УДК 004.85
DOI 10.36910/10.36910/6775-2313-5352-2024-24-15
Світловський Є.В.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

МОДЕЛІ І АЛГОРИТМИ СТВОРЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ДЛЯ АУДІО-ФАЙЛІВ

В статті описано методи сучасної теорії інформаційних процесів та систем, а саме: методи теорії статистичних рішень; методи теорії ймовірностей та математичної статистики; технології об'єктно-орієнтованого програмування; теорія випадкових процесів та полів методи та технології статистичного імітаційного моделювання; методи цифрової обробки та розпізнавання сигналів та зображень; апарат штучних нейронних мереж; методи комп'ютерної стеганографії, а також технології проведення прямого комп'ютерного експерименту, що виконується по відношенню до реальних об'єктів цифрового контенту.

Отримано моделі і алгоритми створення цифрових водяних знаків для об'єктів звукових форматів. Алгоритми створення цифрових водяних знаків для об'єктів, формат представлення даних, а також дослідження їх можливості для застосування файлів звукових форматів. Методики та результати аналізу статистичної помітності і можливості відновлення вбудованої послідовності ЦВЗ стороннім спостерігачем для оцінки якості ЦВЗ в об'єктах звукових форматів. Встановлено доцільність побудови та використання універсальних стискаючих перетворень для стеганографічного вбудовування ЦВЗ в об'єкти-контейнери різних типів з мінімальним рівнем дисперсії спотворень на основі штучних двошарових нейронних мереж прямого поширення, що дає змогу підвищити ефективність та захищеність передачі прихованих даних каналами зв'язку. Розробка спеціального математичного та програмного забезпечення з метою створення цифрових водяних знаків як засобів прихованого маркування об'єктів цифрового контенту, які забезпечують ефективний контроль використання об'єктів інтелектуальної власності, а також для діагностики аудіоданих.

Ключові слова: *цифровий водяний знак, аудіофайл, нейромережа, модель, алгоритм, маркування, цифровий контент, аудіодані, середньоквадратична похибка.*

Постановка проблеми. На сучасному етапі розвитку інформаційних систем та технологій, глобальних комп'ютерних мереж та засобів мультимедіа стимулює розробку нових методів аналізу, зберігання, відтворення та передачі даних каналами інформаційних комунікацій. До них належать методи і засоби забезпечення високонадійної обробки даних в інформаційних структури та системи, методи підвищення надійності та безпеки використання інформаційних технологій.

Зараз одним з найбільш затребуваних підходів у цій галузі є застосування технологій, базуються на використанні методів комп'ютерної стеганографії, що дозволяють приховано вбудовувати необхідні дані в будь-які інформаційні масиви та об'єкти цифрового контенту (ОЦК).

Питання стеганографічного приховування інформації розглядали дослідники: Сіммонс (G.J. Simmons), Д. Фрідріч (J. Fridrich), Р. Андерсон (R. Anderson), Ст Бендер (W. Bender), Н. Андерсон та інші [4-8].

В роботах [4-8] наведено базову систему означень та математичні моделі стеганографічних систем. Велика кількість вітчизняних та зарубіжних публікацій присвячена аналізу головної характеристики стегосистеми – її стійкості.

Результати дослідження стеганографічних алгоритмів на стійкість наводять у своїх роботах Д. Фрідріч (J. Fridrich). Р. Попа (R. Popa), Н. Джонсон (N. Johnson), С. Волошиновський (S. Voloshynovskiy) [6, 8-10].

В роботах [6, 8-10] наведено комплексний огляд теоретико-інформаційного, теоретико-складнісного та теоретико-ігрового підходу до оцінки стійкості стеганографічних систем.

Методи комп'ютерної стеганографії ґрунтуються на тому, що процес вбудовування послідовності даних у вихідний об'єкт цифрового контенту носить прихований характер, при цьому не порушується цілісність та функціональність ОЦК.

Для ефективного застосування технологій цифрових водяних знаків (ЦВЗ) необхідно виконати ряд суперечливих вимог, а саме: забезпечити аудіо- непомітність повідомлень, зберегти вихідну якість вихідного контейнера і одночасно забезпечити високу достовірність вилучення повідомлення з урахуванням можливих ненавмисних та навмисних впливів на каналі передачі. Зазначені протиріччя не знімаються повною мірою у відомих методах та алгоритмах створення ЦВЗ. Оскільки методи створення цифрових водяних знаків почали розроблятися нещодавно, то тут є багато невирішених проблем. Однією з них є проблема збереження якості маркованих при впровадженні ЦВЗ файлів при їх використанні за основним призначенням поєднанні зі стійкістю вбудовуваних міток до можливих перетворень контейнера та забезпечення достовірності подальшого відновлення ЦВЗ. Перспективним завданням є подальший розвиток та розробка нових технологій створення ЦВЗ, що володіють невисокою складністю впровадження та детектування, візуальної непомітністю, адаптованістю та універсальністю, гарною стійкістю до різноманітних спотворень і трансформаціям цифрового об'єкта, що захищається, можливістю виявлення цифрової мітки без вихідного файлу.

