо;

– погіршення радіаційної обстановки в наземному космічному просторі у випадку, коли щільність потоку протонів з енергією більше 25 МеВ становить понад 5÷10 см-2 · с-1);

– зменшення загального вмісту озону в атмосфері понад 25% протягом 2-3 місяців у період вегетації рослин.

Природні пожежі (лісові, польові, торф’яні) – кількість потерпілих понад 15 осіб, кількість загиблих 4 особи і більше; прямі матеріальні збитки понад 100 тис. грн.; великі неконтрольовані пожежі на площі понад 25 га.

Особливо небезпечні хвороби й ураження токсичними хімічними речовинами:

– епідемії – захворювання 30 осіб; групові захворювання невизначеної етомологіі 20 осіб; рівень смертності перевищує середньостатистичний у 3 рази;

– епізоотія – факти масового захворювання або загибелі тварин;

– епіфітотія – масова загибель рослин.

Остаточне рішення щодо рівня надзвичайної ситуації з подальшим відображенням її у даних статистики, у тому числі у разі відсутності достатніх відомостей щодо розвитку надзвичайної ситуації, приймає спеціально уповноважений центральний орган виконавчої влади, до компетенції якого належить вирішення питань захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру, за погодженням у разі потреби із заінтересованими міністерствами та іншими центральними органами виконавчої влади, а також з урахуванням експертного висновку (у разі його надання) регіональної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій щодо рівня надзвичайної ситуації.

РОЗДІЛ 7

ЕКОЛОГІЯ

7.1. Комплексна оцінка екологічності виробництва

Економічна оцінка ефективності окремих екологічних проектів є складовою регіональної (державної) оцінки ефективності охорони навколишнього середовища. На обох рівнях вона потребує актуального підходу до оцінки матеріальних, організаційних, фінансових, природних та соціальних ресурсів, які зазнають екологічного ефекту, а також залучені в процес реалізації природоохоронної діяльності. В свою чергу, координація екологічних проектів як наслідок контролю їх ефективності має здійснюватися з врахуванням відтворювального характеру природних ресурсів, науково-технічних знань та впливу ринкових механізмів на діяльність макро- та мікроекономічних систем.

У вирішенні проблем і завдань охорони природи пріоритетним є комплексний підхід, за яким природа в соціально-господарському аспекті розглядається як елемент навколишнього середовища. Це в найбільшому степені характерно для промислового виробництва, де природний та екологічний фактори взаємозалежні в соціальному аспекті, технологічно та економічно. Це дозволяє сформулювати перелік пріоритетних об’єктів оцінки та контролю в галузі охорони навколишнього середовища [2, с. 147-149; 6, с. 98-102]:

- шкода, завдана в процесі природокористування (природному середовищу, господарським, будівельним і культурним об’єктам);
- екологічна шкода, завдана в наслідок ведення технологічної та виробничо-господарської діяльності;
- напрямки ліквідації поточного забруднення та запобігання потенційно можливому;
- рівень компенсаційних, податкових і штрафних платежів, що справляються за завдану навколишньому середовищу шкоду, та її поточне забруднення;
- ефективність процесів природокористування та пов’язаних з ними екологічних та природоохоронних проблем;

- ефективність природоохоронної діяльності підприємств;

- ефективність функціонування природоохоронних об'єктів (очисних споруд, заповідників і т.д.);

Таким чином, з цілями та результатами природоохоронної діяльності пов'язуються наступні види економічних оцінок:

1) завданої, поточної та потенційно можливої шкоди (у грошовому виразі);

2) операційних і капітальних витрат, спрямованих на ліквідацію завданої шкоди та на попередження потенційної;

3) податкових, компенсаційних і штрафних платежів за забруднення, транзакційних витрат;

4) економічних результатів – отримання товарної продукції та вторинних матеріальних ресурсів, що підлягають утилізації, витрат на очищення та повернення в навколишнє середовище вторинних відходів [4, с. 53; 10, с. 285].

У сукупності все вищенаведене визначає складність: а) оцінки наслідків негативного впливу промислового виробництва (особливо, металургії та хімічної промисловості) та природокористування на навколишнє середовище; б) оцінки ефективності екологічних і природоохоронних заходів; в) оцінки ефективності інвестиційного проекту в екологічний проект або природоохоронної діяльності промислових підприємств.

Подолання цих труднощів відбувається шляхом диференціації горизонтів оцінки результативності реалізації екологічних проектів на рівнях: екологічному, економічному та соціальному. При цьому, критеріями оцінки реалізації екологічних програм є: а) величина соціального та економічного ефекту; б) якість наданих в межах реалізації екологічного проекту послуг; в) ефективність реалізації (за кожним з горизонтів оцінки результативності).

Механізми оцінки можуть відрізнятися залежно від спрямованості екологічного проекту. Так, наприклад, оцінка деяких природоохоронних заходів здійснюється як під час реалізації, так і після їх реалізації, у зв'язку з тим, що ефект від проведення запланованих дій може проявитися з часом. Разом з тим,

проведення ретроспективної оцінки покликане сприяти виявленню недоліків та прорахунків, допущених під час розробки та реалізації екологічних програм.

