НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

КАФЕДРА СИСТЕМНОГО ПРОГРАМУВАННЯ І
СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

«На правах рукопису»
УДК 044.77

«До захисту допущено»

Завідувач кафедри СПСКС

_____ В.П.Тарасенко_
(підпис) (ініціали, прізвище)

"___"_____2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 123 Комп'ютерна інженерія
(Комп'ютерні системи та компоненти)

на тему: Модифікований спосіб ущільнення великих об`ємів даних

Виконав (-ла): студент (-ка) ІІ курсу, групи КВ-61м

Щербакова Галина В'ячеславівна

Науковий керівник доцент кафедри, ктн, Орлова М.М.

Рецензент професор кафедри ОТ, д.т.н., професор Симоненко В.П.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
(Комп'ютерні системи та компоненти)

ЗАТВЕРДЖУЮ
Завідувач кафедри СПСКС
_____ _В.П.Тарасенко__
(підпис) (ініціали, прізвище)
«___»_____2018р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Щербакової Галини В'ячеславівни

1. Тема дисертації Модифікований спосіб ущільнення великих об`ємів даних, науковий керівник дисертації Орлова Марія Миколаївна доцент кафедри СПіСКС, к.т.н., доцент

затверджені наказом по університету від «22» березня 2018 р. №986-с

2. Термін подання студентом дисертації 11 травня 2018 р.

3. Об'єкт дослідження способи ущільнення великих обсягів даних

4. Предмет дослідження великі обсяги даних та тривимірні дані

5. Перелік завдань, які потрібно розробити
   - опис предметної області досліджень та обґрунтування ущільнення даних;
   - шляхи вирішення проблеми ущільнення великих обсягів даних;
   - модифікований спосіб ущільнення тривимірних даних.

6. Перелік ілюстративного матеріалу
   - Процес ущільнення даних.
   - Алгоритми ущільнення даних.

- Представлення тривимірних даних у медицині.
- Розроблений спосіб
- Схема вейвлет-перетворення тривимірних даних
- Процес роботи вейвлет-перетворення тривимірних даних

7. Перелік публікацій

- «Модифікований спосіб ущільнення великих обсягів даних», Міжнародний науковий журнал «Інтернаука». – 2018. – №8;
- X наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2018 (Київ, 21-23 березня 2018 р.);
- XI Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 19-21 квітня 2018 р.);
- IIX наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2016 (Київ, 20-22 квітня 2016 р.);
- IX Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 21-23 квітня 2016 р.).

8. Дата видачі завдання 5 вересня 2016 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Вивчення літератури за тематикою проекту	20.10.2017	
2	Аналіз існуючих рішень	20.12.2017	
3	Підготовка матеріалів першого розділу магістерської дисертації	09.01.2018	
4	Підготовка матеріалів другого розділу магістерської дисертації	05.02.2018	
5	Підготовка матеріалів третього розділу магістерської дисертації	05.03.2018	
6	Підготовка графічної частини дипломного проекту	23.03.2018	
7	Оформлення документації дипломного проекту	20.04.2018	
8	Попередній розгляд магістерської дисертації на кафедрі	26.04.2018	

Студент _____ Щербакова Г.В.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Орлова М.М.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Актуальність теми. Розвиток обчислювальної техніки в сучасному світі технології йде дуже швидкими темпами - зростає частота і продуктивність процесорів, збільшуються обсяги пам'яті і прискорюється час доступу до неї. Однак при такому бурхливому зростанні швидкостей різних пристроїв швидкість передачі даних зростає значно меншими темпами. Особливістю більшості типів даних є їх надлишковість. При зберіганні та передачі великих обсягів інформації надмірність відіграє негативну роль, оскільки вона призводить до зростання не тільки вартості зберігання, а й часу передачі інформації. В зв'язку з цим на сьогоднішній день для забезпечення ефективності зберігання, передачі великих обсягів інформації широко використовуються алгоритми ущільнення.

Об’єктом дослідження є способи ущільнення великих обсягів даних.

Предметом дослідження є великі обсяги даних та тривимірні дані.

Мета роботи: Метою роботи є підвищення ефективності існуючих способів ущільнення даних за рахунок розробки модифікованого способу ущільнення великих обсягів даних.

Наукова новизна полягає в наступному:

1. Розроблено методику, що відрізняється від відомих поєднанням вевлет-перетворення тривимірних даних та ентропійного кодування, що дозволяє отримати ущільнення даних без втрат.
2. Запропоновано модифікований спосіб ущільнення тривимірних даних, який призводить до збільшення показника пікового значення сигналу до шуму та зменшення середньо-квадратичної похибки.

Практична цінність отриманих в роботі результатів полягає в тому, що запропонований спосіб ущільнення інформації дає змогу отримати

покращені результати порівняно з існуючими способами в середньому на 15% без погіршення якості.

Апробація роботи.

– X наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2018 (Київ, 21-23 березня 2018 р.);

– XI Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 19-21 квітня 2018 р.);

– IIX наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2016 (Київ, 20-22 квітня 2016 р.);

– IX Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 21-23 квітня 2016 р.).

Публікації: За матеріалами проведених досліджень опубліковано 5 наукові праці, з них 1 стаття в науковому фаховому видані, яке входить до наукометричних баз даних, та 4 тези доповідей на конференцію.

Структура та обсяг роботи. Магістерська дисертація складається з вступу, трьох розділів та висновків.

У вступі подано загальну характеристику роботи, зроблено оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень, сформульовано мету і задачі досліджень, показано наукову новизну отриманих результатів і практичну цінність роботи, наведено відомості про апробацію результатів і їхнє впровадження.

У першому розділі розглянуто опис предметної області досліджень та було наведено обґрунтування теми магістерської роботи.

У другому розділі наведено опис способів ущільнення великих обсягів даних.

У третьому розділі описано модифікований спосіб ущільнення.

У висновках представлені результати проведеної роботи.

Робота представлена на 84 аркушах, містить посилання на список використаних літературних джерел.

Ключові слова: алгоритм, ущільнення, тривимірні дані, медичні зображення, ущільнення без втрат, зображення, ентропійне кодування.

РЕФЕРАТ

Актуальность темы. Развитие вычислительной техники в современном мире технологии идет очень быстрыми темпами - растет частота и производительность процессоров, увеличиваются объемы памяти и ускоряется время доступа к ней. Однако при таком бурном росте скоростей различных устройств скорость передачи данных возрастает значительно меньшими темпами. Особенностью большинства типов данных является их избыточность. При хранении и передачи больших объемов информации избыточность играет отрицательную роль, поскольку она приводит к росту не только стоимости хранения, но и времени передачи информации. В связи с этим на сегодняшний день для обеспечения эффективности хранения, передачи больших объемов информации широко используются алгоритмы сжатия.

Объектом исследования является способы сжатия данных.

Предметом исследования являются большие объемы данных и трехмерные данные.

Цель работы: Целью работы является повышение эффективности существующих способов сжатия данных за счет разработки модифицированного способа сжатия больших объемов данных.

Научная новизна заключается в следующем:

1. Разработана методика, отличающаяся от известных сочетанием вейвлет-преобразования трехмерных данных и энтропийного кодирования, позволяющая получить сжатия данных без потерь.
2. Предложен модифицированный способ сжатия трехмерных данных, который приводит к увеличению показателя пикового значения сигнала к шуму и уменьшению средне-квадратичной погрешности.

Практическая ценность полученных в работе результатов заключается в том, что предложенный способ сжатия информации позволяет

получить улучшенные результаты по сравнению с существующими способами в среднем на 15% без ухудшения качества.

Апробация работы.

– X научная конференция магистрантов и аспирантов «Прикладная математика и компьютинг» ПМК-2018 (Киев, 21-23 марта 2018);

– XI Международная научно-техническая конференция «Компьютерные системы и сетевые технологии» (Киев, 19-21 апреля 2018);

– IIX научная конференция магистрантов и аспирантов «Прикладная математика и компьютинг» ПМК-2016 (Киев, 20-22 апреля 2016);

– IX Международная научно-техническая конференция «Компьютерные системы и сетевые технологии» (Киев, 21-23 апреля 2016).

Публикации: По материалам проведенных исследований опубликовано 5 научных работ, из них 1 статья в научном профессиональном издании, которое входит в наукометрические базы данных, и 4 тезиса докладов на конференцию.

Структура и объем работы. Магистерская диссертация состоит из введения, трех глав и выводов.

В введении представлена общая характеристика работы, произведена оценка современного состояния проблемы, обоснована актуальность направления исследований, сформулированы цели и задачи исследований, показано научную новизну полученных результатов и практическую ценность работы, приведены сведения об апробации результатов и их внедрение.

В первом разделе рассмотрены описание предметной области исследований и были приведены обоснования темы магистерской работы.

Во втором разделе описаны базовых алгоритмов сжатия без потерь.

В третьем разделе описано улучшенный алгоритм сжатия без потерь.

В выводах представлены результаты проведенной работы.

Работа представлена на 84 листах, содержит ссылки на список использованных литературных источников.

Ключевые слова: алгоритм, сжатие, трехмерные данные, медицинские изображения, сжатие без потерь, изображения, энтропийное кодирование.

ABSTRACT

Actuality of theme. The development of computing technology in the modern world of technology is very fast - the frequency and performance of processors are increasing, memory volumes increase and access time is accelerated. However, with such a rapid growth of speeds of various devices, data rates increase at significantly lower rates. A feature of most types of data is their redundancy. When storing and transmitting large volumes of information, redundancy plays a negative role, since it leads to an increase not only in the cost of storage, but also in the time of transmission of information. In this regard, compression algorithms are widely used to ensure the efficient storage, transmission of large volumes of information.

The object of the study is lossless compression methods of volume data.

The subject of the study is volume data and three-dimensional data.

Purpose: The purpose of the work is increase the efficiency of existing methods of data compression through the development of a modified method of compression of large volumes of data.

The scientific novelty is as follow.

1. A technique that differs from those known for the combination of three-dimensional wavelet transform and entropy coding, which allows data lossless data compression is proposed.
2. The modified method for compressing three-dimensional data, which leads to an increase in the peak signal-to-noise index and a decrease in the mean-square error has been earned.

.

The practical value of the results obtained in the work is that the proposed method for compression of information allows obtaining improved results in

comparison with existing methods by an average of 15% without deteriorating the quality.

Approbation.

- Xth Conference of Masters and Post-graduate students "Applied Mathematics and Computing", PMK-2018 (Kyiv, March 21-23, 2018);
- XI International Scientific-Technical Conference «Computer systems and networking technologies» (Kyiv, April 19-21, 2018);
- IIX Conference of Masters and Post-graduate students "Applied Mathematics and Computing", PMK-2016 (Kyiv, April 20-22, 2016);
- IX International Scientific-Technical Conference «Computer systems and networking technologies» (Kyiv, April 21-23, 2016).

Publications: Based on the materials of the research, 5 scientific works have been published, including 1 in the scientific professional publication, which is part of the science-metric databases, and 4 theses of the reports for the conference.

Structure and scope of work. The master's dissertation consists of introduction, three chapters and conclusions.

The introduction provides a general description of the work, evaluates the current state of the problem, raises the relevance of the direction of research, formulates the goals and objectives of the research, shows the scientific novelty of the results obtained and the practical value of the work, gives information about the approbation of the results and their implementation.

The first section deals with the description of the subject area of research and the justification of the topic of master's work.

The second section describes the basic algorithms of lossless compression.

The third section describes an improved lossless compression algorithm.

The conclusions show the results of the work.

The work is presented on 84 sheets, contains links to the list of used literary sources.

Keywords: algorithm, compression, three-dimensional data, medical images, lossless compression, images, entropy coding.

ЗМІСТ

СПИСОК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 16

ВСТУП 20

1. ОПИС ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕНЬ ТА ОБГРУНТУВАННЯ УЩІЛЬНЕННЯ ДАНИХ 22

1.1 Загальний аналіз методів ущільнення 22

1.2 Методи ущільнення з втратами 29

1.3 Методи ущільнення без втрат 33

Висновки до розділу 1 42

2. ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМИ УЩІЛЬНЕННЯ ВЕЛИКИХ ОБСЯГІВ ДАНИХ 43

2.1. Тривимірні дані 43

2.2. Ущільнення об’ємних даних 46

2.3. Методи ущільнення об’ємних даних 48

2.3.1. Ущільнені об’ємних даних методом кодування довжин серій 50

2.3.2. Ущільнення методом LZ 52

2.3.3. Ущільнення методом Хаффмана 55

2.3.4. Декореляція сигналу 57

2.4. Вейвлет-перетворення 60

Висновки до розділу 2 71

3. МОДИФІКОВАНИЙ СПОСІБ УЩІЛЬНЕННЯ ТРИВИМІРНИХ ДАНИХ 72

3.1. Загальний опис модифікованого способу ущільнення великих обсягів даних 72

3.1.1. Тривимірне вейвлет-перетворення 74

3.2. Детальний опис запропонованого вейвлет-перетворення тривимірних даних та наступні кроки модифікованого способу ущільнення 78

3.3. Оцінка результатів модифікованого способу ущільнення 84

3.3.1. Параметри оцінки модифікованого способу ущільнення 84

3.3.2. Результати оцінки модифікованого способу ущільнення 86

3.4. Порівняння модифікованого способу ущільнення з існуючими алгоритмами ущільнення 90

Висновки до розділу 3 92

ВИСНОВКИ 93

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 95

ДОДАТКИ

Додаток 1. Копії графічних матеріалів

Плакат 1. Процес ущільнення даних.

Плакат 2. Алгоритми ущільнення даних.

Плакат 3. Представлення тривимірних даних у медицині.

Плакат 4. Розроблений спосіб

Плакат 5. Схема вейвлет-перетворення тривимірних даних

Плакат 6. Процес роботи вейвлет-перетворення тривимірних даних

Додаток 2. Копії публікацій за темою роботи.

- Орлова М.М. Модифікований спосіб ущільнення великих обсягів даних / М.М. Орлова, Г.В. Щербакова // Інтернаука. – 2018. - № VIII (48).

- Орлова М.М. Аналіз алгоритмів ущільнення великих обсягів інформації без втрат // М.М. Орлова, Г.В. Щербакова // Прикладна математика та комп'ютинг. ПМК, 2018 : десята наук. Конф. Магістрантів та аспірантів, Київ, 21–23 березня 2018 р.: зб.тез доп./[редкол.: Дичка І.А. та ін.]. – К. : Просвіта, 2018., С. 107-111.

- Щербакова Г.В. Порівняння та аналіз алгоритмів ущільнення великих обсягів даних // Г.В. Щербакова // XI Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології». – 2018.

- Орлова М.М. Аналіз способів шифрування у комп'ютерних мережах// М.М. Орлова, Г.В. Щербакова // Прикладна математика та комп'ютинг. ПМК, 2016 : восьма наук. Конф. Магістрантів та аспірантів,

Київ, 21–23 березня 2016 р.: зб.тез доп./[редкол.: Дичка І.А. та ін.]. – К. : Просвіта, 2016., С. 107-111.

- Щербакова Г.В. Порівняння способів шифрування у комп’ютерних мережах// Г.В. Щербакова // IX Міжнародна науково-технічна конференція «Комп’ютерні системи та мережні технології». – 2016.