Аналіз останніх досліджень і публікацій. Одним із найважливіших напрямів комп'ютерної стеганографії, що набула широкого поширення останнім часом, є застосуванням технологій цифрових водяних знаків (ЦВЗ). ЦВЗ - це спеціальні мітки, що впроваджуються у файл, в цифровий сигнал з метою контролю їх правомірного використання [4].

Застосування ЦВЗ дозволяє не тільки створити складності для порушення авторських прав, але проконтролювати його використання авторизованими користувачами та іншими особами. Поряд з інформацією, представленої у формі цифрових зображень (фотографіями, малюнками, відсканованими паперовими документами і т.д.), ЦВЗ також широко використовуються і для маркування відео- та аудіоданих. ЦВЗ діляться на два типи - видимі та невидимі [8].

Видимі ЦВЗ досить просто видалити чи замінити за допомогою спеціалізованого програмного забезпечення.

Невидимі ЦВЗ - це вбудовані в цифрові файли мітки, що не сприймаються людським оком чи слухом. Для ефективного застосування технологій ЦВЗ необхідно виконати низку суперечливих вимог, а саме: забезпечити аудіо- та візуальну непомітність повідомлень, зберегти вихідну якість вихідного контейнера і одночасно забезпечити високу достовірність вилучення повідомлення з урахуванням можливих ненавмисних та навмисних впливів на канал передачі. Вказані протиріччя не знімаються повною мірою у відомих методах та алгоритмах створення ЦВЗ.

Застосування нейромережевих технологій обробки інформації принципово дозволяє вирішити дві проблеми, пов'язані зі створенням ЦВЗ, а саме: реалізувати функціональний підхід до побудові алгоритмів вбудовування (кодування) та вилучення (декодування) ЦВЗ і одночасно забезпечити універсальний характер виконуваних у своїй перетворень інформації [2, с. 122].

Як показують попередні дослідження, саме функціональний характер виконуваних за допомогою нейронних мереж перетворень, на відміну від класичного алгоритмічного підходу, та застосування штучних нейронних мереж різних типів для реалізації технологій цифрових водяних знаків, дозволяє забезпечити меншу «прозорість» процесу вбудовування та гарний компроміс між візуальною непомітністю, стійкістю впровадження цифрових міток та обсягом використовуваних обчислювальних ресурсів.

Мета роботи. Полягає в дослідженні моделі та алгоритмів створення цифрових водяних знаків в аудіофайлах, заснованих на побудові нейромережевих стискаючих відображень, в інтересах підвищення скритності та стійкості, а також забезпечення універсальності алгоритмів створення ЦВЗ.

Викладення основного матеріалу. Розглядаються три основні типи ЦВЗ: робасні (РЦВЗ), крихкі (КЦВЗ), напівкрихкі (НЦВЗ) (табл. 1) [7, с.454].

Таблиця 1 - Класифікація цифрових водяних знаків

Технологія	Особливості
Робасні (РЦВЗ)	Мають високу стійкість до зовнішніх впливів
Крихкі (КЦВЗ)	Руйнуються при незначній модифікації заповненого контейнер. Застосовуються для автентифікації сигналів.
Напівкрихкі (НЦВЗ)	Стійкі по відношенню до одних впливам і не стійкі - до іншим

Завдання вбудовування та виділення повідомлень з іншої інформації виконує стегосистема (рис. 1) [7, с. 456].