В подальшому, результати оцінки можуть використовуватися для проведення аналізу ефективності заходів екологічного проекту, що дає змогу суттєво вдосконалити якість його розробки. Якщо проект розрахований на кілька років (що характерно для програм в екологічній сфері), то в цьому випадку щорічно проведена оцінка отриманих результатів дозволить скорегувати програмні заходи наступних років. Крім того, проведення ретельно продуманої процедури оцінки ефективності виявляє причинно-наслідковий зв'язок між результатами й програмними заходами. Проте, поглиблений аналіз результатів і ефективності програмних заходів має не лише переваги, але й недоліки. До числа основних переваг можна віднести отримання детальної та перевіреної інформації, а до числа недоліків – порівняно більші фінансові витрати та витрати часу [11, с. 104].

Для екологічних програм особливо важливим є проведення оцінки з погляду ефективності видатків. Для порівняння альтернативних екологічних проектів важливо враховувати індикатори результативності, що характеризують своєчасність і повноту реалізації тієї або іншої функції. Традиційно застосовують наступні критерії оцінки (рис. 1). Зазначені критерії тісно взаємопов’язані та відтворюють різні аспекти ефективності соціальних видатків у процесі виконання бюджету:

- з точки зору економічності – необхідно знати склад витрат і ціни;
- для оцінки продуктивності – якісні стандарти продукції й послуг та порівняльну ресурсоємність реалізації кожного з них;
- для оцінки результативності – необхідна розробка спеціальних індикаторів досягнення цілей.

7.2. Етапи та техніка збору та обробки екологічної інформації

Типи екологічної інформації можна розглядати на основі таких незалежних підстав:

- розглядаються відношення в просторі і/або в часі;
- за масштабами в просторі і/або в часі, в рамках яких розглядаються відносини;
- за типами відношень;
- за провідним об' єктом функцією;
- за найважливішим аргументом;
- за залежним аргументом;
- за множиною аргументів;
- за відображенням тільки прямих зв' язків або прямих і зворотних зв'язків;
- за логічним обсягом функцій і аргументів.

Найважливішою умовою збирання первинної інформації є принцип синхронності спостережень змінних, масштаб яких виділяється як провідна підстава.

Найбільш типові два способи синхронізації: синхронізація спостережень в просторі і синхронізація спостережень у часі. Згідно із загальною теорією адекватне, сумісне зображення двох типів синхронізації в єдиній вимірювальній системі неможливе. Поліпшення часової синхронізації неминуче спричиняє погіршення просторової за якістю або об'ємом інформації і навпаки.

Тип екологічної інформації, при якому відбувається синхронізація спостережень за змінними в просторі, можна визначити як географічний або, точніше, еколого-географічний; тип синхронізації за часом — як власне екологічний.

При синхронізації інформації в просторі зазвичай мають на увазі, що вона збирається в допустимо невеликому єдиному інтервалі часу, так само як при часовій синхронізації забезпечується допустимо невелика відмінність в розміщенні спостережень в просторі. У першому випадку має бути «однорідним» час, у другому — простір. В обох випадках мається на увазі

топологічна однорідність об'єкта, тобто властивості елементів множини, що створює простір об'єкта, мають бути ізоморфними одна одній: за прийнятої точності вимірювання не відрізняється.

Реальні лінійні та часові масштаби синхронізації визначаються власними просторово-часовими відношеннями об'єкта і в окремому випадку для визначення цих масштабів потрібні спеціальні тестові дослідження. Тут масштаб задається власними властивостями об'єктів: у дерев він один, у трав — інший. Проте масштаб може бути визначений і з погляду організації самого простору та часу. При цьому допускається, що в часі і просторі мають місце коливальні процеси з циклами різної тривалості та протяжності.

Коли йдеться про простір, то кажуть про локальний масштаб збирання інформації (зазвичай лінійні розміри системи спостережень мають порядок кількох кілометрів), субрегиональной, регіональний і глобальний.

Для часу в практиці застосовують поняття короткого екологічного часу, великого екологічного часу і тому подібне. Звичайно, це тільки вельми груба прагматична інтерпретація уявлень про просторово-часові масштаби. Реальний їхній спектр значно ширший і сам по собі є наочною областю екологічних досліджень й екологічної інформації. Поняття «локальний», «регіональний», «глобальний» дуже умовні і неточно типізують інформацію за просторовими масштабами. Те саме справедливе і для часових типів.

Важливим загальним принципом є певний зв'язок, або когерентність, між просторовими і часовими типами.

Так, наприклад, говорити про локальну просторову інформацію в еволюційному масштабі часу просто безглуздо, оскільки локальний масштаб у просторі просто нескінченно мала, багато разів зміщена точка в еволюційному масштабі часу. Справедливо і зворотне. Для багатьох реальних екологічних процесів, кажучи про глобальний масштаб змін, безглуздо розглядати такі часові масштаби, як добові, річні, десятирічні, а для деяких процесів і сто- і тисячолітні. Чим з меншою внутрішньою інерцією системи пов'язаний процес,

тим менші часові масштаби змін зіставні з глобальним рівнем, чим більше інерційність, тим відповідно ці масштаби будуть більші.

Загалом зрозуміло, що коли йдеться про глобальні зміни клімату, то маються на увазі масштаби часу в кілька десятків років. Але якщо пов'язувати зі зміною клімату глобальні перетворення зональної структури рослинного або ґрунтового покриву, то йтися вже може про десятки тисяч, сотні тисяч і мільйони років.