СПИСОК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

1-D	Одномірний простір
2-D	Двомірний простір.
3-D	Тримірний простір.
7-Zip	Файловий архіватор з високим ступенем ущільнення.
CCITT	The International Telegraph and Telephone Consultative Committee Консультативний комітет з міжнародного телеграфу та телефонного зв'язку.
CT	Computed Tomography scan Комп’ютерна томографія.
DCT	Discrete Cosine Transform Алгоритм дискретного косинусного перетворення.
DEFLATE	Варіація на LZ
DICOM	Digital Media and Communications in Medicine Розширення медичних зображень.
DWT	Discrete Wavelet Transform Дискретне вейвлет-перетворення
FFT	Fast Fourier Transform Перетворення Фур'є
GIF	Graphics Interchange Format Растровий графічний формат.
gzip	Утиліта ущільнення та відновлення файлів.
ISO	International Organization for Standardization Міжнародна організація зі стандартизації.
JFIF	Jpeg File Interchange Format Графічний формат.

JP3D	Стандарт для тривимірних даних.
JPEG	Joint Photographic Experts Group Об'єднана група експертів по фотографії.
JPEG	Joint Photographic Experts Group Алгоритм ущільнення зображень.
JPEG2000 чи JP2	Алгоритм ущільнення, який замість дискретного косинусного перетворення використовує вейвлет-перетворення.
JPG	Розширення файлів, які містять дані JPEG.
JPEG-LS	Стандарт ущільнення без втрат.
LZ	Lempel-Ziv – Алгоритм Лемпеля-Зіва Універсальний алгоритм ущільнення даних без втрат.
LZR	LZ-Renau Алгоритм ущільнення з сімейства LZ.
LZW	Lempel-Ziv-Welch Алгоритм Лемпеля-Зіва-Велча – Алгоритм ущільнення даних без втрат.
LZX	Алгоритм ущільнення з сімейства LZ.
MJPEG	Motion JPEG Неофіційна назва групи стандартів кодування відео, в яких кожен кадр цифрової відео послідовності незалежно закодований за алгоритмом JPEG.
MPEG	Moving Picture Experts Group Експертна група з питань рухомого зображення.
MRI	Magnetic resonance imaging Томографічний метод

	дослідження внутрішніх органів і тканин з використанням фізичного явища ядерного магнітного резонансу.
PDF	Portable Document Format Відкритий формат файлу, для представлення двовимірних документів у незалежному від пристрою виведення та роздільної здатності вигляді
PKZIP	Файловый архиватор, выпущенный компанией PKWARE.
PNG	Portable Network Graphics Растровий формат збереження графічної інформації, що використовує ущільнення без втрат.
PSNR	Peak Signal-to-Noise Ratio Співвідношення між максимумом можливого значення сигналу та потужністю шуму, що спотворює значення сигналу.
PET	Positron-emission tomography Позитрона емісійна томографія.
RLE	Run-Length Encoding Кодування довжин серій –алгоритм ущільнення даних, який оперує послідовностями, в яких один і той же символ зустрічається кілька разів поспіль.
SPECT	Single-photon emission computed tomography Комп'ютерну томографію з однокомпонентним випромінюванням.
TIFF	Tagged Image File Format Графічний формат представлення високоякісних зображень, які використовуються у поліграфічній галузі.

Zip	Формат ущільнення та архівації даних.
ВЧ	Висока частота
МРТ	Магнітно-резонансна томографія.
НЧ	Низька частота

ВСТУП

На сьогоднішній день розвиток обчислювальної техніки йде дуже швидкими темпами – постійно зростає частота і продуктивність процесорів, збільшуються обсяги пам'яті і прискорюється час доступу до неї. При такому бурхливому зростанні швидкостей різних пристроїв виникає проблема швидкості передачі даних. Це відбувається через те, що особливістю більшості типів даних є їх надлишковість.

При передачі та збереженні великих обсягів інформації надмірність відіграє негативну роль, оскільки вона не тільки призводить до збільшення часу передачі і функціональної надійності передачі інформації та її зберігання, а й до зростання сукупної вартості. В зв'язку з цим на сьогоднішній день для забезпечення ефективності передачі великих обсягів інформації та зберігання широко використовуються різноманітні способи ущільнення.

Але також при ущільнені даних виникає ситуація, коли частина даних втрачається. Інколи ці втрати не відіграють значної ролі, але бувають ситуації, коли втрата даних може стати критичною. Саме тому способи ущільнення без втрат користуються популярністю та постійно розвиваються.

Особливо такі способи важливі під час ущільнення великих обсягів даних, коли постає необхідність зменшити розмір оригінальних даних, але при цьому мати змогу відновити ущільнені дані без втрати.

Прикладом таких даних є тривимірні дані. До них відносяться медичні зображення. Ущільнення медичних зображень необхідно оскільки вони займають багато місця і це суттєво впливає на швидкість передачі.

Метою магістерської роботи є підвищення ефективності існуючих способів ущільнення даних за рахунок розробки модифікованого способу ущільнення великих обсягів даних

Розглядаються та аналізуються основні способи ущільнення даних. На основі аналітичного аналізу розроблено модифікований спосіб ущільнення великих обсягів даних. Розроблений спосіб ущільнення підходить для

зменшення об’ємів тривимірних даних, наприклад, медичних зображень. Проведено порівняння отриманих результатів з існуючими алгоритмами. Завдяки порівнянню доведено, що модифікований спосіб ущільнення має оптимальні показники. Що доводить наукову новизну даної магістерської роботи.

1. ОПИС ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕНЬ ТА ОБГРУНТУВАННЯ УЩІЛЬНЕННЯ ДАНИХ

1.1 Загальний аналіз методів ущільнення

Характерною особливістю більшості типів даних є їх надлишковість. Коли мова йде про зберігання та передачі даних у комп’ютерних мережах, то надмірність відіграє негативну роль, оскільки вона призводить до зростання вартості зберігання та передачі інформації. У зв'язку з цим, постійно виникає проблема зменшення надмірності або ущільнення даних.

Ущільнення - це спосіб кодування цифрових даних таким чином, щоб вони займали менший обсяг пам'яті і вимагали для передачі менше смуги пропускання мережі (рис. 1.1) [1].

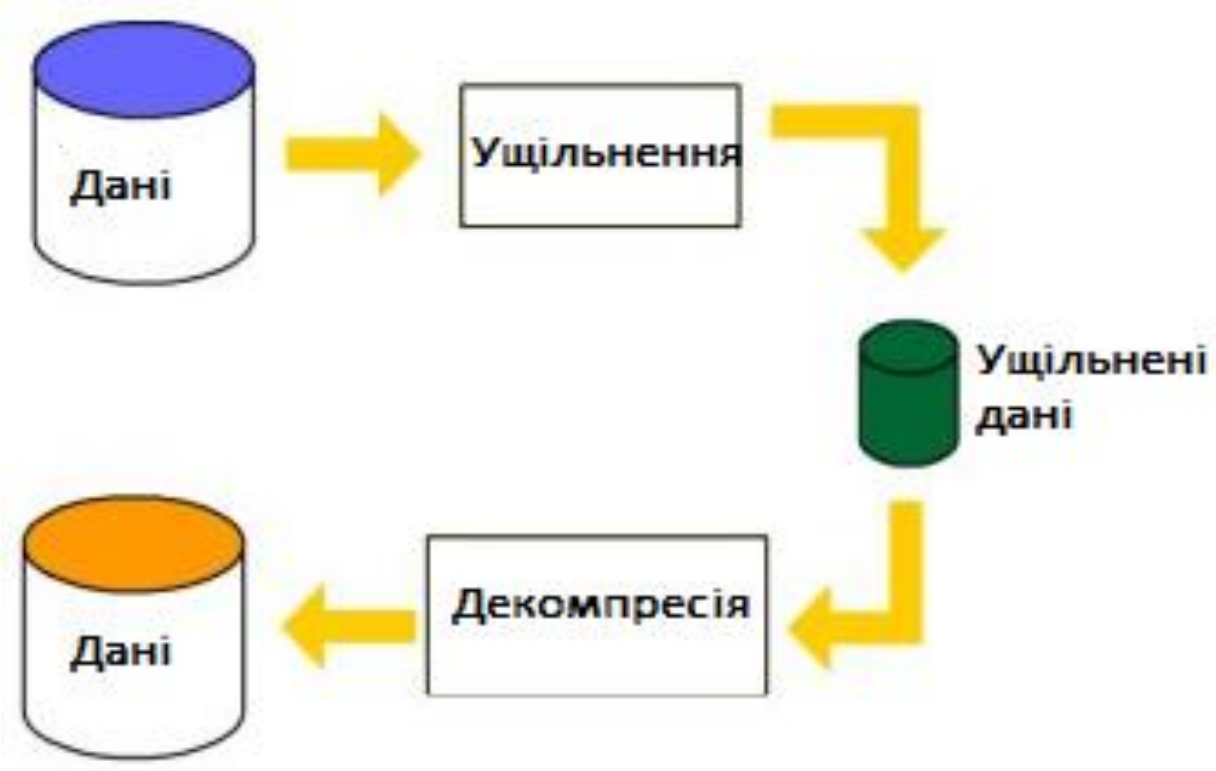


Рисунок 1.1 – Процес ущільнення даних

Ущільнення базується на усуненні надлишку інформації, яка міститься у вихідних даних. Наприклад, повторення в тексті фрагментів (наприклад, слів природної або машинної мови). Подібний надлишок зазвичай усувається заміною повторюваних послідовностей коротшим значенням (кодом). Інший

вид надлишковості пов'язаний з тим, що деякі значення в даних, які ущільняються, трапляються частіше інших, при цьому можна замінювати дані, що часто трапляються, коротшими кодами, а ті, що рідше – довшими (ймовірнісне ущільнення). Ущільнення даних, які не мають властивості надлишку (наприклад випадковий сигнал чи шум), неможливе. Також, зазвичай, неможливо стиснути зашифровану інформацію [1].

Ущільнення поділяється на таки види (рис. 1.2) [1].

1. Ущільнення без втрат — можливе відновлення вихідних даних без спотворень.
2. Ущільнення зі втратами — відновлення можливе з незначними спотвореннями.

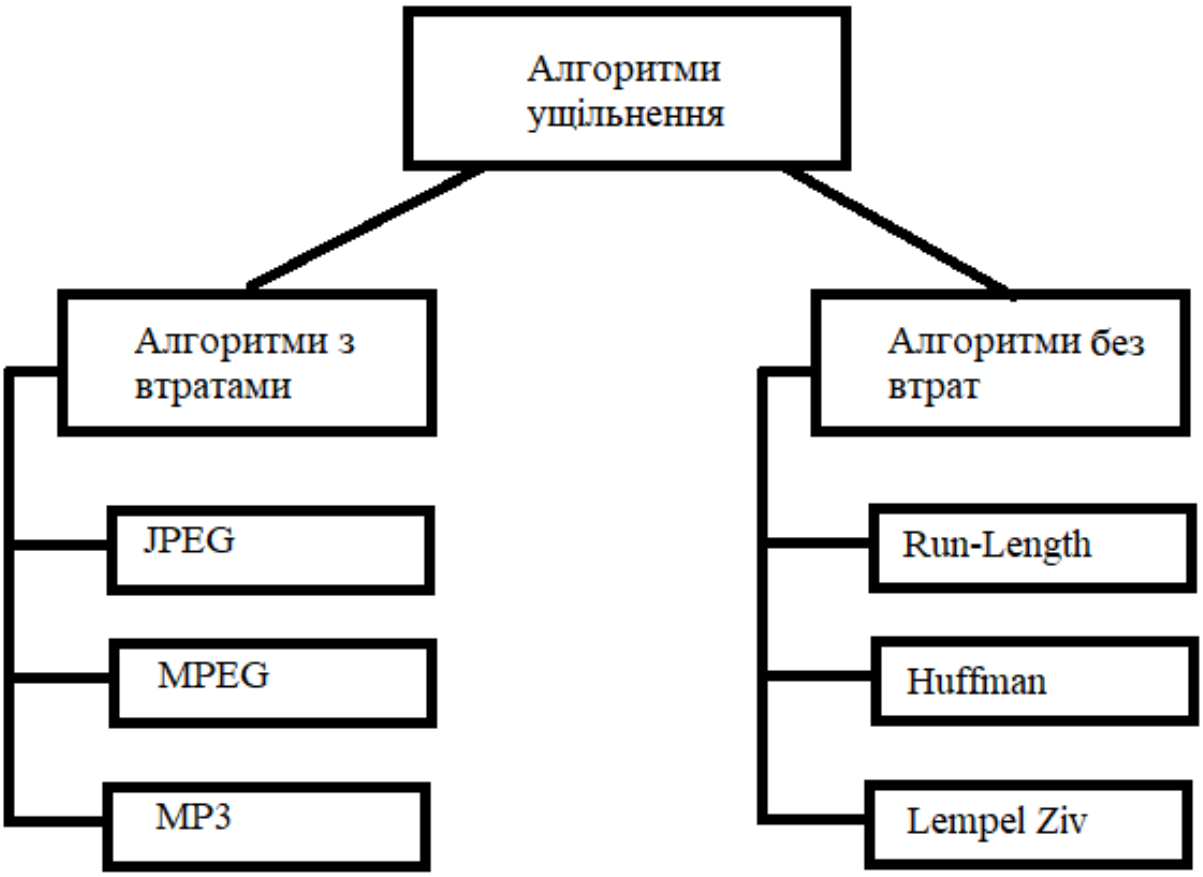


Рисунок 1.2 – Приклади алгоритмів

До тих пір поки смуга пропускання мережі буде дорогим ресурсом, а люди - нетерплячими, ущільнення даних не втратить актуальності. Інакше

кажучи, методи ущільнення перетворять дані - текст, графіку, аудіо або відео - в відновлюваний за допомогою комп'ютера формат, при цьому обсяг отриманої «інформації» становить 10-99% від початкового [1]. Дані займають при зберіганні менше місця і при передачі по мережі Інтернет вимагають меншої смуги пропускання. Крім того, багато методів дають змогу ущільнювати декілька файлів в один, який називають архівом.

Методи ущільнення без втрат стискають інформацію, не спотворюючи її і нічого не втрачаючи під час цього процесу. Після відновлення оригінальний документ ідентичний вихідному з точністю до біта. Методики з втратою даних дозволяють ще більше стиснути файл, але деякі дані при цьому втрачаються безповоротно.

Ущільнення з втратами виявляється ефективним при застосуванні до графічних зображень та оцифрованого голосу. За своєю природою ці оцифровані відображення аналогових явищ є не ідеальними з самого початку, тому ідея невідповідності введених та виведених даних є більш прийнятною.

Більшість методів ущільнення з втратами може бути налаштована на різні рівні якості, отримуючи більшу точність в обмін на менш ефективне ущільнення. До недавнього часу ущільнення з втратами здійснювалося, перш за все, за допомогою спеціального устаткування. Протягом останніх років потужні програми ущільнення з втратами були перенесені на настільні процесори, але навіть у цьому полі все ще переважають апаратні реалії.