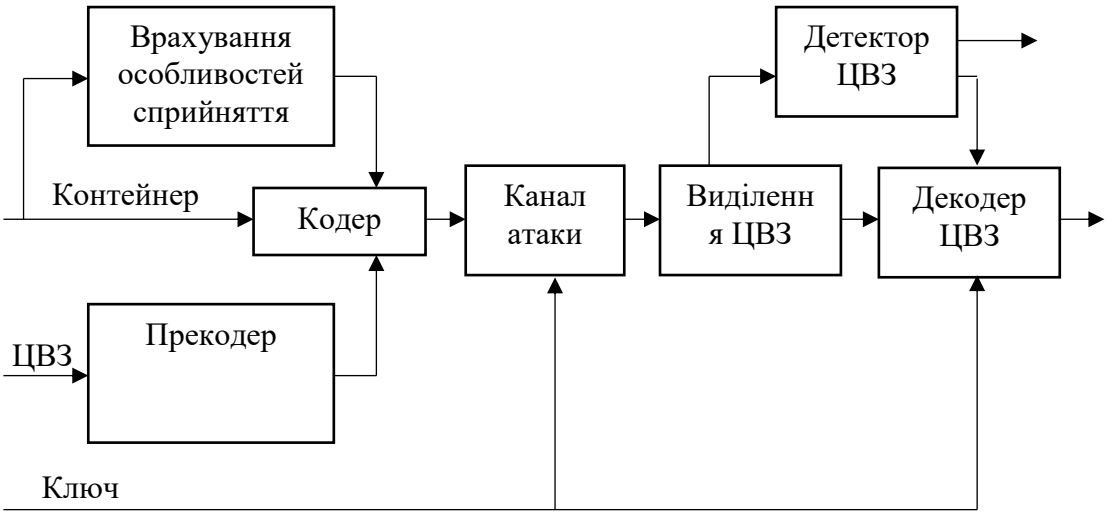


Рисунок 1 – Структурна схема стегосистеми ЦВЗ

Стегосистема складається з наступних основних елементів:

– прекодер – пристрій, призначений для перетворення приховуваного повідомлення до вигляду, зручному для вбудовування сигнал-контейнер;

– стегокодер - пристрій, призначений для здійснення вкладення прихованого повідомлення до інших даних з урахуванням їхньої моделі;

– пристрій виділення вбудованого повідомлення;

– стегодетектор – пристрій, призначений для визначення наявності стегоповідомлення;

– декодер - пристрій, що відновлює приховане повідомлення. Цей вузол може бути відсутнім.

Особливість вказаного підходу полягає в тому, що комплекс спеціально навчених нейронних мереж використовується для реалізації ЦВЗ, як для приховання, так і відновлення перетворень. Саме функціональний характер виконуваних за допомогою нейронних мереж перетворень (на відміну класичного алгоритмічного підходу) і застосування штучних нейронних мереж різних типів для реалізації технологій цифрових водяних знаків, що дозволяє забезпечити меншу «прозорість» процесу вбудовування та гарний компроміс між непомітністю, стійкістю впровадження цифрових міток та обсягом використовуваних обчислювальних ресурсів. [9, с. 22]

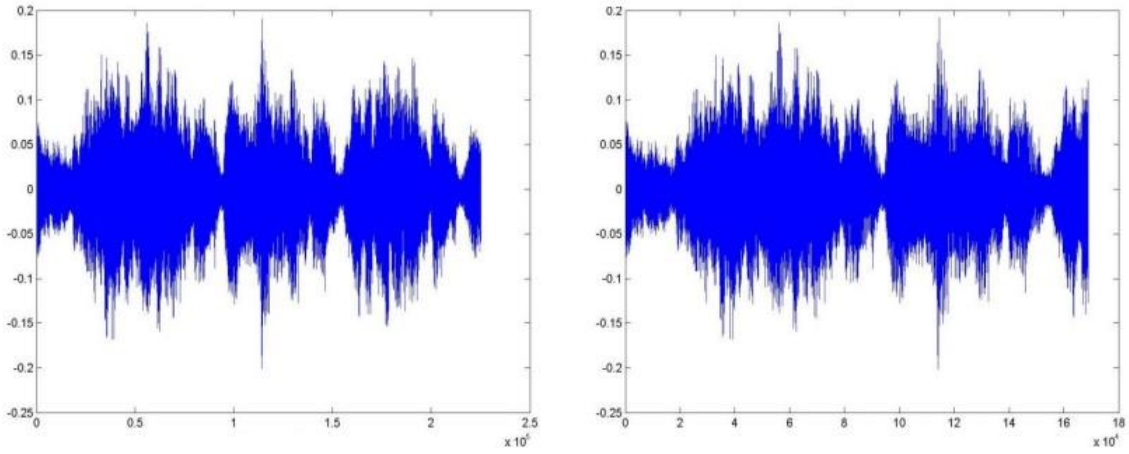
Апарат штучних нейронних мереж дозволяє реалізувати алгоритми, при використання яких процес вбудовування даних у файл-контейнер носить значно менш стійкий характер. Для відновлення ЦВЗ та ідентифікаційних номерів підвищеної скритності використовується нейромережеві алгоритми статистичної класифікації елементів раніше прихованої послідовності даних, які навчаються з урахуванням особливостей реалізованої процедури вбудовування. Функціональні можливості використовуваних нейромережевих алгоритмів обробки інформації орієнтовані, перш за все, на мінімізацію спотворень файлів-контейнерів, представлених у форматах високої якості, та забезпечення меншої «прозорості» процесу створення ЦВЗ, що дозволяє розробити нову високонадійну технологію створення ЦВЗ, яка не впливає на сприйняття об'єкта [1, с. 21].