Типологія екологічної інформації за об'єктами дослідження має автоматично відображати множину змінних. Кожна змінна може бути відображена, починаючи з найбільш високого загального рівня.

Звернемося до логічних побудов В. І. Вернадського. Його першим логічним посиланням є твердження, що в найбільш спрощеному вигляді земні оболонки — це відображення динамічної рівноваги незалежних змінних, таких як температура, тиск, фізичний стан і хімічний склад речовини тощо.

Другим посиланням є твердження, що всі емпірично встановлені земні оболонки (геосфери) можуть бути схарактеризовані такими змінними: термодинамічними (температура і тиск), фазовими (фізичний стан речовини — газоподібний, твердий і рідкий), хімічними (хімічний склад речовини).

Третє посилання зводиться до того, що в цій системі не врахована ще одна незалежна змінна — жива речовина, що має абсолютно автономне внутрішнє термодинамічне поле і внутрішні рівноваги всіх змінних, що і дає змогу виділити живу речовину, живі організми як ще одну незалежну змінну.

Цілком зрозуміло, що взаємодія всіх змінних реалізується в потоці космічного і сонячного випромінювань (ще одна змінна) і в полі дії гравітаційних сил.

Визначення змінних дає, по суті, перший рівень класифікації можливих екологічних баз даних за об'єктами-функціями: біологічна екологічна база даних, геофізична екологічна база даних (термодинамічні змінні, фазові стани), геохімічна екологічна база даних, екологічна база даних променевої енергії, екологічна база даних космічного випромінювання.

Цілком зрозуміло, що можуть існувати й існують або формуються бази даних у кожній предметній області без визначення «екологічна». Але в них жодним чином не відбиті відносини компонентів. Так, наприклад, в кліматичних базах даних зберігаються відомості про тиск на планеті за різні інтервали часу, про температури, про опади, про хмарність тощо як за станціями, так і за прийнятою растровою мережею, але в них немає відомостей про стан живої речовини або відомостей про газовий склад атмосфери і навпаки.

Звичайно, за певних умов ці бази даних можна об'єднати і досліджувати відносини. Проте таке об'єднання не може бути здійснене суто механічно: по-перше, потрібно синхронізувати спостереження за різними компонентами, по-друге, в об'єднаній базі даних потрібні далеко не всі змінні і їх відповідним чином потрібно відібрати, по-третє, сама синхронізація все-таки буде неминуче не ідеальна і прийнятна лише з деякими допущеннями. Так або інакше створення бази даних екологічного типу — цілком спеціальне завдання і в ідеалі вона має будуватися на основі реальних синхронізованих спостережень, про які поки лише йдеться.

Залежно від того, яку змінну ми визначаємо як функцію, а які змінні — як аргументи, визначається і тип екологічної інформації. Якщо ми визначаємо як функцію живу речовину, то аргументами стає геофізична і геохімічна інформація та інформація про променисту енергію. Якщо як функція розглядається клімат, то відповідно змінюються і об'єм, і зміст інформації.

Складається враження, що неважко — окрім суто технічних затрат — зробити інформаційну систему рівнопотужною, наприклад, і за кліматичними змінними, і за біологічними, і за хімічними, до того ж так, аби вона однаково задовольняла відповідних фахівців. Проте теорія і практика показує, що універсалізм приводить або до великих втрат, так що система не задовольняє практично нікого, або до гігантизму, неповороткості і до подальшої неминучої диференціації на підсистеми, що функціонально діють відносно незалежно.

Оскільки ядром екологічної інформації є жива речовина і людина, то подальшу її типізацію логічно вести саме за цими змінними.

Ієрархічна структура організації живої речовини на надорганіз-менному рівні виглядає таким чином:

- популяційний рівень (сукупність споріднених організмів на обмеженій території, здатних до тривалого самовідтворювання);
- рівень співтовариств (сукупність організмів різних видів, об'єднаних єдністю місця і часу та здатних до тривалого сумісного стійкого співіснування і відтворення);
- екосистемний, або біогеоценотичний, рівень (співтовариство у взаємодії з абіотичними, косними природними тілами, що є його власним (внутрішнім) середовищем).

Для кожного з цих рівнів правомірно говорити про об'єкти різного просторово-часового масштабу: на популяційному рівні — від локальних популяцій до сукупності популяцій, що утворюють вид відповідного організму, на рівні співтовариств — від конкретної, відносно однорідної сукупності організмів до біомів, на екосистем-ному рівні — від конкретної екосистеми з лінійними розмірами конкретного співтовариства до біосфери.

Відповідно екологічна інформація може збиратися на рівні популяції, на рівні співтовариств, на рівні екосистем з урахуванням відповідних аргументів — зовнішніх змінних. При цьому для рівня популяції аргументом можуть бути відомості, що відображають стани співтовариств.

Простір ознак, спостережуваних на кожному рівні, і простір аргументів можуть суттєво різнитися.

Оскільки відношення і відповідно процес є найважливішим атрибутом екологічної інформації, то наступна незалежна змінна при її класифікації зв'язується з функціональною роллю живої речовини в біосфері: продуценти (автотрофи, хемоавтотрофи) і консументи (гетеротрофи 1, 2, 3 порядків, деструктори, редуценти).