Під час ущільнення з втратами виконується перетворення вхідного потоку даних, при якому вихідний потік, заснований на певному форматі інформації, являє собою досить схожий за зовнішніми характеристиками на вхідний потік об'єкт, однак відрізняється від нього обсягом. Ступінь подібності вхідного і вихідного потоків визначається ступенем відповідності деяких властивостей об'єкта (тобто ущільненої та неущільненої інформації, відповідно до деяким певним форматом даних), яку представляє даний потік інформації.

Такі підходи і алгоритми використовуються для ущільнення, наприклад, даних растрових графічних файлів з низьким ступенем повторюваності байтів в потоці. При такому підході використовується властивість структури формату графічного файлу і можливість представити графічну картинку приблизно схожу за якістю відображення (для сприйняття людським оком) декількома (а точніше n) способами. Тому, крім ступеня або величини стиснення, в таких алгоритмах виникає поняття якості.

Оскільки вихідне зображення в процесі стиснення змінюється, то під якістю можна розуміти ступінь відповідності вихідного і результуючого зображення, що оцінюється суб'єктивно, виходячи з формату інформації. Для графічних файлів така відповідність визначається візуально, хоча є і відповідні інтелектуальні алгоритми і програми. Алгоритми ущільнення з втратами неможливо застосовувати в областях, в яких необхідно мати точну відповідність інформаційної структури вхідного і вихідного потоків. Даний підхід реалізований в популярних форматах відео і фото інформації, відомих як JPEG і JFIF алгоритми і JPG і JIF формати файлів.

Ущільнення без втрат складається з тих методів, які гарантують створення точного дубліката потоку вхідних даних після циклу ущільнення/декомпресія. Це тип ущільнення, який використовується при зберіганні записів бази даних, електронних таблиць або файлів обробки текстів. У цих програмах втрата навіть одного біту може бути катастрофічною [2].

Ущільнення інформації без втрат завжди призводить до зниження обсягу вихідного потоку інформації без зміни його інформативності, тобто – без втрати інформаційної структури. Більш того, з вихідного потоку, за допомогою відновлюючого або декомпресивного алгоритму, можна отримати вхідний потік. Такий процес відновлення називається декомпресією або розпакуванням, і тільки після процесу розпакування дані придатні для обробки відповідно до їхнього внутрішнього формату.

В алгоритмах ущільнення без втрат кодування як процес можна розглядати зі статистичної точки зору, що ще більш корисно, не тільки для побудови алгоритмів ущільнення, а й для оцінки їх ефективності. Для всіх алгоритмів ущільнення без втрат існує поняття вартості кодування. Під вартістю кодування розуміється середня довжина кодового слова в бітах. Надмірність кодування дорівнює різниці між вартістю і ентропією кодування, а хороший алгоритм ущільнення завжди повинен мінімізувати надмірність (під ентропією інформації мається на увазі міра її невпорядкованості). Фундаментальна теорема Шеннона про кодування інформації говорить про те, що "вартість кодування завжди не менш ентропії джерела, хоча може бути як завгодно близька до неї". Тому, для будь-якого алгоритму, завжди є певний межа ступеня ущільнення, яка визначається ентропією вхідного потоку [2].

Різні алгоритми ущільнення можуть вимагати різної кількості ресурсів обчислювальної системи, на яких їх застосовують [2]:

1) оперативної пам'яті під проміжні дані;
2) постійної пам'яті під код програми і константи;
3) процесорного часу.

У цілому ці вимоги залежать від складності та «інтелектуальності» алгоритму. Загальна тенденція така: чим ефективніший і універсальніший алгоритм, тим більші вимоги до обчислювальних ресурсів він пред'являє. Тим не менш, у специфічних випадках прості і компактні алгоритми можуть працювати не гірше складних і універсальних. Системні вимоги визначають їх споживчі якості: чим менш вимогливий алгоритм, тим у простішій, а отже, компактній, надійній і дешевій системі він може працювати.

Так як алгоритми ущільнення і відновлення працюють в парі, має значення співвідношення системних вимог до них. Нерідко можна, ускладнивши один алгоритм, значно спростити інший. Таким чином, існують три наступні варіанти [2].

1. Алгоритм ущільнення вимагає більших обчислювальних ресурсів, ніж алгоритм відновлення. Таке співвідношення найпоширеніше та характерне для випадків, коли одноразово ущільнені дані будуть використовуватися багато разів. Як приклад можна навести цифрові аудіо- та відеопрогравачі.
2. Алгоритми ущільнення і відновлення вимагають приблизно рівних обчислювальних ресурсів. Найбільш прийнятний варіант для ліній зв'язку, коли стиснення і відновлення відбувається одноразово на двох її кінцях (наприклад, в цифровій телефонії).
3. Алгоритм ущільнення істотно менш вимогливий, ніж алгоритм відновлення. Така ситуація характерна для випадків, коли процедура ущільнення реалізується простим, часто портативним пристроєм, для якого обсяг доступних ресурсів дуже критичний, наприклад, космічний апарат або велика розподілена мережа датчиків. Це можуть бути також дані, розпакування яких потрібно в дуже малому відсотку випадків, наприклад запис камер відеоспостереження.

Можуть виникнути ситуація, коли необхідно ущільнити дані невідомого формату [2].

Існують два основних підходи для ущільнення даних невідомого формату.

1. На кожному кроці алгоритму стиснення черговий ущільнювальний символ або міститься у вихідний буфер стискального кодера як є (зі спеціальним прапором для позначення, що він не був стиснутий), або група з кількох стискуваних символів замінюється посиланням на відповідну групу з уже закодованих символів. Оскільки відновлення стислих таким чином даних виконується дуже швидко, такий підхід часто використовується для створення саморозпаковувальних програм.
2. Для кожної послідовності символів, яку ущільнення, одноразово або в кожний момент часу збирається статистика її появи в кодованих даних. На основі цієї статистики обчислюється ймовірність значення

чергового кодованого символу (або послідовності символів). Після цього застосовується той чи інший різновид ентропійного кодування, наприклад, арифметичне кодування або кодування Хаффмана, для представлення частіших послідовностей короткими кодовими словами, а рідкіших — довшими.

Якщо очевидно, що необхідне ущільнення, то потрібно вирішити, який тип технології слід використовувати. Навіть якщо це не зрозуміло з першого погляду, ущільнення може призвести до деяких переваг і може запропонувати додаткові функціональні можливості через збережені ресурси. Під час вибору конкретної технології ущільнення є важливими наступні критерії [3]:

1) Вимірювання даних: 1-D, 2-D, 3-D.
2) Ущільнення з втратами чи без втрат.
3) Необхідна якість.
4) Складність, швидкість, затримка алгоритму.
5) Апаратне або програмне рішення: швидкість і ціна.
6) Стійкість до помилок.
7) Який об’єм даних.
8) Необхідні стандарти: створюється закрита система, яка не призначена для взаємодії з іншими системами чи необхідно обмінюватися даними по багатьох системах.
9) Багаторазове кодування/декодування: повторне застосування стиснення з втратами, наприклад у редакції відео.
10) Адаптивність: очікуються дані з різноманітними властивостями чи можна попередньо адаптуватися до певних властивостей.
11) Перекодування: чи можна змінювати типи даних (наприклад, MJPEG на MPEG).

1.2 Методи ущільнення з втратами

До недавнього часу ущільнення з втратами виконувалося переважно на спеціальному апаратному забезпеченні. Поява недорогих цифрових сигнальних процесорів (DSP) почала рух ущільнення з втратами від плати на стаціонарні комп’ютери [4].

Існують наступні методи ущільнення з втратами.

1. Зниження глибини кольору.
2. Метод головних компонент.
3. Фрактальне ущільнення.
4. JPEG-LS.
5. ДИКМ (Диференціально-імпульсивна кодова модуляція).
6. Ієрархічна сіточна інтерполяція.
7. CALIC.
8. JPEG
9. Диференційне ущільнення.

Ущільнення з втратами принципово відрізняється від ущільнення без втрат в наступному відношенні: він допускає невелику втрату даних для полегшення ущільнення. Ущільнення з втратами, як правило, застосовується для аналогових даних, що зберігаються в цифровому режимі, причому в основному застосовується для графічних та звукових файлів.

Є дві основні схеми роботи методів ущільнення з втратми.

1. Перший прохід над даними виконує функцію обробки сигналів високого рівня. Це полягає в перетворенні даних у частотну область, використовуючи алгоритми, подібні до відомого швидкого перетворення Фур'є (FFT).
2. Після того як дані були перетворені, він «згладжує», округлюючи високі та низькі точки. Тут відбувається втрата сигналу. Нарешті, точки частоти стискуються за допомогою звичайних методів без втрат.

Функція згладжування, яка працює на даних частотної області, як правило, має "якісний фактор", який вбудований в неї що визначає, наскільки

відбувається згладжування. Чим більше дані «загладжуються», тим більшою буде втрата сигналу та більше ущільнення [4].

У малих системах світу більша кількість робіт виконується при ущільнені графічного зображення як для нерухомих, так і для рухомих зображень. Міжнародна організація зі стандартизації (ISO) та Консультативний комітет з міжнародного телеграфу та телефонного зв'язку (CCITT) об'єднали два комітети: Об'єднана група експертів по фотографії (JPEG) та Експертна група з питань рухомого зображення (MPEG).

Об'єднана група експертів з фотографії опублікувала стандарт ущільнення, зараз багато виробників постачають апаратне і програмне забезпечення сумісне з JPEG. Експертна група з питань рухомого зображення завершили стандарт ущільнення початкового зображення, що рухається, і завершує другий стандарт – MPEG-II [4].

Стандарт JPEG використовує алгоритм дискретного косинусного перетворення (DCT) для перетворення графічного зображення до частотній області. Алгоритм дискретного косинусного перетворення використовувався для графічних перетворень протягом багатьох років, тому його ефективні реалізації є в загальному доступі. JPEG вказує коефіцієнт якості від 0 до 100, і це дозволяє компресору визначати, який фактор потрібно вибрати.

Використання алгоритму JPEG на зображеннях може призвести до низьких коефіцієнтів ущільнення. З невеликою кількістю чи без погіршення, коефіцієнти стиснення 90-95 відсотків є звичайними. Приймаючи незначне погіршення, співвідношення становить 98-99% [4].

Програмна реалізація алгоритмів JPEG і MPEG все ще намагається досягти продуктивності в режимі реального часу. Більшість мультимедійних програм для розробки, які використовують цей тип ущільнення, як і раніше залежить від використання плати співпроцесора, щоб зробити ущільнення впродовж прийнятної кількості часу.

Ущільнення інформації з втратами використовується в основному для зменшення розміру трьох видів даних [4]:

1) Графіка.
2) Звук.
3) Відеоінформація.

Загалом, ущільнення з втратами використовується, коли втрата інформації не буду суттєвою.

Основна перевага алгоритмів ущільнення з втратами - це простота їх реалізації. Крім того, такі алгоритми забезпечують дуже високу ступінь ущільнення, при цьому зберігають необхідну для відновлення кількість інформації. Використання подібних алгоритмів, як правило, вигідно для ущільнення аналогових величин, наприклад, звуків або зображень. У подібних випадках кінцевий результат, найвірогідніше, буде дуже відрізнятися від оригіналу. Однак людина, яка не забезпечена спеціальним обладнанням, цю різницю може зовсім не помітити. Приклад ущільнення з втратами зображено на рис. 1.3.

Перевага методів стиснення з втратами над методами ущільнення без втрат полягає в тому, що перші уможливлюють велику ступінь стиснення, продовжуючи задовольняти поставленим вимогам, а саме - спотворення повинні бути в допустимих межах чутливості людських органів фізичних почуттів [4].

Методи ущільнення з втратами часто використовуються для ущільнення аналогових даних - найчастіше звуку або зображень.

У таких випадках розпакований файл може дуже сильно відрізнятися від оригіналу на рівні порівняння «біт в біт», але практично не відрізняється для людини «на слух» і «на око» в більшості застосувань.

Багато методів ущільнення з втратами фокусуються на фізичних особливостях органів почуттів людини. Психоакустична модель визначає те, як сильно звук може бути ущільнений без погіршення якості звуку, яке сприймає людина. Недоліки, завдані ущільнення з втратами, які помітні для людського вуха або очі, відомі як артефакти ущільнення.

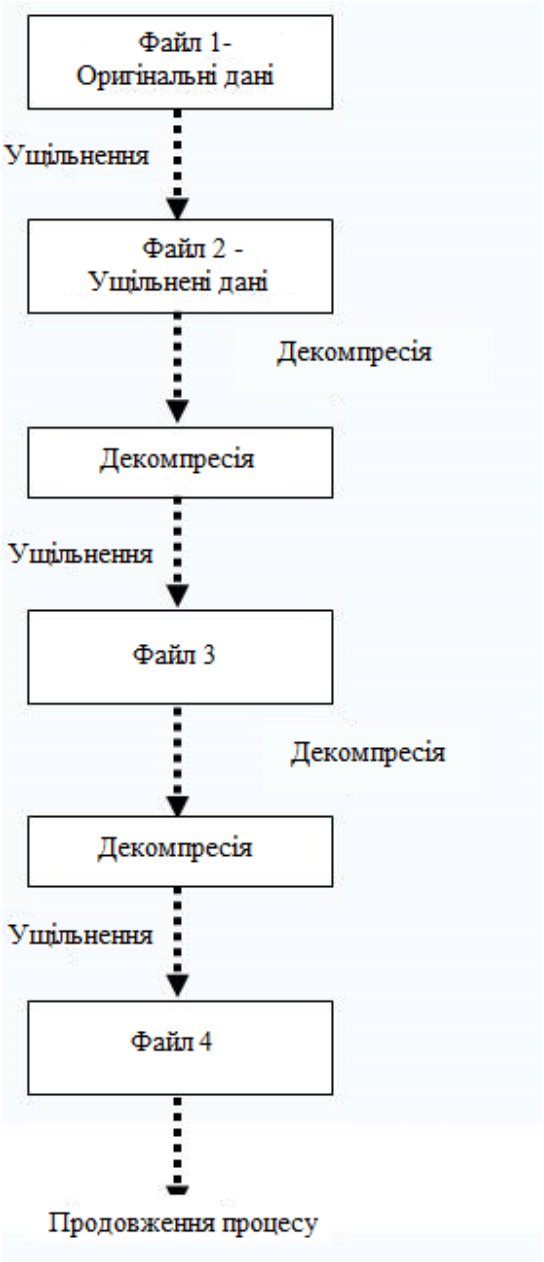


Рисунок. 1.3 – Приклад ущільнення з втратами

Фотографії, записані в форматі JPEG, можуть бути прийняті судом як докази незважаючи на те, що зображення було ущільнене з втратами.

Однак методи стиснення з втратами мають і ряд недоліків. Перший полягає в тому, що ущільнення інформації з втратами застосовна не для всіх випадків аналізу графічної інформації. Наприклад, якщо в результаті ущільнення зображення на обличчі зміниться форма родимки (але обличчя при цьому залишиться незмінним), то ця фотографія виявиться цілком прийнятною, щоб послати її поштою знайомим, однак якщо пересилається

фотознімок легенів на медекспертизу для аналізу форми затемнення - це вже зовсім інша справа. Крім того, в разі машинних методів аналізу графічної інформації результати ущільнення з втратою (непомітні для очей) можуть бути «помітні» для машинного аналізатора [4].