Дослідження показують, що багато характеристик звуку є для кожної людини суб'єктивними та індивідуальними. Частотна характеристика звуку для більшості людей є однаковою. Дослідження сприйняття звуку показало, що поріг чутності на різних частотах неоднаковий, тому вбудовування ЦВЗ у високочастотну область аудіофайл буде істотно менш помітно для слухача. Відповідно, були проведені дослідження питань створення ЦВЗ для аудіо-файлів при варіації різних параметрів (частота дискретизації сигналу, бітність амплітуди сигналу та кількість каналів відтворення) [5, с. 324].

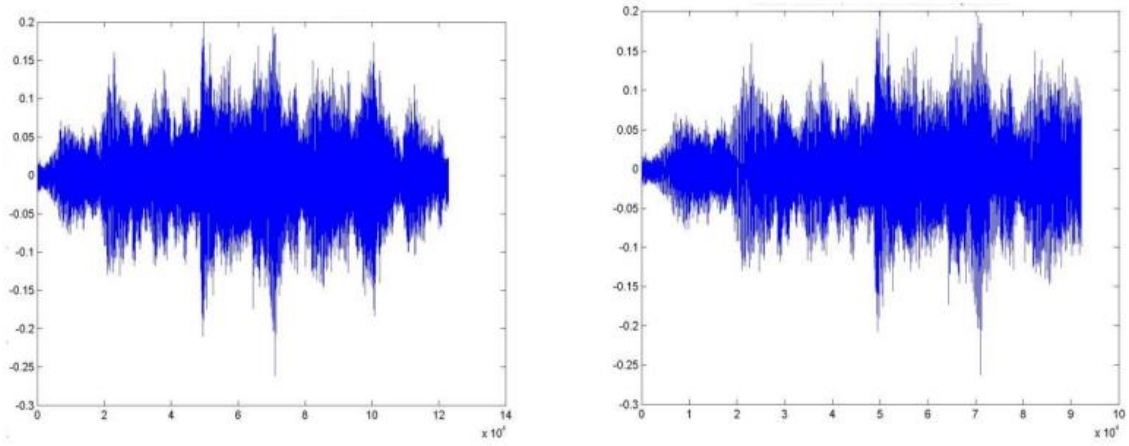
При моделюванні мінімальне значення амплітуди задавалася рівним, виходячи з типової розрядності (16 біт) представлення аудіо-файлів.

$$a_m = 0.5/65535$$

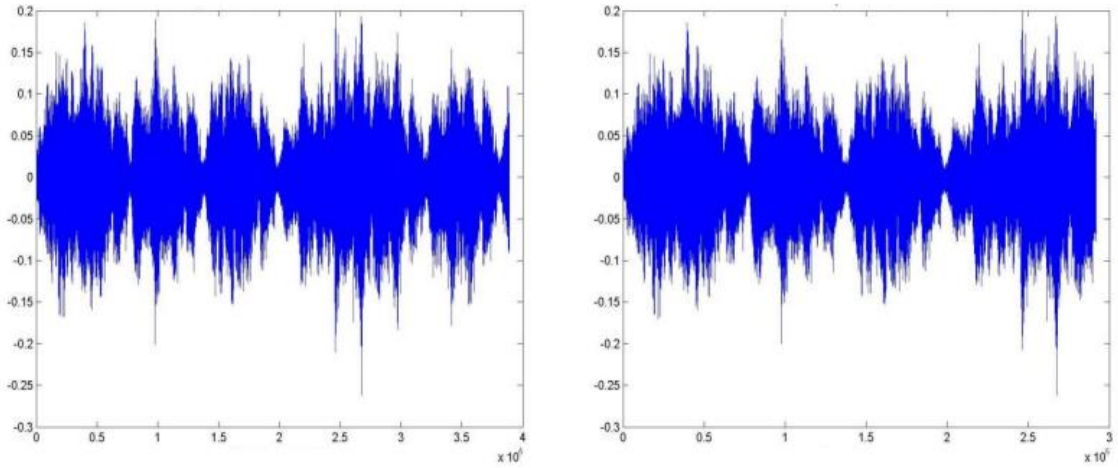
Дослідимо якість алгоритму залежно від частоти дискретизації сигналу. На рисунку 2а представлений вихідний моно сигнал з параметрами: частота дискретизації сигналу 11025 Гц, розрядність вихідного сигналу 16 біт, рисунку 2б представлений результуючий сигнал, що містить вбудовану послідовність ЦВЗ. На рис. 2в представлено вихідний моно сигнал із параметрами: частота дискретизації сигналу 22050 Гц, розрядність вихідного сигналу 16 біт, рис. 2г - результуючий сигнал, що містить вбудовану послідовність ЦВЗ. На рис. 2д представлений вихідний моно сигнал із параметрами: частота дискретизації сигналу 44100 Гц, розрядність вихідного сигналу 16 біт, на рисунку 2е представлений результуючий сигнал, що містить вбудовану послідовність ЦВЗ.