Найкомпактніше подається інформація про автотрофи (рослини), сукупності яких добре спостережувані як ціле. Відомості про гетеротрофи на рівні співтовариств надходять в основному через сукупність частинних

показників. Цей класифікаційний рівень екологічної інформації диференціює її на рівні популяцій і співтовариств, але не поширюється на рівень екосистем. На рівні екосистем функціональні типи організмів утворюють ознаковий простір.

Далі класифікація екологічної інформації будується на основі класифікації життєвих форм, яка іноді збігається з токсономічною класифікацією, наприклад:

1. Автотрофи (вищі рослини (трав'янисті (..., ...), дерева (..., ...), чагарники (..., ...), (нижчі рослини (...,...)).

2. Гетеротрофи (фітофаги 1-го порядку (безхребетні, хребетні)) тощо.

Найменування життєвої форми на кожному рівні з відповідною повнотою відображає відношення об'єкта до структури всієї системи і відповідно — функціональне значення відповідної інформації.

В екологічну інформацію на рівні популяції і на рівні співтовариств інформація про параметри середовища зазвичай включається за тими змінними і в тому об'ємі, який необхідний відповідно до загальної концепції для відображення відносин.

Так, автотрофним організмам притаманні такі показники, як сумарний прихід прямої і розсіяної фотосинтетично активної радіації, середні температури, суми біологічно активних температур, середні екстремальні значення температур, середня амплітуда температур за певний період або дисперсія, вологість повітря (екстремальні значення) за періодами, сума опадів за періоди, показники радіаційного балансу і різного типу індекси сухості, тобто всі ті змінні, які відповідно до гіпотези можуть впливати на стан і функціонування автотрофних організмів. Цілком зрозуміло, що такого роду інформація здебільшого є результатом спеціального перетворення інформації, зібраної в рамках вузько-предметної інформаційної системи. Відповідно в більшості випадків аргументи зображаються через вторинну інформацію.

ВИСНОВКИ

У результаті виконання магістерської роботи :

- була вирішена задача автоматизації процесу перевірки цілісності цифрового аудіо–сигналу;
- проведений аналіз існуючих методів перевірки цілісності цифрового сигналу, який показав, що реалізація програмного продукту для виявлення та локалізації фальсифікації цифрового аудіо, збереженого у форматі із втратою інформації, є надзвичайно актуальною;
- була проведена адаптація для цифрового аудіо-сигналу методу виявлення та локалізації фальсифікації цифрового зображення, заснованого на аналізі дослідження функції середньоквадратичного відхилення значень коефіцієнтів ДКП матриці цифрового зображення;
- за результатами обчислювального експерименту в якості порогового значення для відділення частини цифрового аудіо, що містить фальсифікацію від оригінальних частин, було запропоновано використовувати значення 40;
- програмно реалізовано алгоритм виявлення та локалізації фальсифікації цифрового аудіо-сигналу, збереженого у форматі з втратою інформації на основі аналізу дослідження функції середньоквадратичного відхилення значень коефіцієнтів ДКП вектора цифрового аудіо від їх повторно відквантованих значень із різними коефіцієнтами квантування.
- на основі розробленого програмного продукту проведено експериментальні дослідження на реальних аудіо - записах, що підтверджують ефективність його використання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Grigoras C. Digital Audio Recording Analysis: The Electric Network Frequency(ENF) Criterion / C. Grigoras // The International Journal of Speech Language and the Law, 2010. - Vol.12,№1. - P.63–76.

2. Huijbregtse M. Using the ENF Criterion for Determining the Time of Recording of Short Digital Audio Recordings / M. Huijbregtse, Z. Geradts // IWCF 2009: Proceedings of 3rd International Workshop on Computational Forensics, 13-14 August 2009. - Hague, Netherlands, 2009. - P. 116-124.

3. Kraetzer C. Digital Audio Forensics: A First Practical Evaluation on Microphone and Environment Classification / C. . Kraetzer, A. Oermann, J. Dittmann // ACM MM&SEC 2007: Proceedings of the Multimedia and Security Workshop 2007, 20-21 September 2007. - Dallas, Texas, USA, 2007. - P.63-74.

4. Oermann A. Verifyer–tupel for audio–forensic to determine speaker environment / A. Oermann, A. Lang, J. Dittmann // ACM MM&SEC 2005: Proceedings of the Multimedia and Security Workshop 2005, 1-5 August 2005. - New York, USA, 2005. - P.57-62.

5. Гонсалес Р., Вудс Р. Цифровая обработка зображений / Гонсалес Р.- М.: Техносфера, 2012.- 1072 с.

6. Деммель Дж. Вычислительная линейная алгебра / Деммель Дж. – М.: Мир, 2009. - 430 с.

7. Кобозева А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект.- 2007.- №4.- С.531-538.

8. Нариманова Е. В. Исследование эффекта двойного квантования и его использование при обнаружении фальсификации ЦИ / Е. В. Нариманова // Вісник Східноукр-го національного університету імені В. Даля, 2010. - с. 80-85.

9. Нариманова Е. В. Обнаружение и локализация фальсификации цифрового изображения в различных условиях её проведения / Е. В.

Нариманова, Ю. В. Чумаченко //Додаток до журналу «Холодильна техніка і технологія» №5 (133). – 2011. - С.41-42.