Друга причина полягає в тому, що повторне ущільнення і декомпресія з втратами призводять до ефекту накопичення похибок. Якщо говорити про ступінь застосовності формату JPEG, то, очевидно, він корисний там, де важливим є великий коефіцієнт ущільнення при збереженні вихідної колірної глибини. Саме ця властивість зумовила широке застосування даного формату в поданні графічної інформації в Інтернеті, де швидкість відображення файлу (його розмір) має першорядне значення. Негативна властивість формату JPEG - погіршення якості зображення, що робить практично неможливим його застосування в поліграфії, де цей параметр є визначальним [4].

1.3 Методи ущільнення без втрат

Алгоритми стиснення без втрат застосовується для зменшення розміру даних в тому випадку, коли важливо відновити дані в точності такими, які вони були до стиснення.

На поточний час існує велика кількість алгоритмів стиснення без втрат, які умовно можна розділити на дві великі групи (рис. 1.4) [4].

1. Потокові і словникові алгоритми. До цієї групи належать наступні алгоритми:
    1.1. Алгоритм RLE (Run-Length Encoding),
    1.2. Алгоритм LZ.
    1.3. Алгоритм LZW.
    1.4. Алгоритм LZR (LZ-Renau).
    1.5. Алгоритм DEFLATE.

Особливістю всіх алгоритмів цієї групи є те, що при кодуванні використовується не інформація про частоти символів в повідомленні, а інформація про послідовності, що зустрічалися раніше.

2. Алгоритми статистичного (ентропійного) стиснення. Ця група алгоритмів стискає інформацію, використовуючи нерівномірність частот, з якими різні символи зустрічаються в повідомленні. До алгоритмів цієї групи відносяться алгоритми арифметичного і префіксного кодування.

2.1. Алгоритм Шеннона-Фанно.

2.2. Алгоритм Хаффмана.

3. В окрему групу можна виділити алгоритми перетворення інформації. Алгоритми цієї групи не виробляють безпосереднього ущільнення інформації, але їх застосування значно спрощує подальше ущільнення з використанням поточних, словникових та ентропійних алгоритмів [4].

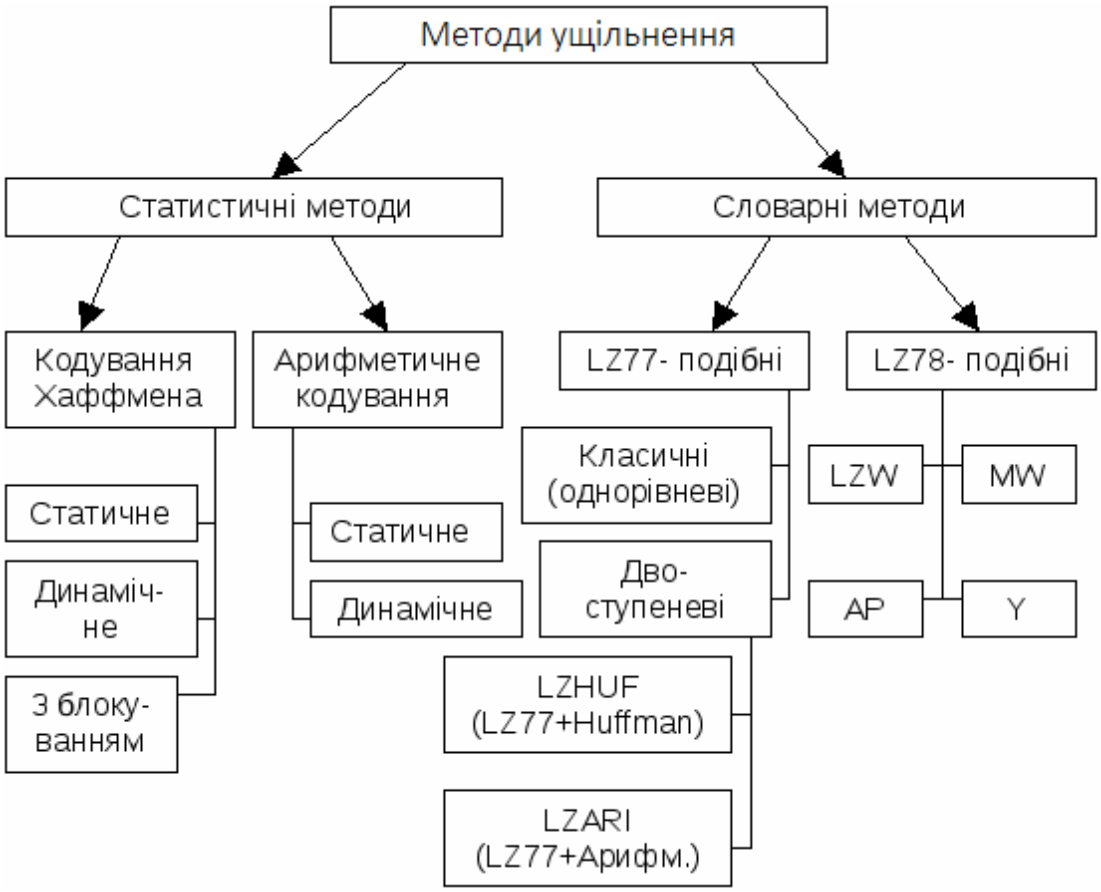


Рисунок 1.4 – Алгоритми ущільнення без втрат

Теоретичний фон ущільнення забезпечується теорією інформації та теорією бітової швидкості. Ці області були створені Клодом Шенноном, який опублікував основні роботи з цієї теми в кінці 1940-х та початку 1950-х років [4].

Багато систем ущільнення даних без втрат можна розглядати в термінах чотириступеневої моделі.

Кодування довжин серій

Кодування довжин серій – це один з найпростіших і розповсюджених алгоритмів стиснення даних. У цьому алгоритмі послідовність символів, що повторюються замінюється символом і кількістю його повторів (рис. 1.5).

Даний метод ущільнення ефективно застосовувати для даних, що містять велику кількість серій, наприклад, для простих графічних зображень, таких як іконки та графічні малюнки. Однак він не підходить для зображень з плавним переходом тонів, таких як фотографії [4].

Також цей метод ущільнення підходить для зменшення розміру звукових даних, які мають довгі послідовні серії байт. Але спочатку до них необхідно застосувати дельта-кодування.

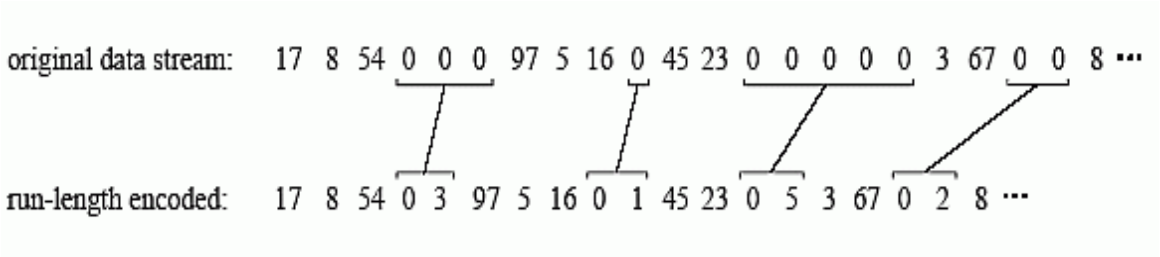


Рисунок 1.5 – Приклад кодування довжин серій

Методи ущільнення Lempel-Ziv

Методи ущільнення Lempel-Ziv (LZ) є одними з найбільш популярних алгоритмів ущільнення без втрат (рис. 1.6).

DEFLATE - це варіація на LZ, яка оптимізована для збільшення швидкості декомпресії та коефіцієнта ущільнення, хоча ущільнення може бути повільним.

DEFLATE використовується для наступних видів даних:

1) PKZIP.
2) gzip.
3) PNG.

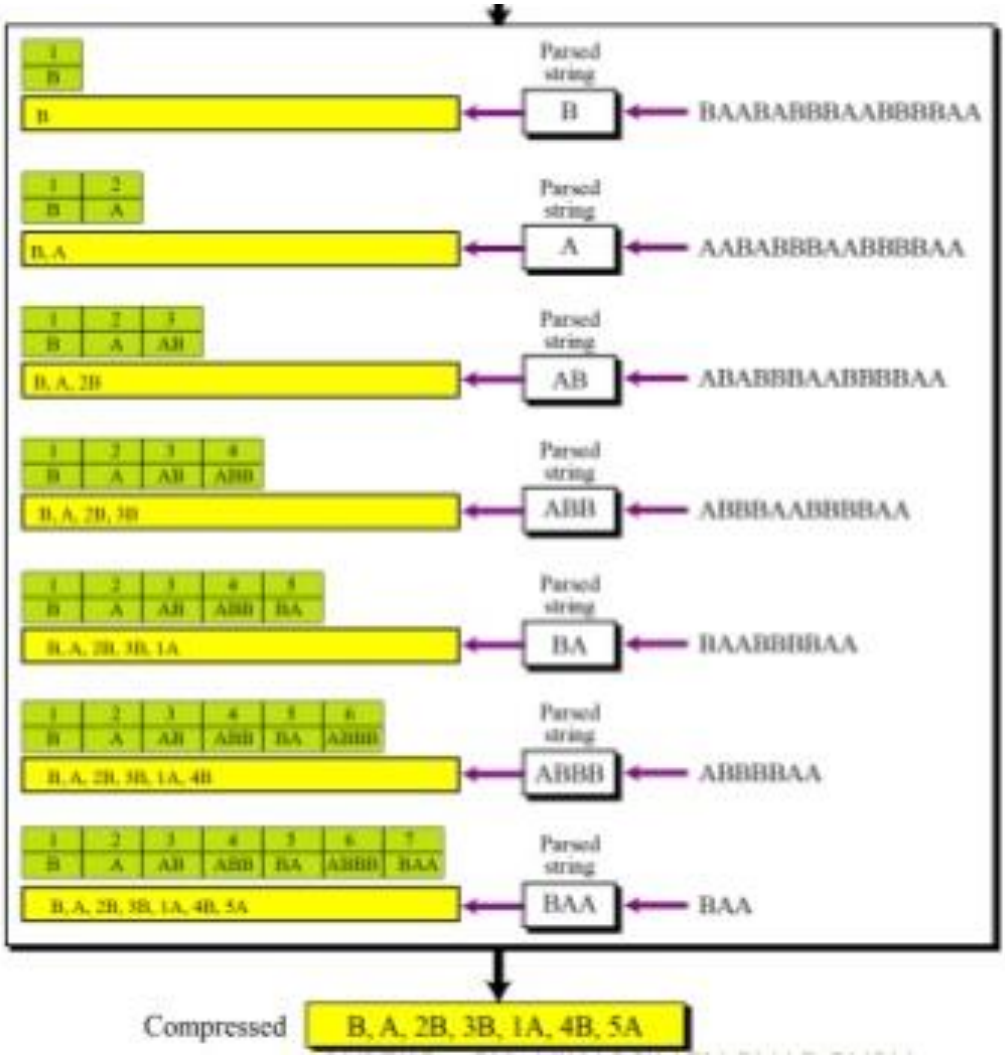


Рисунок 1.6 – Приклад алгоритму Lempel-Ziv

LZW (Lempel-Ziv-Welch) запатентовано Unisys до червня 2003 року, і використовується в зображеннях GIF. Також варто відзначити методи LZR (LZ-Renau), які служать основою методу Zip [4].

Методи LZ використовують модель ущільнення на основі таблиці, де записи таблиць замінюються повторними рядками даних. Для більшості методів LZ ця таблиця генерується динамічним методом з попередніх даних на вході.

Сама таблиця часто кодується алгоритмом Хаффманом (наприклад, SHRI, LZX). Два поточних LZX використовуються у популярному 7-Zip архіваторії [5].

Найкращі алгоритми ущільнення використовують імовірнісні моделі арифметичного кодування. Арифметичне кодування, винайдене Джормою Ріссаненом і перетворене на практичний метод завдяки Віттену, Нілу і Клірі, досягає оптимальних показників ущільнення, як найбільш відомий алгоритм Хаффмана, і особливо добре підходить для адаптивних задач ущільнення даних, де прогнози сильно контекстнозалежні.

Алгоритм Шеннона-Фано

Алгоритм Шеннона-Фано – один з перших розроблених алгоритмів ущільнення. Цей алгоритм був розроблений Клодом Елвудом Шенноном і Робертом Фано в 1949 році. Цей алгоритм замінює всі символи на двійковий код, довжина якого визначається частотою виникнення символу (Adhitama, 2009) [4].

Приклад алгоритму Шеннона-Фано зображено на рис. 1.7.

Основні етапи.

1. Символи первинного алфавіту m_1 виписують в порядку зменшення ймовірностей.
2. Символи отриманого алфавіту ділять на дві частини, сумарні ймовірності символів яких максимально близькі один одному.
3. У префіксному коді для першої частини алфавіту присвоюється двійкова цифра «0», другої частини — «1».
4. Отримані частини рекурсивно діляться і їх частинам призначаються відповідні двійкові цифри в префіксному коді.

Коли розмір підалфавіту стає рівним нулю або одиниці, то наступне подовження префіксних коду для відповідних йому символів первинного алфавіту не відбувається, таким чином, алгоритм привласнює різним символам префіксні коди різної довжини.

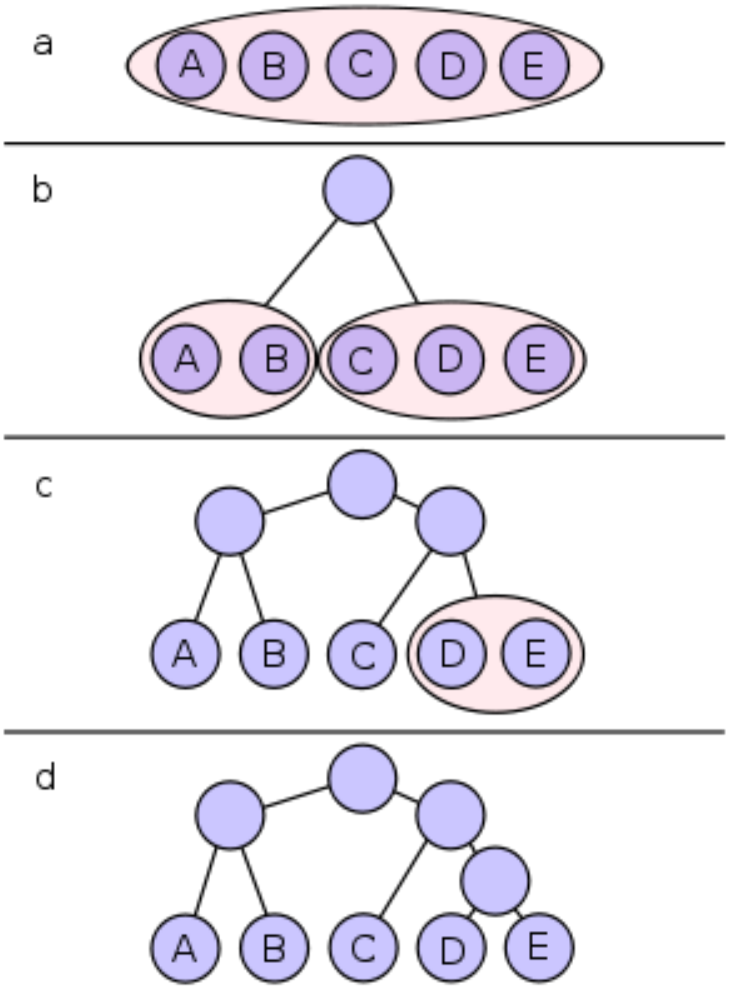


Рисунок 1.7 – Приклад алгоритму Шеннона-Фано

На кроці ділення алфавіту існує неоднозначність, так як різниця сумарних ймовірностей p_0-p_1 може бути однакова для двох варіантів поділу (враховуючи, що всі символи первинного алфавіту мають ймовірність більше нуля) [6].