а) б)



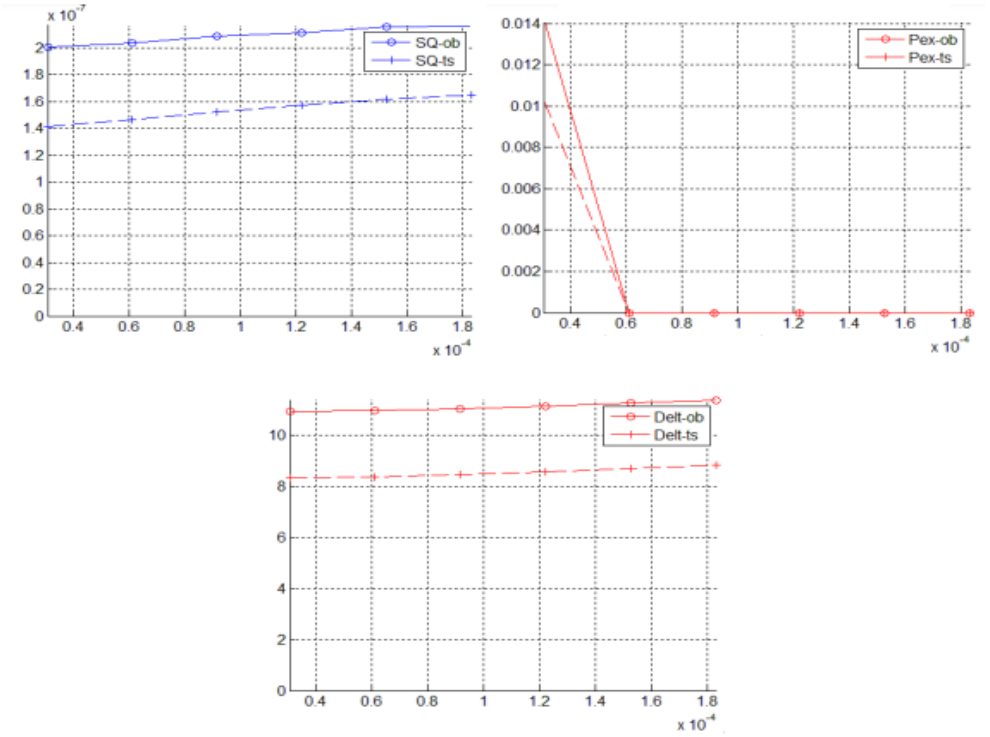
в) г)



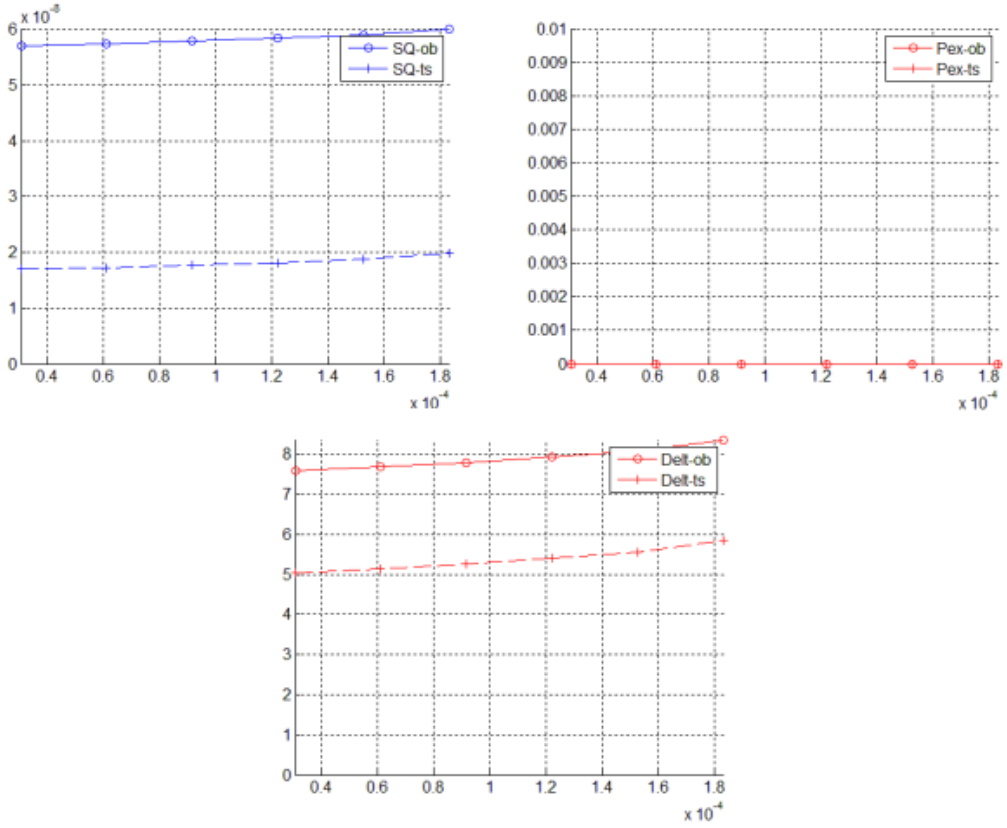
д) е)