10. Рибальський О. В. Застосування вейвлет–аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово–акустичній експертизі / О. В. Рибальский.- К.: НАВСУ, 2004. - 167 с.

11. Рыбальский О. В. Модели нестандартной подделки цифровых фонограмм /О. В. Рыбальский // Реєстрація, зберігання і обробка даних, 2003. - Т. 5, № 4. - С. 25-32.

12. Рыбальский О. В. К экспериментальной проверке достоверности положений теории выявления следов цифровой обработки фонограмм // Реєстрація, зберігання та обробка даних, 2004. - Т.6, №3. - С. 85-98.

13. Рыбальский О. В. Современные методы проверки аутентичности магнитных фонограмм в судебно–акустической экспертизе / О. В. Рыбальский, Ю. Ф. Жариков.- К.: НАВСУ, 2004. - 167с.

14. Рыбальский О. В. Анализ и классификация возможных способов подделки фонограмм/О.В.Рыбальский //Захист інформації,2004.- Спецвыпуск. - С. 44-48.

15. Сэломон Д. Сжатие данных, изображения и звука / Д. Сэломон - М. : Техносфера, 2012. –С. 320-324 .

16. Трифонова Е. А. Адаптация теории матриц для анализа цифрового аудио / Е. А. Трифонова // IV Міжнародна науково–технічна конференція «Сучасні інформаційно–комунікаційні технології» COMINFO–2008. Збірник тез, 2008.– С. 166-168.

17. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. – К.: Юниор, 2003. - 501 с.

18. Хорн Р., Джонсон Ч. Матричный анализ / Хорн Р., Джонсон Ч. — М.: Мир,1989. — 656 с.

19. Фергюсон, Н. Практична криптографія [Текст]: монографія / Н. Фергюсон, Б. Шнайер;Пер. з англ. М.М. Селін. – М. і ін.: ВД Вільямс: Діалектика, 2005. – 421 с.

20. Michael Fink Social- and Interactive-Television Applications Based on Real-Time Ambient-Audio Identification: Fink M., Covel M., Baluja S., Proc. EuroITV'06 Conf., Israel, Center for Neural Computation, Hebrew University of Jerusalem, 2006.

21. Jaap Haitsma, Antonius Kalker, "A Highly Robust Audio Fingerprinting System", International Symposium on Music Information Retrieval (ISMIR) 2002, pp. 107-115.

22. Content and Control: Assessing the Impact of Policy Choices on Potential Online Business Models in the Music and Film Industries. [Електронний ресурс] / John Palfrey, Derek Bambauer, Urs Gasser, Derek Slater, Meg Smith Режим доступу: http://cyber.law.harvard.edu/media/files/content_control.pdf.

23. Cox I.J., The first 50 years of electronic watermarking. Cox I.J., Miller M.L., Journal of Applied Signal Processing, V.2. - 2002, P 126-132.

24. Cano P., Audio Fingerprinting: Concepts and Applications. / Cano P., Gómez E., Batlle E., Gomes L., Bonnet M. // Proceedings of 2002 International Conference on Fuzzy Systems Knowledge Discovery. – Singapore. – 2002.

25. Gomez E. Mixed Watermarking-Fingerprinting Approach for Integrity Verification of Audio Recordings. / Cano P., Gómez E., Batlle E., Gomes L., Bonnet M. // Proceedings of the International Telecommunications Symposium, Natal (Brazil). - 2002.

26. Ананьев А.Б. Спектральное сопоставление музыкальных произведений / Ананьев А.Б., Просвиров Д.В. // Акустичний вісник. – 2004. - Т.7, №3.- С.7-13

27. Rabiner L. R. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition // Proc. of the IEEE. – 1989.- Vol.77, No.2.- P. 257-286 .

28. YouTube / [Електронний ресурс] // Режим доступу: http://www.youtube.com.

29. Philips. Audio Fingerprinting technology / [Електронний ресурс] // Режим доступу: http://www.research.philips.com/initiatives/contentid/audiofp.html. 92

30. Microsoft. Communication, Collaboration, and Signal Processing / [Електронний ресурс] // Режим доступу: http://research.microsoft.com/research/ccsp/.

31. Google / [Електронний ресурс] // Режим доступу: http://www.google.com.

32. Secure Digital Music Initiative / [Електронний ресурс] // Режим доступу: http://www.sdmi.org.

33. Battle E. Scalability issues in an HMM-based audio fingerprinting / Battle E., Masip J., Guaus E., Cano P. // International Conference on Multimedia Computing and Systems.- 2004.- Vol. 1. – P. 735-738. \

34. Lourens J. Detection and Logging Advertisements Using Its Sound // Proc. COMSIG.- Johannesburg (SAR).- 1990.

35. Kurth F. Identification if Highly Distorted Audio Material for Quering Large Scale Databases / Kurth F., Ribbrock A., Clausen M. // Proc. AES 112th Int. – Munich (Germany). – 2002.

36. Batlle E. Feature Decorrelation Methods in Speech Recognition. A Comparative Study / Batlle E., Nadeu C., Fonollosa J. // Proc. of International Conference on Speech and Language Processing. – 1998. - Sydney (Australia).- P. 951-954.

37. Lu L. A robust audio classification and segmentation method / Lu L., Jiang H., Zhang H., Proc. ACM Multimedia (MM'01).– Ottawa (Canada). - 2001. P. 203–211.