Алгоритм Хаффмана

Класичний алгоритм Хаффмана на вході отримує таблицю частот з якими зустрічаються символи у повідомленні. Далі на підставі цієї таблиці будується дерево кодування Хаффмана (Н-дерево) [7].

1. Символи вхідного алфавіту утворюють список вільних вузлів. Кожен лист має вагу, яка може бути рівною або ймовірності, або кількості входжень символу у стиснене повідомлення.
2. Вибираються два вільних вузли дерева з найменшими вагами.

3. Створюється їхній батьківський вузол з вагою, рівною їх сумарній вазі.

4. Вузол-батько додається в список вільних вузлів, а два його нащадки видаляються з цього списку.

5. Одній дузі, котра виходить з вузла батька, ставиться у відповідність біт 1, інший — біт 0.

6. Кроки, починаючи з другого, повторюються доти, поки в списку вільних вузлів не залишиться тільки один вільний вузол. Він і буде вважатися коренем дерева.

Припустимо, є наступна таблиця частот (таблиця 1.1).

Цей процес можна представити як побудову дерева, коріння якого – символ з сумою ймовірностей об'єднаних символів, що вийшов при об'єднанні символів з останнього кроку, його n_0 нащадків - символи з попереднього кроку та інше [7].

Щоб визначити код для кожного з символів, що входять в повідомлення, ми повинні пройти шлях від листа дерева, що відповідає поточному символу, до його кореня, накопичуючи біти при переміщенні по гілках дерева (перша гілка в дорозі відповідає молодшому біту). Отримана таким чином послідовність бітів є кодом даного символу, записаним в зворотному порядку.

Таблиця 1.1. – Таблиця частот

Частота	Символ
А	15
Б	7
В	6
Г	6
Д	5

У таблиці 1.2. наведено таблицю символів кодів Хаффмана.

Таблиця 1.2. – Таблиця символів кодів

Частота	Символ
А	000
Б	100
В	101
Г	110
Д	111

Оскільки жоден з отриманих кодів не є префіксом іншого, вони можуть бути однозначно декодовані при читанні їх з потоку. Крім того, найбільш частий символ повідомлення А закодований найменшою кількістю біт, а найбільш рідкісний символ Д – найбільшим [7].

При цьому загальна довжина повідомлення, що складається з наведених у таблиці символів, складе 87 біт (в середньому 2,2308 біта на символ). При використанні рівномірного кодування загальна довжина повідомлення склала б 117 біт (рівно 3 біта на символ). Зауважимо, що ентропія джерела, незалежним чином породжує символи з зазначеними частотами, становить приблизно 2,1858 біта на символ, тобто надмірність побудованого для такого джерела коду Хаффмана, що розуміється як відмінність середнього числа біт на символ від ентропії, становить менше 0,05 біт на символ.

Побудування дерева для даного прикладу зображено на рис. 1.8.

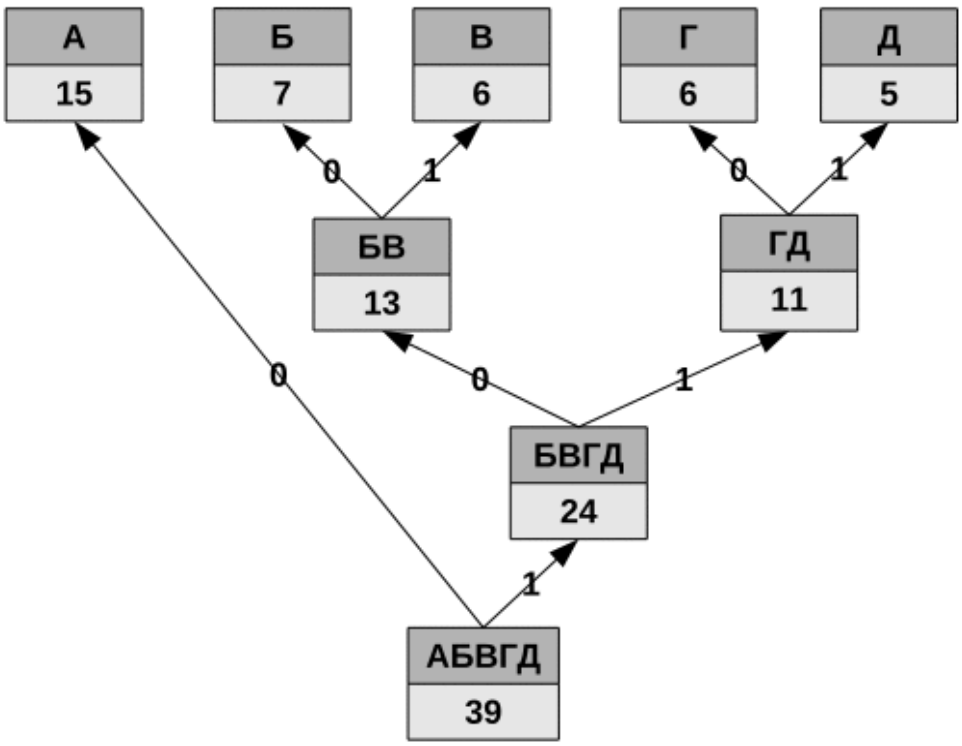
Класичний алгоритм Хаффмана має ряд істотних недоліків.

1. Для відновлення вмісту стиснутого повідомлення декодер повинен знати таблицю частот, якою користувався кодер. Отже, довжина повідомлення, що ущільнено, збільшується на довжину

таблиці частот, яка повинна надсилатися попереду даних, що може звести нанівець всі зусилля з ущільнення повідомлення. Крім того, необхідність наявності повної частотної статистики перед початком кодування вимагає двох проходів по повідомленню: одного для побудови моделі повідомлення (таблиці частот і Н-дерева), іншого для вже кодування.

2. Надмірність кодування звертається в нуль лише в тих випадках, коли ймовірності кодованих символів є зворотними ступенями числа 2.

3. Для джерела з ентропією, що не перевищує 1 (наприклад, для двійкового джерела), безпосереднє застосування коду Хаффмана не має сенсу.



Итого:

А	Б	В	Г	Д
0	100	101	110	111

Рисунок 1.8 – Побудова дерева

Висновки до розділу 1

Розглянуто та проаналізовано основні існуючі алгоритми ущільнення даних. Розглянуто процес ущільнення різними варіантами алгоритмів, показані їх переваги та недоліки.

Проведене дослідження існуючих алгоритмів ущільнення показало, що для того, щоб блок даних, який зберігається, займав менший обсяг, необхідно елементи, які часто використовуються, заміняти короткими кодами, а ті, які рідко використовуються – довгими кодами.

Наведені алгоритми використовують для одномірних даних. Вони не підходять для ущільнення тривимірних (3-D) даних. Оскільки для таких даних (особливо для медичних 3-D зображень) важливо, щоб відновлені після ущільнення дані були ідентичні оригінальним, то для їх ущільнення необхідно використовувати алгоритми без втрат.

На сьогоднішній день невирішеним питанні ущільнення тривимірних даних. Показано, що всі відомі алгоритми ущільнення на сьогоднішній день використовуються тільки для одномірних даних і не підходять для ущільнення тривимірних даних, оскільки такі дані представлені у трьох площинах. Особливо важливо, щоб тривимірні дані були ущільнені без втрати якості.

2. ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМИ УЩІЛЬНЕННЯ ВЕЛИКИХ ОБСЯГІВ ДАНИХ

2.1. Тривимірні дані

Метою даної роботи є розробка модифікованого способу ущільнення великих обсягів даних. Під великими обсягами даних маються на увазі тривимірні дані.

Тривимірні дані широко використовуються в науковому світі. Для медичного застосування, а також для дистанційного зондування і моделювання фізичних моделей часто потрібно об'ємне уявлення 3D, що призводить до складних наборів даних. Приклад тривимірних даних у медичному застосуванні зображено на рис. 2.1 та рис. 2.2.

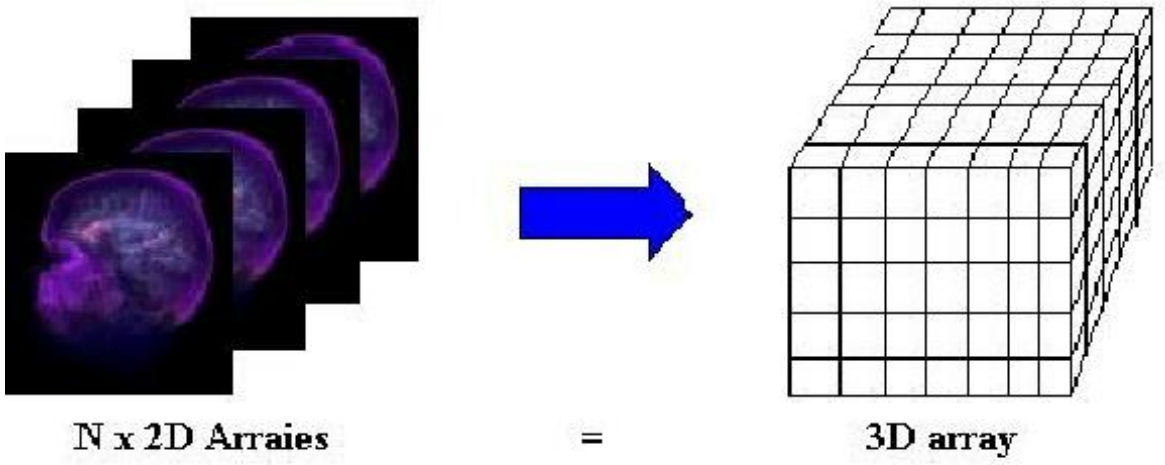


Рисунок 2.1 – Представлення об’ємних у медицині

Така складність охоплює методи представлення, обробки і ущільнення, що використовуються в управлінні цифровими об'ємними даними. Більш того, ці операції, як правило, є обов'язковими для правильної інтерпретації даних і їх зручного зберігання. Хоча стандартизована структура для обробки і зберігання об'ємних даних в даний час не використовується, але в науковому співтоваристві витрачатися багато зусиль на їх визначення і прийнятність.

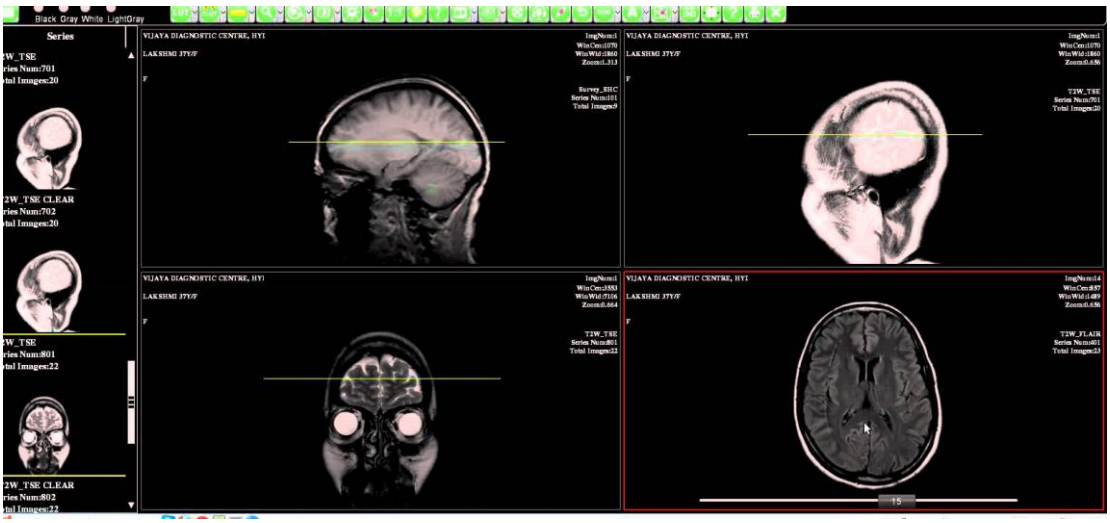


Рисунок 2.2 – Тривимірні медичні зображення

На додаток до досліджень, проведеним університетами і високотехнологічними компаніями, для визначення такого стандарту працюють кілька організацій. Наприклад, Об'єднана група експертів по фотографії (ISO / IEC SC29 WG01) недавно запустила діяльність JPEG2000 Part10, пов'язану з кодуванням тривимірних даних і розширенням JPEG2000 від плоских до об'ємних зображень (JP3D). Аналогічним чином, комітет по стандартизації Digital Media and Communications in Medicine (DICOM) працює над впровадженням і інтеграцією багатокадрових і тривимірних методів стиснення в медичній сфері [8].

Об'ємні дані зазвичай визначається тривимірною матрицею цілих або дійсними значень, що відображають локальну інтенсивність сигналу, що представляє інтерес (рис. 2.3). Залежно від застосування, це може характеризувати енергію для переданої, відбитої або випромінюваної радіації, місцевого тиску, щільності, вологості або поточної швидкості тощо.

Як і в випадку двомірних зображень, сигнал повинен бути просторово відібраний у багато паралелепіпедних блоків, а його діапазон піддається квантуванню для отримання об'ємного цифрового зображення. Основний блок називають вокселем, 3D-аналогом 2D пікселя.