Рисунок 2 – Вихідний сигнал та результуючий сигнал 11025 Гц (а,б); вихідний аудіо-сигнал та результуючий сигнал 22050 Гц (в, г) вихідний аудіо-сигнал та результуючий сигнал 44100 Гц (д,е)

На рисунку 3 наведено залежності середньої квадратичної та абсолютної похибок спотворення контейнера та ймовірності похибки відновлення контейнера від амплітуди вбудовуваної послідовності, отримані для вихідних аудіофайлів з різними частотами дискретизації сигналу.



а)



б)

Рисунок 3 – Залежність середньоквадратичної похибки спотворення контейнера, ймовірності похибки відновлення ЦВЗ, абсолютної помилки спотворення контейнера для аудіофайлів з різними частотами дискретизації сигналу 11025 Гц (а); 22050 Гц (б);

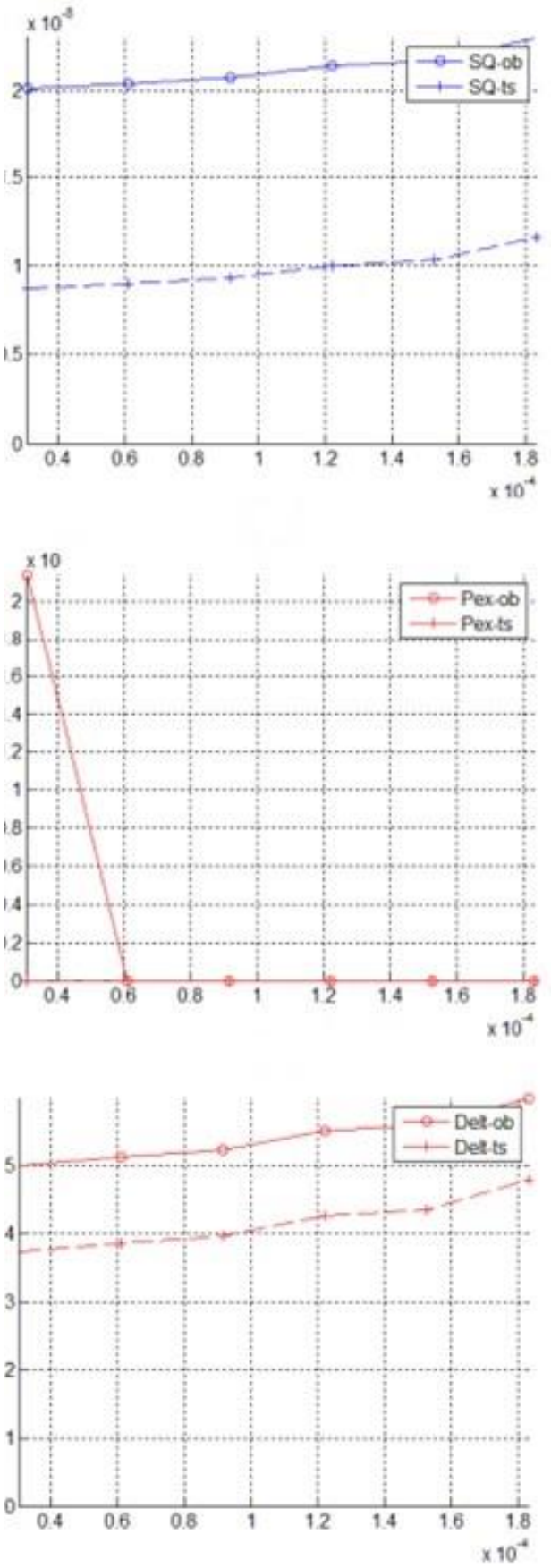


Рисунок 4 – Залежність середньоквадратичної похибки спотворення контейнера, ймовірності похибкики відновлення ЦВЗ, абсолютної похибки спотворення контейнера для аудіофайлів з частотою дискретизації сигналу 44100 Гц

При роботі з аудіо-контентом часто зустрічається не тільки моносигнал, який передає один канал звучання, а й більше каналів. Серед часто використовуваних варіацій кількості каналів передачі аудіо сигналу використовується стерео сигнал, який включає 2 канали.