38. Batlle E. Automatic song identification in noisy broadcast audio / Batlle E., Masip J., Guaus E. // Proc. of the SIP. - 2002.

39. Morishima M. Phonetically adaptive cepstrum mean normalization for acoustic mismatch compensation / Morishima M., Isobe T., Takahashi J. // Proc. Automatic Speech Recognition and Understanding. – Santa Barbara (USA). - 1997.- P. 436-441.

40. Haitsma J. Robust audio hashing for content identification / Haitsma J., Kalker T., Oostveen J. // Proc. of the Content-Based Multimedia Indexing - Firenze (Italy) .- 2001. 93

41. Cano P. Obust sound modeling for song detection in broadcast audio / Cano P., Batlle E., Mayer H., Neuschmied H. //Proc. AES 112th Int. Conv.- Munich (Germany). – 2002.

42. Zhang T., Hierarchical classification of audio data for archiving and retrieving // Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing.– 1999. – Phoenix (USA). - Vol. 6, pp. 3001–3004.

43. Жирков А.О. Графический метод представления и нейросетевое распознавание частотно-временных векторов речевой информации / Жирков А.О., Корчагин Д.Н., Лукин А.С., Крылов А.С., Баяковский Ю.М. // Программирование.- 2003.- №4.- С.41-52.

44. Allamanche E. Content-Based Identification of Audio Material Using MPEG-7 Low Level Description / Allamanche E., Herre J., Helmuth O., Fröba B., Kasten T. // Proc. International Symposium of Music Information Retrieval. - Indiana (USA). - 2002.

45. Cano P. A review of algorithms for audio fingerprinting. / Cano P., Batlle E., T. Kalker, Haitsma J. //Proc. IEEE Workshop on Multimedia Signal Processing. - 2002. - P. 169-173.

46. Neuschmied H. Content-based identification of audio titles on the internet / Neuschmied H., Mayer H., Batlle E. // Proc. International Conference on Web Delivering of Music.- 2001.

47. Haitsma J. Highly Robust Audio Fingerprinting System// Proc. of the 3rd Int. Symposium on Music Information Retrieval. – 2002. - P. 144-148.

48. Sd Jin Soo Seo. Linear speed-change resilient audio fingerprinting // Sd Jin Soo Seo, Haitsma J., Kalker T., Proc. IEEE Benelux Workshop on Model based Processing and Coding of Audio. – Leuven (Belgium). – 2002.

49. Zwicker E., Fastl H. Psychoacoustics: Facts and Models / Springer Verlag, 2nd ed. - 1999.

50. Plomp, R., & Levelt, W. J. M. Tonal consonance and critical bandwidth // Journal of the Acoustical Society of America. – 1965. - Vol. 37, P.548-560.

51. Dudley H. Remaking speech // Journal of the Acoustical Society of America. – 1939. – Vol. 11. No 2. – P.169-177. 94

52. Drullman R. Effect of temporal envelope smearing on speech reception / Drullman R., Festen J.M., Plomp R. // JASA. – 1994. – Vol. 95. No.2. - P.1053-1064.

53. H. J. M. Steeneken. A physical method for measuring speech transmission quality. H. J. M. Steeneken and T. Houtgast. Journal of the Acoustical Society of America, 67(1):318-326, January 1980.

54. Rhebergen, K. S., ”A Speech Intelligibility Index-based approach to predict the speech reception threshold for sentences in fluctuating noise for normal-hearing listeners,” J. Acoust. Soc. Am. 117, - 2005, P. 2181-2192.

55. T. Chi. “Spectrotemporal modulation transfer functions and speech intelligibility,” / T. Chi, Y. Gao, M. Guyton, P. Ru, and S. Shamma // Journal of Acoustical Society of America, vol. 106, no. 5, pp. 2719–2732, 1999.

56. S. Sheft “Temporal integration in amplitude modulation detection,”/ S. Sheft and W. Yost // Journal of Acoustical Society of America, vol. 88, - 1990. pp. 796–805.

57. Marrakchi-Mezghani I. Robustness of audio fingerprinting systems for connected audio applications / Marrakchi-Mezghani I., Turki-Hadj Alouane M., Jaidane-Saidane M. // Proc. Second International Symposium on Communications, Control and Signal Processing.- 2006.