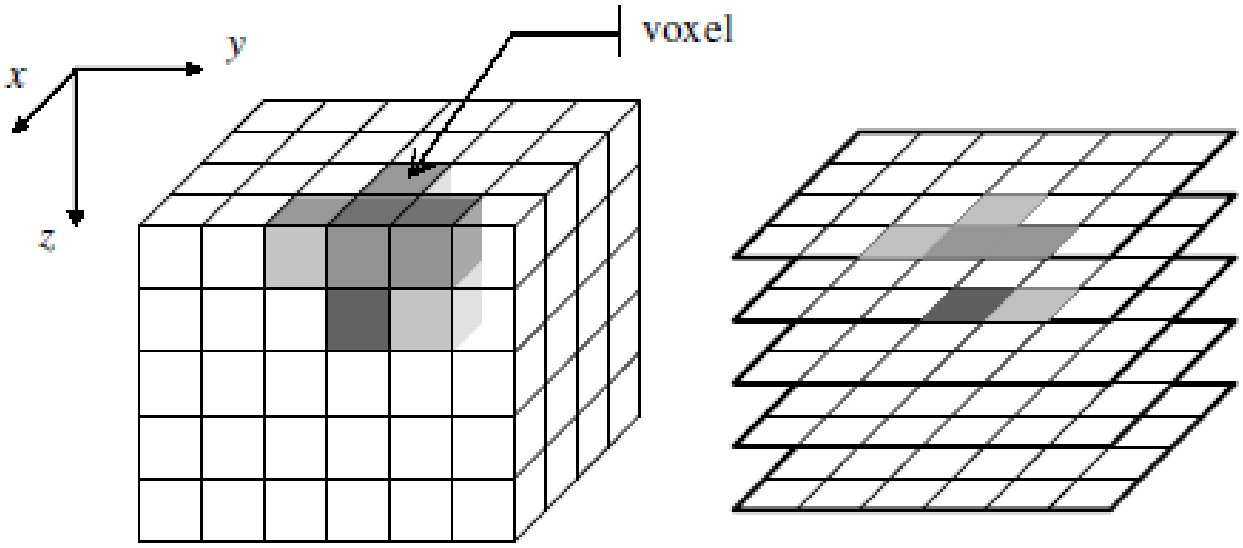


Рисунок 2.3 – 3D та стек представлення об'ємних даних

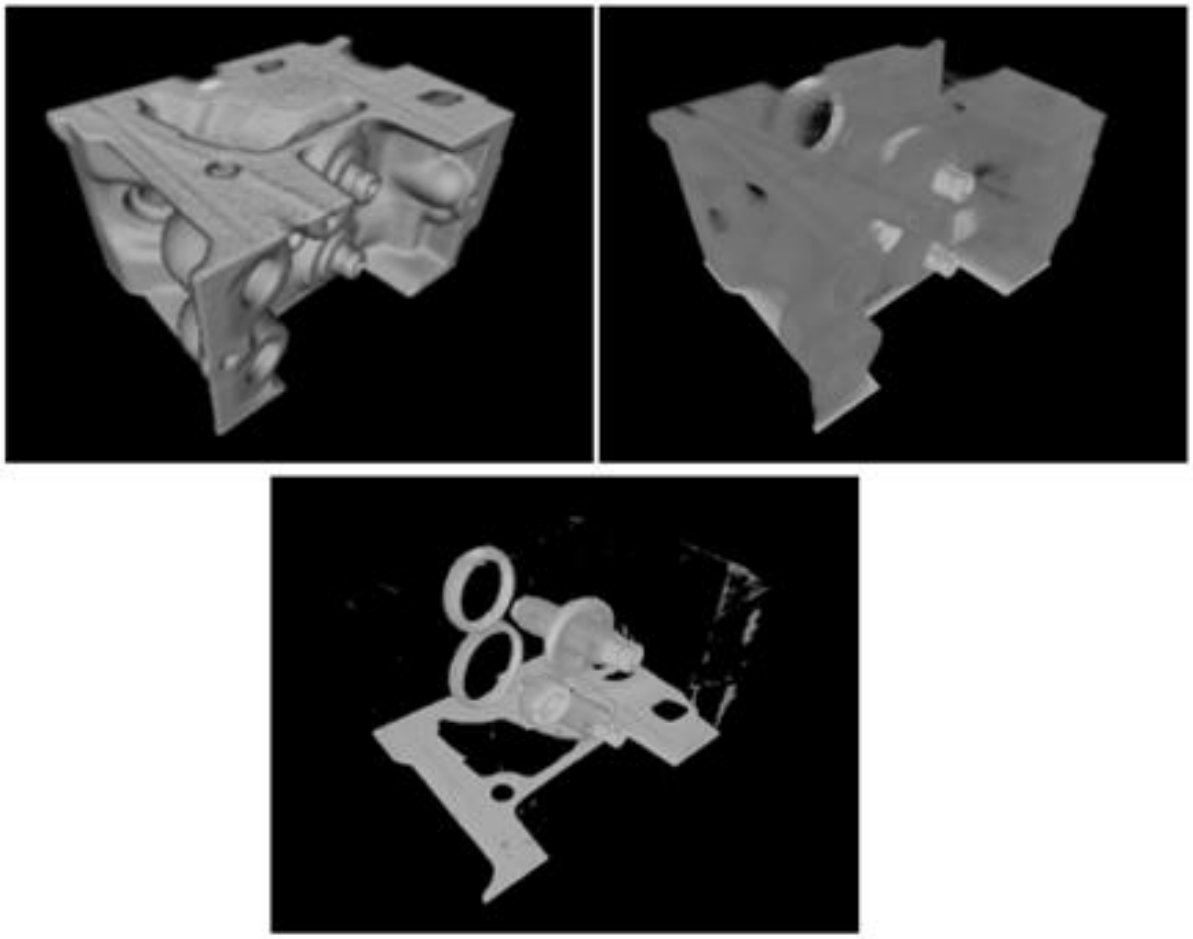


Рисунок 2.4 – Об'ємне відтворення CT-сканування двигуна, отримане шляхом зміни скалярної функції відображення непрозорості, щоб показати всю об'ємну інформацію

Біт глибини може варіюватися від 8 до 32 біт залежно від програми. У той час як 12-бітна глибина є загально використовуваною, 32 бітна глибина з плаваючою комою використовується для наукових моделей фізичних наборів даних. Тривимірне відтворення CT-сканування (комп'ютерна томографія) двигуна показано на рис. 2.3. Змінюючи значення скалярних значень непрозорості, можна повністю ілюструвати вміст зображення. Об'ємне зображення також може розглядатися як збірка плоских секцій.

2.2. Ущільнення об'ємних даних

Основною метою ущільнення даних є спрощення управління інформацією, яка потребує надмірного обсягу зберігання даних з її природним представленням. Теорія ущільнення даних та зображень походить від понять статистичної та тимчасової надмірності та невідповідності. Фактично, експлуатація раніше наведених властивостей дозволяє визначити і реалізувати всі кодування.

Ущільнення об'ємних даних є навіть більш актуальним, ніж у звичайних зображення, оскільки вони вимагають великих обсягів зберігання. Наприклад, середній вихідний набір CT-даних, виконаний з 100 площинних розділів з роздільною здатністю 512 × 512 пікселів та 12 бітною глибиною, потребує приблизно 50 Мб для зберігання. Оскільки типовий радіологічний відділ може щоденно робити десятки таких іспитів, легко уявити, що будь-яка ємність може бути легко заповнена за відносно короткий час.

Хоча об'ємні зображенні можуть розглядатися як розширення традиційних зображень, методологія кодування таких даних не може бути тією ж самою. Фактично, в силу особливості таких образів та їх прийняття в діагностиці, плануванні лікування та наукових програмах, особлива увага повинна приділятися при проектуванні нової схеми ущільнення.

Об'ємні дані мають важливі структурні особливості, які слід враховувати при визначенні нового способу ущільнення. Наприклад,

томографічні пристрої генерують збірку плоских секцій, які, як правило, не є ізотропними, тобто роздільна здатність вздовж напрямків внутрішніх плоскостей відрізняється ніж між зрізами. Типовим прикладом є комп'ютерна томографія, де площина роздільна здатність, як правило, тонша, ніж 1 мм, а роздільна здатність між різцями може становити кілька міліметрів. У цьому випадку алгоритм ущільнення не зможе виявити та використовувати подібну статистичну надмірність вздовж різних напрямків. На рис. 2.5 показано приклад МРТ-сканування головного мозку, де роздільна здатність вздовж осі міжрізних частин майже в шість разів перевищує площинні напрямки; сагітальні та корональні види чудово показують наслідки недостатньої вибірки.

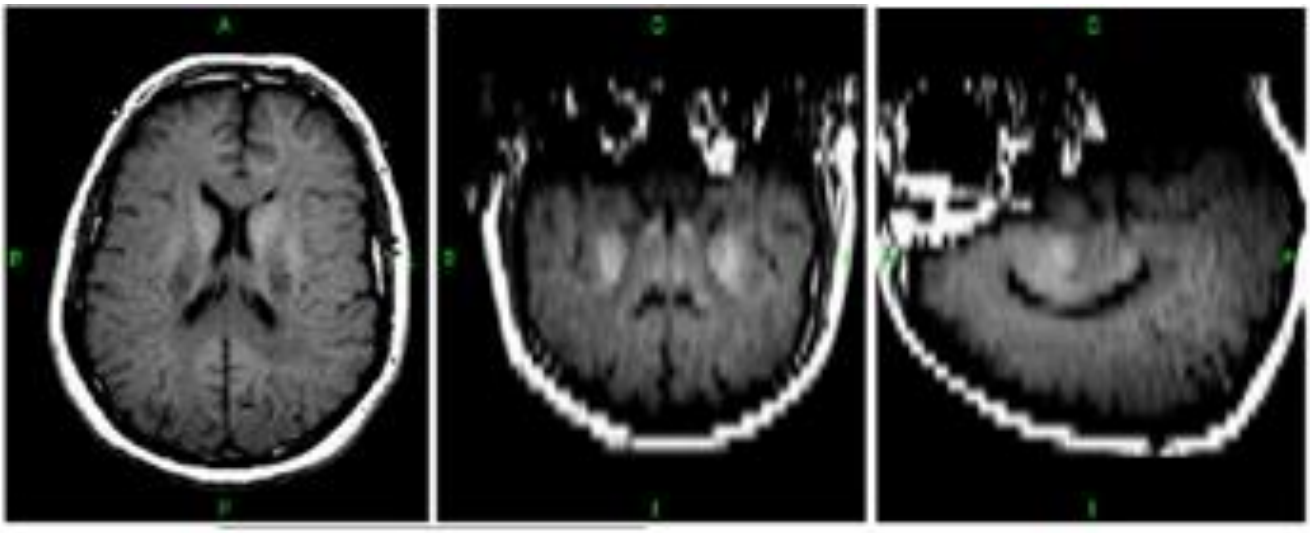


Рисунок 2.5 – Приклад МРТ мозку, що показує різні роздільні здатності по різним напрямкам

Інший ключовий аспект - специфічне застосування, де потрібні об'ємні зображення. Діагностичні або наукові цілі зазвичай використовують ущільнення без втрат. Проте нові способи ущільнення втрат повинні бути краще оцінені для таких програм. Вони можуть знадобитися для передачі, таких випадках, як телемедичні системи (рис. 2.6).

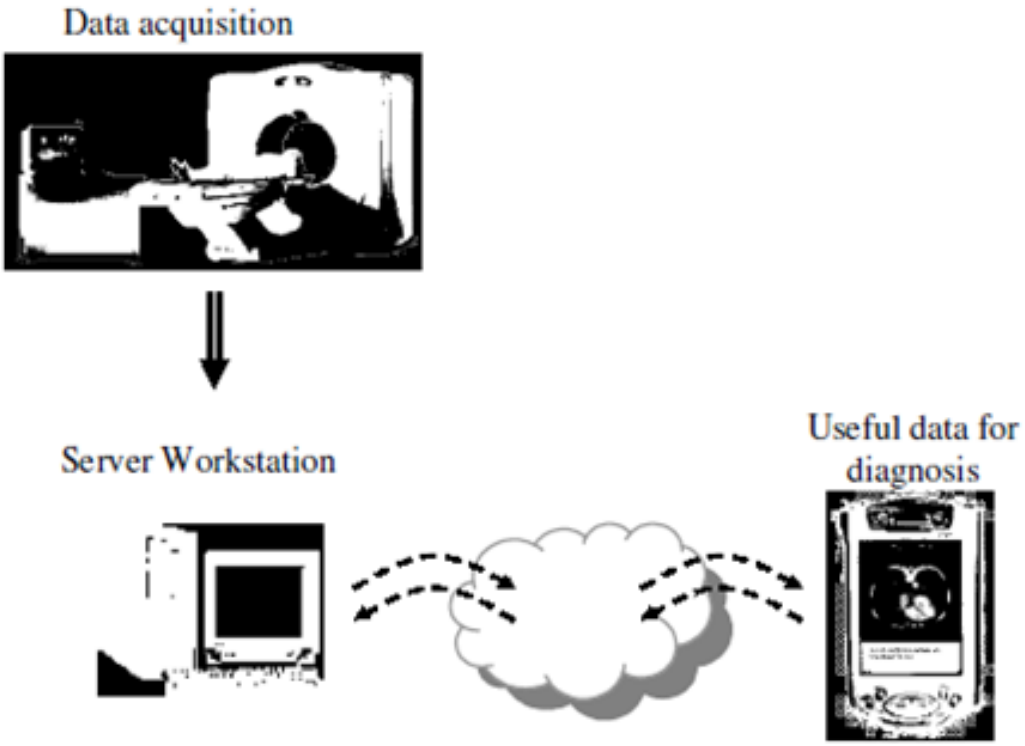


Рисунок 2.6 – Телемедична система

2.3. Методи ущільнення об’ємних даних

Одним з найпоширеніших методів ущільнення без втрат є ентропійне кодування, яке базується на теорії інформації.

В математиці і теоретичній інформатиці, ентропійне ущільнення є інформаційною теоретичними методами для доказу, що випадковий процес не є нескінченним, спочатку використовувався Робіном Моузером, щоб довести алгоритмічний варіант локальної леми Lovász [9].

Згідно Шеннону ентропія є мірою, яка встановлює середню кількість інформації на символ повідомлення. Для послідовності з m статистично незалежних символів, що з'являються з вірогідністю p_i, ентропія (2.1) виражається в наступному вигляді:

$$H = -\sum_{i=1}^{m} p_i \log_2 p_i, \qquad (2.1)$$

де: log_2 - двійковий логарифм, i - номер символу.

Якщо ймовірність появи деякого символу повідомлення дорівнює одиниці, а інших нулю, тобто невизначеність появи даного символу відсутня, і ентропія буде дорівнює нулю. У разі ж, коли ймовірності появи всіх символів однакові [10]:

$$p_i = \frac{1}{m} \tag{2.2}$$

ентропія досягає свого максимального значення, рівного:

$$H_{max} = -\sum_{i=1}^{m} \frac{1}{m} \log_2 \frac{1}{m}. \tag{2.3}$$

Зіставляючи знайдене значення ентропії з її максимальним значенням, визначають величину надмірності сигналу наступним чином [10]:

$$R = 1 - \frac{H}{H_{max}}. \tag{2.4}$$

У тому випадку, коли ймовірності появи всіх символів однакові:

$$p_i = \frac{1}{m} \tag{2.5}$$

і надмірність, як це зрозуміло з викладеного, відсутня.

Коефіцієнт ущільнення (6) показує у скільки разів можна зменшити число двійкових одиниць коду, потрібних для подання повідомлень джерела з ентропією *H* (в даному випадку зображення), в порівнянні з випадком, коли при тому ж наборі символів всі символи джерела повідомлення кодуються кодовими словами однакової довжини.

$$k_{\text{ущ}} = \frac{H_{max}}{H}. \tag{2.6}$$

Передбачається, що до кодування окремі елементи послідовності мають різну ймовірність появи. Після кодування в результуючій послідовності ймовірності появи окремих символів практично однакові (ентропія на символ максимальна).

Розрізняють декілька варіантів кодів.

1. Зіставлення кожному елементу вхідної послідовності різного числа елементів результуючої послідовності.
2. Чим більше вірогідність появи вхідного елемента, тим коротше відповідна результуюча послідовність. Прикладом можуть служити код Шеннона - Фано, код Хаффмана
3. Зіставлення кількох елементів вхідної послідовності фіксованого числа елементів кінцевої послідовності. Прикладом є код Танстола.
4. Інші структурні коди, засновані на операціях з послідовністю символів.