На рисунку 5 наведено залежність середньої квадратичної та абсолютної помилок спотворення контейнера та ймовірності помилки відновлення контейнера від амплітуди вбудовуваної послідовності для вихідного сигналу з параметрами 22050 Гц, 16 біт, сигнал стерео.

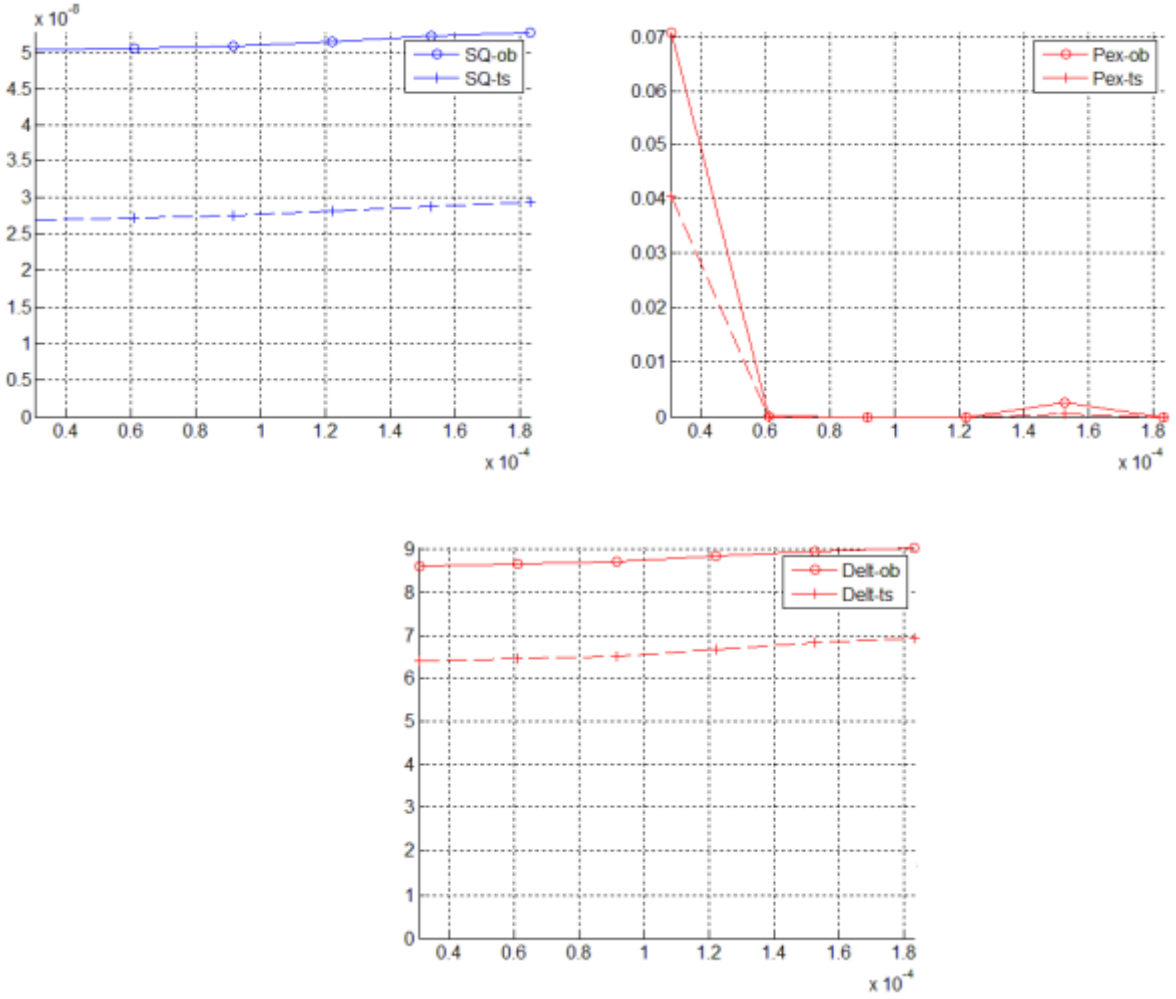


Рисунок 5 – Залежність середньої квадратичної, абсолютної похибок спотворення контейнера та ймовірності похибки відновлення контейнера від амплітуди вбудовуваної послідовності для вихідного сигналу з параметрами 22050 Гц, 16 біт, сигнал стерео

Як показали результати експериментів, алгоритми для аудіо-файлів продемонстрували хороші результати з мінімізації спотворень при створенні маркованих контейнерів (алгоритм функціонального вбудовування та нейромережевий алгоритм модифікації усередненого значення блоків), а також при відновленні ЦВЗ.