ДОДАТОК А
ЛІСТИНГ ПРОГРАМИ

```
function varargout = TestAudio(varargin)
% TESTAUDIO M-file for TestAudio.fig
%      TESTAUDIO, by itself, creates a new TESTAUDIO or raises the existing
%      singleton*.
%
%      H = TESTAUDIO returns the handle to a new TESTAUDIO or the handle to
%      the existing singleton*.
%
%      TESTAUDIO('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in TESTAUDIO.M with the given input arguments.
%
%      TESTAUDIO('Property','Value',...) creates a new TESTAUDIO or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before TestAudio_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to TestAudio_OpeningFcn via varargin.
%
%      *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
%
% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help TestAudio

% Last Modified by GUIDE v2.5 14-May-2013 18:01:41

% Begin initialization code - DO NOT EDIT
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @TestAudio_OpeningFcn, ...
                   'gui_OutputFcn',  @TestAudio_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end
```

```
if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before TestAudio is made visible.
function TestAudio_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to TestAudio (see VARARGIN)

handles.Audio=[];
 handles.E1=[];
 handles.E2=[];
 handles.E3=[];
 handles.E4=[];

% Choose default command line output for TestAudio
handles.output = hObject;

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes TestAudio wait for user response (see UIRESUME)
% uiwait(handles.figure1);


% --- Outputs from this function are returned to the command line.
function varargout = TestAudio_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;
```

```
% --- Executes on button press in open_file.
function open_file_Callback(hObject, eventdata, handles)
% hObject    handle to open_file (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
[FileName, PathName] = uigetfile;
% Перевірка вибору файлу
if FileName~=0
    cla(handles.axes1);
    cla(handles.axes2);

    % Формування повного шляху до файлу
    handles.Audio = [PathName FileName];
    % Зчитування із файлу
    [m,fs] = wavread( handles.Audio);
    m=m(:,1);
    m=m(1:28672);
    m=m./max(abs(m));
    m =m(1:(floor(size(m,1)/(64)))*(64));
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    I=[];
    num= G_vec2mat(sqrt(64), [1:64]');
    for k=1:64:size(m,1)
        sod2=m(k:k+63);
        I=[I sod2(num)];
    end
    t=(floor(sqrt(floor(size(I,2)/8))))*8;
    II=[];
    for ww=1:t:size(I,2)
        if (ww+t-1>size(I,2))
        else
            kkk=I(1:8,ww:ww+t-1);
            II=[II;kkk];
        end
    end
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

    handles.gimage=II;
    handles.my_audio =m(1:(size(II,1)*size(II,2)),1);
    handles.my_fs =fs;
    guidata(hObject, handles);
    plot(handles.axes1,handles.my_audio,'b');
    hold on
```

```
 end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [ M ] = G_vec2mat(n, V)
if mod(size(V,1),(n*n))~=0
    V=V(1:floor(size(V,1)/(n*n))*(n*n));
end
M=[];
for i=1:(n*n):size(V,1)
    temp = G8_vec2mat(V(i:(i+(n*n)-1)));
    M=[M;temp];
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [ M ] = G8_vec2mat(V)
I_Z=[];
for i=1:sqrt(size(V,1)):size(V,1)
    I_Z=[I_Z;[i:(i+sqrt(size(V,1)))-1]];
end
M=V(I_Z);

% --- Executes on button press in pushbutton2.
function pushbutton2_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% Зчитування із файлу
A1=wavread(handles.Audio);
A=double(A1(:,1));
II=A(1:28672);

I=round(((II+1)./2).*255);
PBS1=I(1:7168);
PBS2=I(7169:14336);
PBS3=I(14337:21504);
PBS4=I(21505:28672);



fun=@dct;
B1=blkproc(PBS1,[64 1],fun);
B2=blkproc(PBS2,[64 1],fun);
B3=blkproc(PBS3,[64 1],fun);
B4=blkproc(PBS4,[64 1],fun);
```

```
for ii=1:30
    fun=@(x) round(x./ii).*ii;
    B1_=blkproc(B1,[64 1],fun);
    B2_=blkproc(B2,[64 1],fun);
    B3_=blkproc(B3,[64 1],fun);
    B4_=blkproc(B4,[64 1],fun);
    D1=(B1-B1_).^2;
    D2=(B2-B2_).^2;
    D3=(B3-B3_).^2;
    D4=(B4-B4_).^2;
    dd1=0;
    dd2=0;
    dd3=0;
    dd4=0;
    for ch=10:64:7168
        dd1=dd1+D1(ch);
        dd2=dd2+D2(ch);
        dd3=dd3+D3(ch);
        dd4=dd4+D4(ch);
    end;
    ddd1(ii)=dd1;
    ddd2(ii)=dd2;
    ddd3(ii)=dd3;
    ddd4(ii)=dd4;
  end;
      y1=polyfit(1:ii,ddd1,1);
      y2=polyfit(1:ii,ddd2,1);
      y3=polyfit(1:ii,ddd3,1);
      y4=polyfit(1:ii,ddd4,1);

      %розрахунок суми для різних кутів
      S1=abs(y1(1,1)-y2(1,1))+abs(y1(1,1)-y3(1,1))+abs(y1(1,1)-y4(1,1));
      S2=abs(y2(1,1)-y1(1,1))+abs(y2(1,1)-y3(1,1))+abs(y2(1,1)-y4(1,1));
      S3=abs(y3(1,1)-y1(1,1))+abs(y3(1,1)-y2(1,1))+abs(y3(1,1)-y4(1,1));
      S4=abs(y4(1,1)-y1(1,1))+abs(y4(1,1)-y2(1,1))+abs(y4(1,1)-y3(1,1));

      % загальна сума
      S=S1+S2+S3+S4;

      %відносне значення
       handles.E1=(S1./S).*100
       handles.E2=(S2./S).*100
```

```
        handles.E3=(S3./S).*100
        handles.E4=(S4./S).*100

         x=1:ii;

         guidata(hObject, handles);
         H1=plot(handles.axes2,x,y1(1,1)*x+y1(1,2));
         set(H1,'color', [1 0 0]); hold on;

         H2=plot(handles.axes2,x,y2(1,1)*x+y2(1,2));
         set(H2,'color', [0 1 0]); hold on;

         H3=plot(handles.axes2,x,y3(1,1)*x+y3(1,2));
         set(H3,'color', [0 0 1]); hold on;

         H4=plot(handles.axes2,x,y4(1,1)*x+y4(1,2));
         set(H4,'color', [1 1 0]); hold on;


function edit1_Callback(hObject, eventdata, handles)
% hObject    handle to edit1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of edit1 as text
%        str2double(get(hObject,'String')) returns contents of edit1 as a double


% --- Executes during object creation, after setting all properties.
function edit1_CreateFcn(hObject, eventdata, handles)
% hObject    handle to edit1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end

% --- Executes on button press in Analise.
function Analise_Callback(hObject, eventdata, handles)
```

```
% hObject    handle to Analise (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
K= str2double(get(handles.edit1,'String'));


cla(handles.axes1);
axes(handles.axes1);
test=0;

I= handles.Audio;
I=I-min(min(I));
I=I./max(max(I));
 x=1:28224;
    y=handles.my_audio(1:28224,1);
    plot(x,y,'b');hold on

    if (K<= handles.E1)
        x=1:7056;
        y=handles.my_audio(1:7056,1);
        plot(x,y,'r');
        test=1;
    end
    if (K<= handles.E2)
        x=7057:14112;
        y=handles.my_audio(7057:14112,1);
        plot(x,y,'r');
        test=1;
    end
    if (K<= handles.E3)
        x=14112:7057+14112;
        y=handles.my_audio(14112:7057+14112,1);
        plot(x,y,'r');
        test=1;
    end
    if (K<= handles.E4)
        x=7057+14112:28224;
        y=handles.my_audio(7057+14112:28224,1);
        plot(x,y,'r');
        test=1;
    end




hold on
   if(test==0)
    MsgBox('Фальсифікація не виявлена');
end
```