Прикладом є кодування довжин серій [11].

2.3.1. Ущільнені об’ємних даних методом кодування довжин серій

Кодування довжин серій, або як його ще називають RLE (Run-Length Encoding), в даний час широко застосовується при запису графічних зображень в файли або як самостійний метод, або в складі більш складних алгоритмом мов кодування, що застосовуються в різних форматах графічних файлів, наприклад в JPEG [11]. Цей метод застосовується також у таких поширених форматах, як PCX, TIFF і TARGA [10].

Відомо, що багато графічних зображень, наприклад, креслення, плакати та інше включають в себе значні однорідні області, що мають однакові яскравість і колір. При розкладанні таких зображень в растр наявність однорідних областей призводить до появи в рядках послідовностей відліків, що мають одні і ті ж значення. Ця особливість дозволяє при їх ущільнені витрачати менше двійкових одиниць, ніж при традиційному методі кодування, записуючи лише довжину серії (число повторень однакових відліків) і значення яскравості, з якого починається серія. Так при використанні методу кодування довжин серій для кодування відліків яскравості, показаних на рис. 2.7, отримаємо наступну кодову послідовність:

0,0; 2,1; 5,3; 1,2. З викладеного випливає, що при використанні цього методу в кодованому сигналі усуваються (строго кажучи, послаблюються) кореляційні зв'язки [10].

Необхідно визначити величину коефіцієнта ущільнення, яке забезпечується при використанні цього методу.

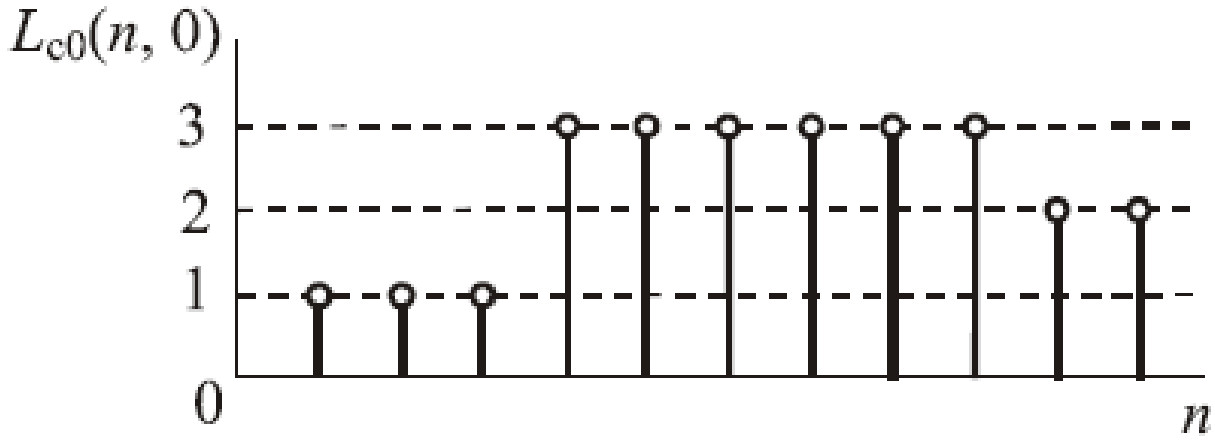


Рисунок 2.7 – Метод кодування довжин серій

З огляду на, що для запису числа повторень однакових відліків в послідовності, максимальна протяжність якої дорівнює N, необхідно затратити $log_2 N$ двійкових одиниць, а також необхідно затратити log2m двійкових одиниць для запису значення самої величини, де m - число рівнів квантування яскравості в кодованому зображенні, знайдемо, що витрата двійкових одиниць для запису послідовності складе [10]:

$$N_{\text{посл}} = \log_2 N + \log_2 m. \qquad (7)$$

Позначаючи ймовірність нового значення, тобто ймовірність появи послідовності, через рнов, а число рядків в зображенні і число відліків в рядку, відповідно, через $N_{стр}$ і $N_{пікс}$, знайдемо, що повна витрата двійкових одиниць коду для запису зображення буде дорівнює $p_{нов} N_{стр} N_{пікс}$ $(log_2 N + log_2 m)$. Беручи до уваги, що при традиційному кодуванні для запису такого зображення буде потрібно $N_{стр} N_{пікс} \times log_2 m$ двійкових одиниць, знаходимо,

що коефіцієнт ущільнення $k_{ущ}$, який забезпечувався б від застосування методу кодування довжин серій, складе [10]:

$$k_{\text{ущ}} = \frac{\log_2 m}{p_{\text{нов}}(\log_2 N + \log_2 m)}. \quad (8)$$

З цієї формули видно, що коефіцієнт ущільнення сильно залежить від ймовірності появи нових значень $p_{нов}$. При малих значеннях ймовірності нових значень коефіцієнт ущільнення виявляється більшим, але швидко зменшується при її збільшенні. На жаль, статистика напівтонових зображень така, що при 256 рівнях квантування практично кожен новий відлік (піксель) представляє нове значення, тобто рнов ≅1. Якщо звернутись до формули, то видно, що при рнов ≅1 коефіцієнт ущільнення буде менше одиниці, тобто застосування описаного методу призводить не до скорочення числа двійкових одиниць, а до збільшення. Пояснюється це тим, що в цьому випадку додаткова витрата двійкових одиниць йде на уявлення тривалості послідовностей, хоча їх протяжність майже завжди дорівнює одиниці.

Недоліком цього методу є також його низька завадостійкість. Навіть рідкісні перешкоди призводять або до появи на зображеннях протяжних штрихів, оскільки перешкода змінює значення яскравості всієї послідовності, або, що ще гірше, до "розсмикування" рядків, якщо перешкода спотворює дані про кількість повторення відліку в послідовності. Перевагою ж цього методу є простота його реалізації. Зазначені особливості визначили і область його застосування, а саме під час запису графічних зображень, в тому числі кольорових, що містять великі однорідні поля. Але для ущільнення об’ємних даних цей метод не підходить.

2.3.2. Ущільнення методом LZ

На сьогоднішній день метод LZW використовується в форматах запису як графічної, так і гіпертекстової інформації: GIF, TIFF, PDF і ряді інших.

Особливістю цього методу є адаптивність і використання кодів змінної довжини з максимальною довжиною 12 двійкових одиниць [11].

Методу ущільнення LZ полягає в наступному. Якщо вважати, що ущільненню підлягає чорно-біле півтонуване зображення, проквантованное по яскравості на 256 рівнів. Ущільнення починається з того, що будується первісна таблиця кодів, в якій кожному рівню квантування зіставляється код, який представляє собою двійкову запис номера рівня квантування. Так, наприклад, нульовому рівню квантування приписується значення коду – 0, першому рівню квантування значення – 1 і так далі, 255-му рівню квантування значення – 255 [9].

Така таблиця містить 256 значень кода. Далі в таблицю записуються ще два коду: код очищення, якому присвоюється значення 256, і код кінця запису – 257. Код очищення використовують для того, щоб не сталося переповнення таблиці, яка за може включати коди протяжністю не більше 12 двійкових одиниць (числа , що не перевищують 4095).

Він необхідний, так як у міру заповнення таблиці і відповідного збільшення довжини кодового слова має місце перехід до кодів протяжністю в 10, 11 і 12 довічних одиниць. Код очищення ініціалізує таблицю заново, стираючи в ній все коди, починаючи з 258 і вище і звільняючи тим самим місце для кодового представлення зустрічаються в зображенні комбінацій символів. Код кінця запису, як це видно з його назви, сигналізує про те, що послідовність, яка кодується, закінчилася. Після завершення підготовчих операцій алгоритм готовий до початку ущільнення даних (зображення) [10].

Алгоритм ущільнення даних можна записати в такий спосіб:

1. Ініціалізація, тобто ввід початкової таблиці кодів.
2. Очистити таблицю кодів, починаючи з коду 258 і до кінця.
3. Очистити буфер рядка (String), буфер рядка (Test) і буфер рядка (Byte).
4. Далі в циклі:

4.1. прочитати черговий байт кодованих даних в буфер (Byte);

4.2. зчепити (конкатенувати) String + Byte і помістити результат в буфер Test;

4.3. перевірити, чи є в таблиці кодів код, відповідний комбінації, вміщеній в буфер Test:

4.3.1. якщо є, то вміст буфера Test переписати в буфер String і перейти в початок циклу;

4.3.2. якщо немає, то додати в таблицю код, відповідний вмісту буфера Test, присвоївши йому значення, що збігається з наступним вільним порядковим номером, вивести в вихідний потік код, відповідний вмісту буфера String, переписати вміст буфера Byte в String і перейти в початок циклу.

5. Робота програми закінчується тим, що робляться записи в вихідний потік коду вмісту String і коду кінця запису.

В результаті застосування такого алгоритму отримуємуються коди змінної довжини, причому для поєднань з двох-трьох символів, кожен з яких окремо описується в таблиці 8-розрядних кодом, довжина отриманих кодів становитиме не 16 і не 24 біта, а суттєво менше [10].

Метод ущільнення LZW може бути застосований не тільки для ущільнення даних, кожна одиниця яких має розмір в один байт, наприклад, відліків яскравості чорно-білого напівтонового зображення, але також і для ущільнення даних, що мають довільний розмір. В цьому випадку кодові послідовності цих даних об'єднуються в групи по 8 двійкових одиниць. Так якщо кожен відлік містить 4 довічні одиниці, то об'єднання в групи відбувається по два відліку, а якщо один відлік представлений 16 двійковими одиницями коду, то така кодова послідовність ділиться навпіл. Величина ущільнення півтонових і кольорових зображень, що забезпечується при використанні цього методу, невелика і складає приблизно 1,2 рази [10].

2.3.3. Ущільнення методом Хаффмана

Цей метод дозволяє отримати код з мінімальною середньою довжиною при заданому розподілі ймовірностей значень некорелірованних відліків сигналів за умови, що ймовірності появи відліків з цими значеннями будуть рівні $1/2^n$, де n - ціле число. В іншому випадку ступінь ущільнення, що забезпечується використанням цього коду, буде нижче. Сказане пояснюється рис. 2.8, на якому тонкою лінією показано кількість двійкових одиниць коду, потрібних на відлік при ідеальному ущільнення, а жирною лінією - кількість двійкових одиниць коду при використанні коду Хаффмана [10].

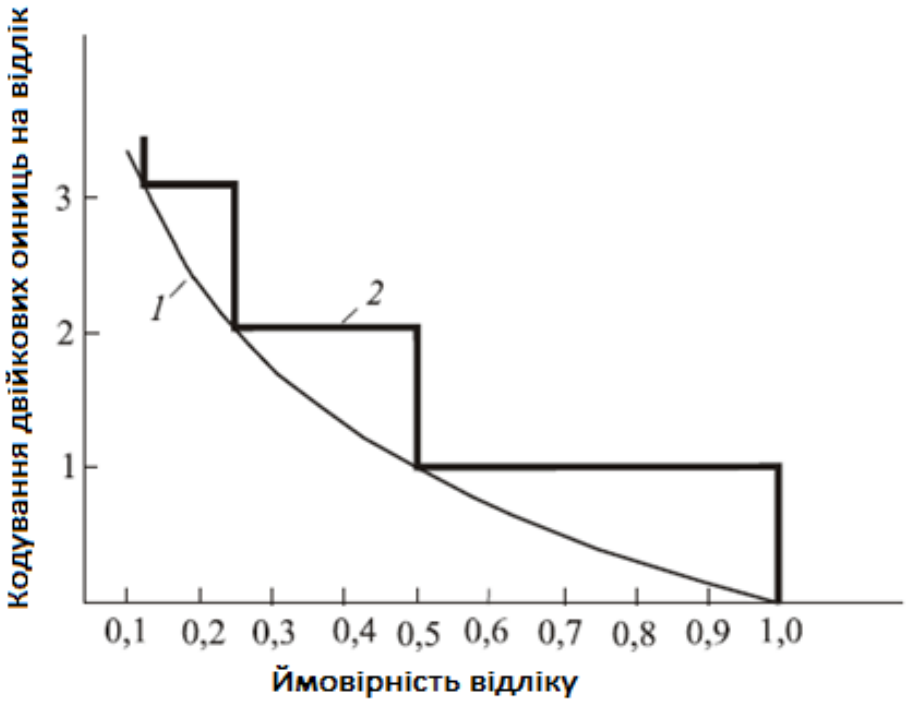


Рисунок 2.8 – Залежність необхідної кількості двійкових одиниць на відлік: 1 - при ідеальному методі ущільнення; 2 - при ущільнення методом Хаффмана

Особливістю цього методу кодування є використання кодів змінної довжини, при цьому найбільш Ймовірним символам присвоюються найбільш короткі кодові слова, а менш ймовірним - довгі.

Це можна пояснити на прикладі побудови кодової таблиці. На рис. 2.9 показано кодове дерево стосовно до випадку кодування шести символів A_1,

A_2, A_3, A_4, A_5, A_6, які можуть являти собою значення яскравості пікселів зображення, і наведені ймовірності, з якими вони з'являються [10].

Побудова кодової таблиці починається з того, що два символи з найменшими ймовірностями об'єднуються в вузол кодового дерева, якому приписується їх сумарна ймовірність.

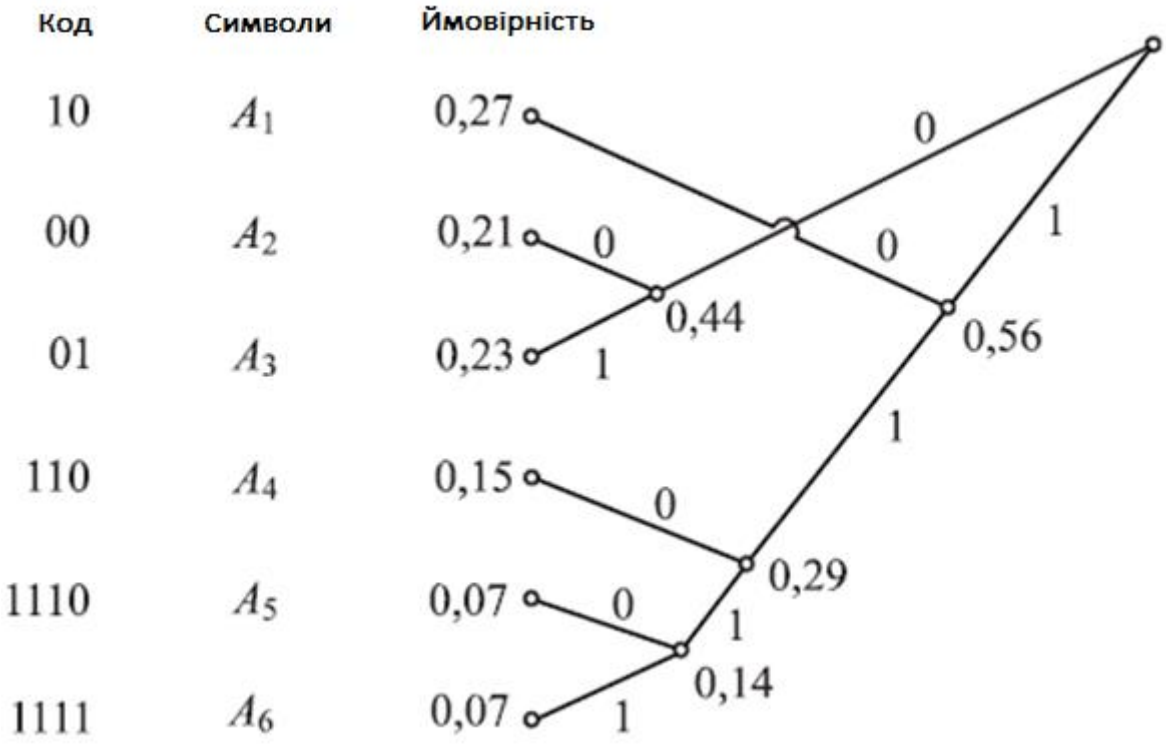


Рисунок 2.9 – Кодове дерево

У даному прикладі мова йде про символи A_5 і A_6, сумарна ймовірність яких дорівнює 0,14. Далі об'єднуються такі символи або вузли з найменшою ймовірністю, як це показано на малюнку. Цей процес триває до тих пір, поки гілки кодового дерева зійдуться до одного вузла, розташованого в вершині [9].