Висновки. Результати проведених експериментальних досліджень для аудіо-файлів (WAV формату) показують можливість приховування великих обсягів інформації, за рахунок того, що вибрані формати не передбачають попередньої декомпресії та наступного після приховування стиснення (наприклад, MPEG), при цьому проведено дослідження для сигналів різної бітності та частоти дискретизації. При реалізації вказаного підходу до створення ЦВЗ для аудіо-файлів забезпечується відносна середня квадратична похибка спотворення фрагментів контейнера порядку 10^{-7} ...10^{-8} при ймовірності похибки відновлення елементів двійкової послідовності ЦВЗ порядку 10^{-1} ...10^{-2} залежно від частоти дискретизації сигналу.

Інформаційні джерела

1. Бабич І. В. Огляд стеганографічних методів перетворення інформації. Захист інформації. 2022. № 1. С. 18-24

2. Навроцький Д. О. Дослідження результатів стеганорафічного приховування повідомлень у файлах як засобу забезпечення захисту інформації. Вісник Національного технічного університету України «КПІ». 2022. №50. С. 121-128.

3. Кущ С. Алгоритм формування стеганограм на основі LSB-методу. Захист інформації і безпека інформаційних систем. Л. 2021. С. 110-111.

4. Anderson, R. J. Stretching the Limits of Steganography. Information Hiding Springer Lecture Notes in Computer Science. 2016. P. 39-48.

5. Bender, W. Techniques for Data Hiding. IBM Systems Journal. 2016. Vol. 35. P. 313-336.

6. Fridrich, J. Steganalysis of LSB Encoding in Color Images. Proceedings of ICME. 2020. Vol. 3. P. 1279-1282.

7. Gustavus, J. Simmons. The History of Subliminal Channels. II IEEE Journal on Selected Areas of Communications. 2018. Vol. 16. №4. P. 452-461.

8. Johnson, N. F. Information Hiding: Steganography and Watermarking - Attacks and Countermeasures. Springer. 2021. 137 p.

9. Popa, R. An Analysis of Steganographic Techniques. The Polytechnic University of Timisoara. Faculty of Automatics and Computers. Department of Computer Science and Software Engineering. 2021. 59 pp.

10. Schneier, B. Applied Cryptography: Protocols. Algorithms, and Source Code in C. John Wiley and Sons. 2016. 784 p.

Svitlovskyi Y.
National Technical University of Ukraine «Ihor Sikorsky Kyiv Polytechnic Institute»

MODELS AND ALGORITHMS FOR CREATING DIGITAL WATERMARKS FOR AUDIO FILES

To justify and investigate models and algorithms for creating digital watermarks in audio files based on the construction of neural network compressive maps, in the interests of increasing stealth and stability, as well as ensuring the universality of algorithms for creating CVZ. The methods and approaches of the modern theory of information processes and systems were used, namely: methods of the theory of statistical solutions; methods of probability theory and mathematical statistics; technologies of object-oriented programming; theory of random processes and fields, methods and technologies of statistical simulation modeling; methods of digital processing and recognition of signals and images; apparatus of artificial neural networks; methods of computer steganography, as well as the technology of direct computer experiment, which is performed in relation to real objects of digital content.

Algorithms for creating digital watermarks for audio format objects have been obtained. Algorithms for creating digital watermarks for objects, the format of data presentation, as well as researching their possibility for the use of sound format files. Methods and results of the analysis of statistical visibility and the possibility of restoring the built-in sequence of TVS by a third-party observer for assessing the quality of TVS in objects of sound formats. The expediency of building and using universal compressive transformations for steganographic embedding of CVZ into container objects of various types with a minimum level of dispersion of distortions on the basis of artificial two-layer forward propagation neural networks has been established. The results of the research are of practical importance for the development of special mathematical and software in the interests of creating digital watermarks as means of hidden marking of digital content objects, which provide effective control of the use of intellectual property objects, as well as for audio data diagnostics.

***Key words**: digital watermark, audio file, neural network, algorithm, marking, digital content, audio data, root mean square error.*