ДОДАТОК Б - КОПІЯ ПУБЛІКАЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

11–12 грудня 2019 року

ТЕРНОПІЛЬ
2019

УДК 681.3.06

П. Телевяк, Л. Матійчук
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЇХ КЛАСИФІКАЦІЯ

UDC 681.3.06

P. Televyak, L. Matiychuk
(Ternopil Ivan Puluj National Technical University, Ukraine)

ANALYSIS OF MODERN INFORMATION PROTECTION METHODS AND THEIR CLASSIFICATION

Для організації успішного бізнесу все більшого значення набуває використання інформаційних технологій. Адже за допомогою своєї інформаційної системи (ІС) кожна компанія організовує всі внутрішні процеси, взаємодіє із зовнішніми партнерами, контрагентами, державними органами. Забезпечення безпеки й постійної працездатності інформаційної системи є одним із пріоритетних завдань будь-якого підприємства.

Створення сучасних комп'ютерних систем і поява глобальних комп'ютерних мереж радикально змінили характер і діапазон проблем захисту інформації. У широко комп'ютеризованому й інформатизованому сучасному суспільстві володіння реальними цінностями, керування ними, передача цінностей або доступ до них часто побудовані на інформації, існування якої не обов'язково пов'язується з яким-небудь записом на фізичному носії. Тому досить важливо створювати й застосовувати ефективні засоби для реалізації всіх необхідних функцій, пов'язаних із забезпеченням конфіденційності й цілісності електронної інформації.

Методи захисту інформації можна класифікувати по меті їх використання на методи активного та пасивного захисту. Метою методів активного захисту інформації є збереження всіх категорій інформації. Методи пасивного захисту інформації (МПЗІ) націлені на те, щоб дати відповідь, чи було зроблено навмисне порушення якоїсь категорії інформації. МПЗІ за способом їх реалізації можна розділити на методи експертної оцінки, програмно-технічні й програмні.

Методи експертної оцінки використовують візуальне або акустичне оцінювання інформації фахівцем. Головним недоліком методів експертної оцінки є наявність людського фактору.

Програмно-технічні МПЗІ грунтуються на знанні специфічних особливостей пристроїв аудіо –, відео – або фотофіксації та (або) впливу якихось зовнішніх факторів на проведення запису. До програмно-технічних МПЗІ відносяться методи, присвячені доведенню цілісності цифрових звукозаписів, засновані на перевірці технічних засобів фіксації аудіосигналів та аналізі можливих способів фальсифікації сигналограм.

У процесі теоретичних досліджень були встановлені способи проведення такої обробки. Виявлено, що фонограми можуть бути оброблені або способом компіляції фрагментів в персональній електронній обчислювальній машині (ПЕОМ) за допомогою звукових редакторів, або способом синтезу необхідного тексту за заданими зразками голосів фігурантів створюваної фонограми. Однак, при використанні будь-якої з цих технологій, попередньо необхідно ввести в ПЕОМ фонограми із зразками мовлення фігурантів. Такі первинні фонограми можуть бути записані на цифровій апаратурі запису аналогових сигналів (ЦАЗАС) і введені в машину в цифровій або аналоговій формі (залежно від типу використовуваної апаратури запису). Таким же чином вони можуть бути введені з комп'ютера при перезапису обробленої фонограми на ЦАЗАС. Можливий ще варіант перезапису обробленої фонограми по акустичному каналу. Крім того, у процесі створення обробленої фонограми завжди використовується операція стробування і вирізання фрагментів, оскільки, навіть при використанні способу синтезу, оброблена фонограма повинна містити діалог як мінімум двох осіб.