Після цього гілки дерева в залежності від того, в який бік вони розходяться від вузла, позначаються нулями або одиницями (в даному прикладі праві гілки позначені нулями, а ліві одиницями). Для того щоб знайти значення кодового слова, яке слід приписати кожному символу, необхідно йти від вершини кодового дерева до даного символу, записуючи нулі або одиниці, якими позначені пройдені гілки [10].

У разі застосування коду Хаффмана для ущільнення об’ємних даних необхідно спочатку здійснити декорреляцію сигналу, яким представлено данні, а вже потім застосовувати кодування по Хаффману.

2.3.4. Декореляція сигналу

Надмірність зображення обумовлена наявністю сильних кореляційних зав’язків між значеннями яскравості суміжних пікселів і, крім того, нерівномірністю розподілу щільності ймовірності їх значень, яка мала за значенням, це пояснюється на рис. 2.10, на якому наведена щільність ймовірності значень яскравості в оригінальних даних W (L) [10].

Рисунок 2.10 – Графік залежності щільності ймовірності W (L) від яскравості L

У зв'язку з цим, першим кроком при використанні деяких видів ентропійного кодування є декорреляції послідовності пікселів, що кодується, при якій встановлюються статистичні зв'язки між кодованими пікселями. Внаслідок декорреляції збільшується нерівномірність розподілу щільності ймовірності їх інтенсивностей, і вже тільки після цього проводиться кодування статистично незалежних відліків. Найпростішим, але не оптимальним способом декорреляції, є перетворення послідовності відліків

кодованого сигналу, що представляє яскравість пікселів зображення *L (n)*, в послідовність відліків збільшень цієї яскравості *ΔL (n)* при переході з одного пікселя на інший, тобто

$$\Delta L(n) = L(n+1) - L(n), \qquad (9)$$

де n - номер відліку. В результаті такого перетворення статистичні зв'язки між кодованими відліками сильно послаблюються, а розподіл щільності ймовірності їх значень стає різко нерівномірним. Зазначене пояснюється на рис. 2.11, на якому наведена щільність ймовірності збільшення яскравості *W (ΔL)*.

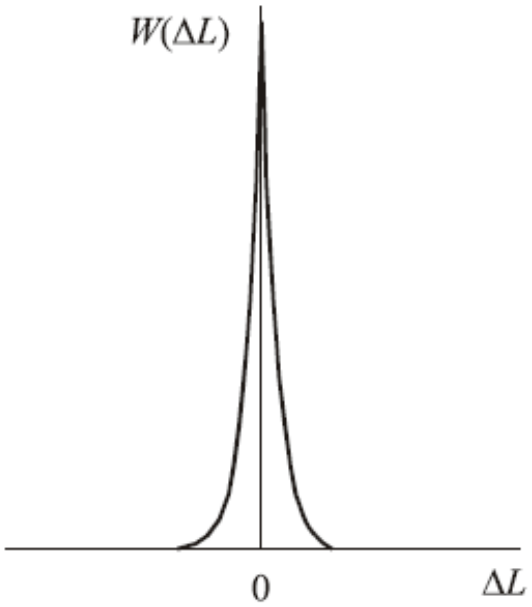


Рисунок 2.11 – Графік залежності щільності ймовірності *W (L)* від яскравості *ΔL*

Якщо порівняти рис. 2.10 та рис. 2.11 видно, що в другому випадку щільність ймовірності розподілу прирощень різко нерівномірна, завдяки чому сигнал послідовності прирощень має велику надмірністю, а, отже, може бути більше зменшений [10].

Зображення, представлені на рис. 2.12, та рис. 2.12, ілюструють сказане.

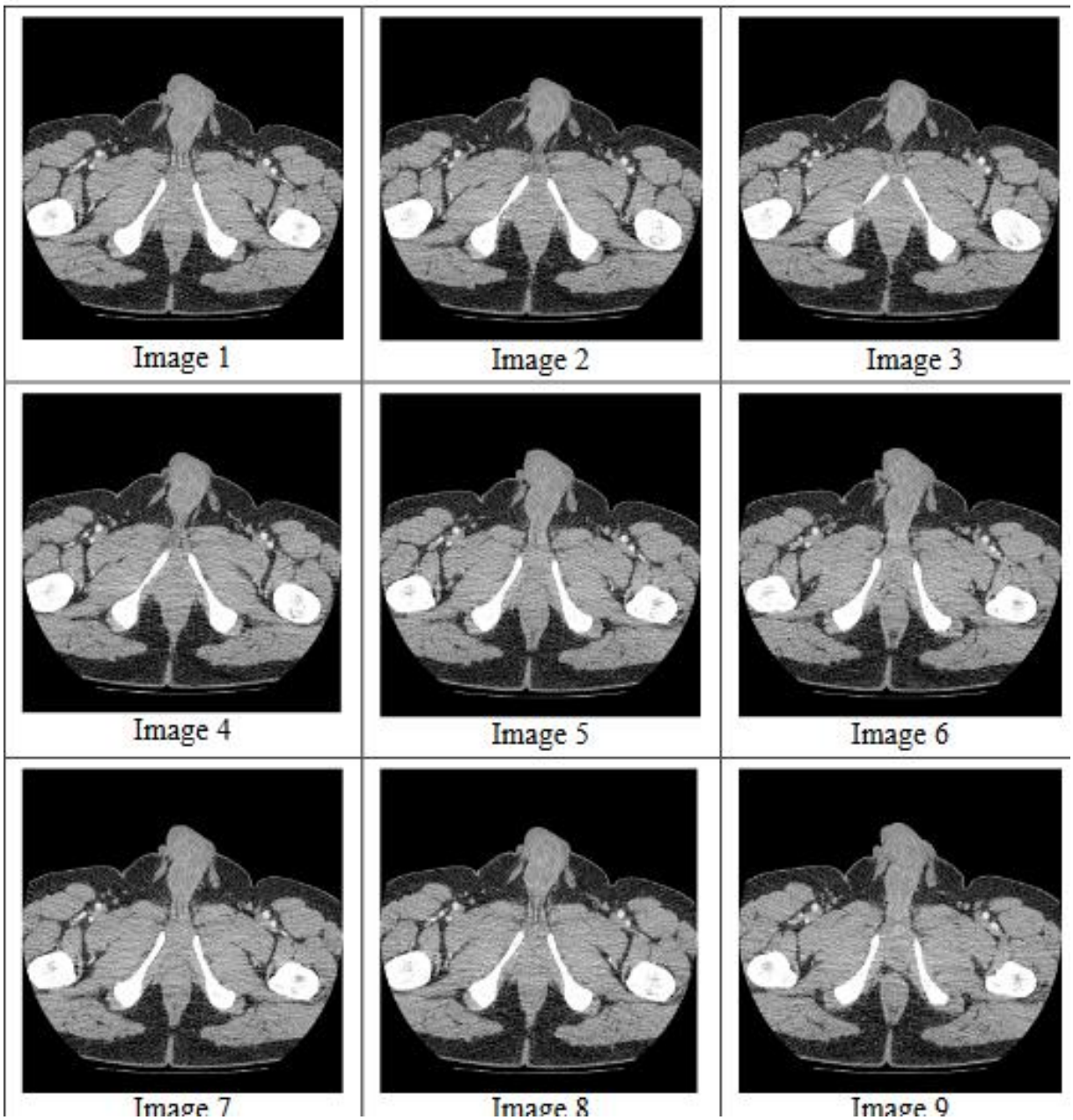


Рисунок 2.12 – Група оригінальних даних

Рис. 2.12, а являє собою групу вихідних зображень, а рис. 2.13 - ці ж зображення, але після їх декорреляції. При виготовленні рис. 2.13 до приростень яскравості $\Delta L\ (n)$, що виникають при переході з одного пікселя на інший, доданий сірий фон для того, щоб відтворити негативні збільшення яскравості, які в іншому випадку були б обмежені. Порівнюючи ці зображення, можна помітити, що в оригінальних даних представлені всі градації яскравості приблизно з однаковою ймовірністю, в той час як в декорреліpованном зображенні ймовірність великих збільшень (великих

відхилень від сірого фону) порівняно мала і має місце тільки на контурах [10].

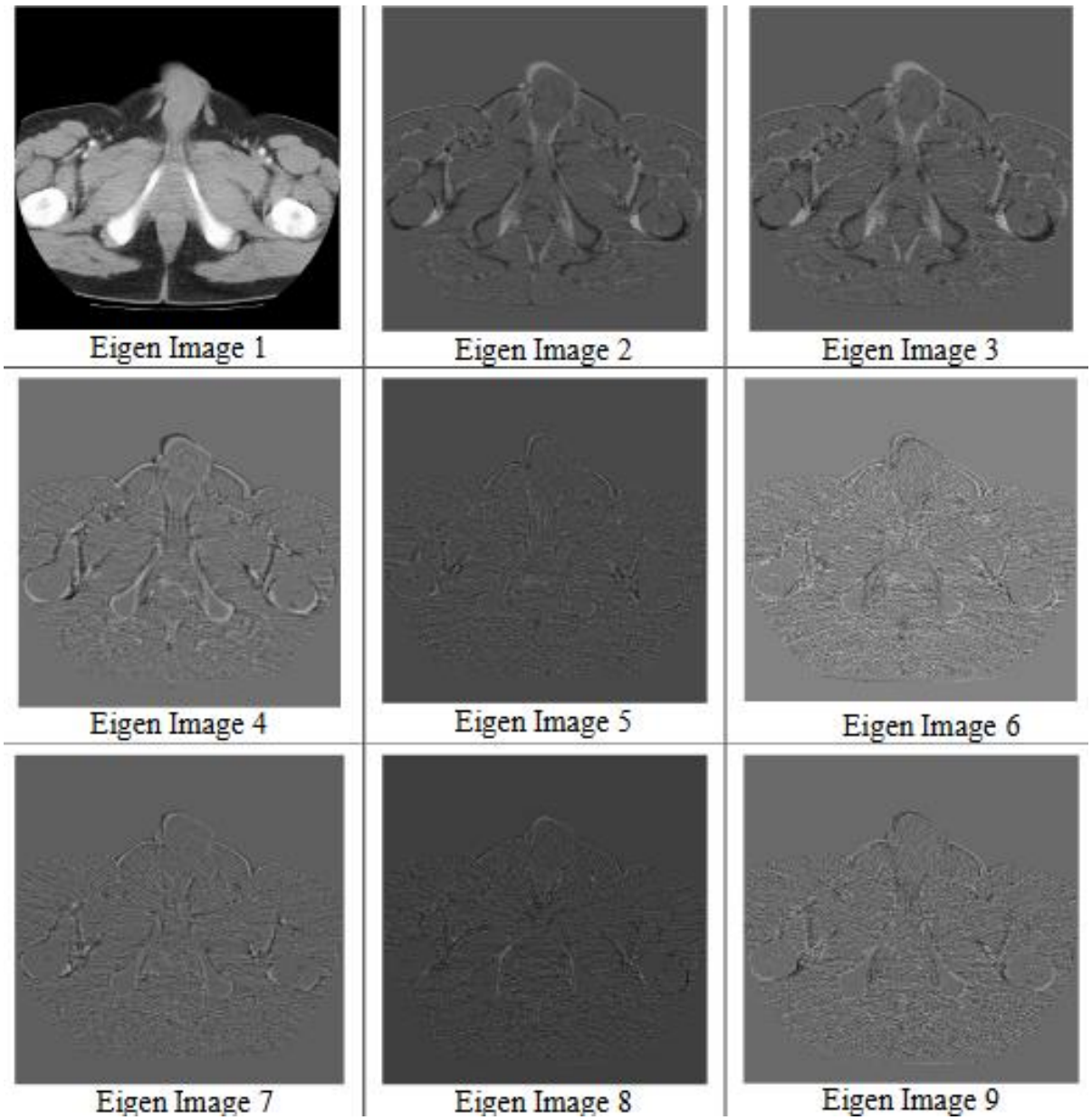


Рисунок 2.13 – Група зображень після декориляції

2.4. Вейвлет-перетворення

Вейвлет-перетворення може розглядатися як корисний підхід у вирішенні проблеми аналізу обробки сигналу/зображення як у часі, так і в частоті. Спочатку дані (наприклад, зображення/сигнал) знаходяться в просторовому обласному значенні, який потрібно перетворити в частотну

область, щоб витягнути ознаки або значущу інформацію про дані. Таким чином, перед ущільненням будь-яких даних (зображення/сигналу) необхідно перетворити дані з часового домену (також відомий як просторовий домен) до частотного домену. Для цього використовується дискретне вейвлет-перетворення для досягнення високої якості даних, а також кращої ефективності ущільнення [13].

Згідно з методом вейвлет-перетворення, розбиття об’ємних даних виконується на різних рівнях для отримання коефіцієнтів цих даних. Ці коефіцієнти відомі як частотні компоненти. Після того, як тільки коефіцієнти стають відомими, зображення ділиться на менші блоках. На кожному блоці, то кодування виконується з використанням різних функцій [13].

Процес кодування виконується таким чином, що найбільш значущі пікселі будуть залишалися на зображенні, а пікселі з низьким значення буде видалено з зображення. Після цього етапу, інформація про зображення та ущільнений варіант будуть ефективно отримані з оригінальних даних. Ці блоки коефіцієнтів об'єднуються використовуючи зворотний метод дискретного вейвлет-перетворення (DWT).

Після того, як зображення побудоване, отримується ущільнена форма оригінальних даних. Після цієї стадії ущільнення, виявлення області інтересів (ROI) здійснюється на підставі значного аналізу. На підставі цього аналізу, визначаються сегменти над зображенням, а на основі аналізу мінімальної відстані, здійснюється відображення зображення в сегменти. Після отримання сегментів проводиться аналіз середньої інтенсивності для визначення цілісності цих сегментів. Цей циклічний процес продовжується до тих пір, поки не буде отримана фактична інформація про дані.

Для більш наочної ілюстрації ідеї вейвлет-перетворення уявімо собі, що розглянутий числовий потік кодує деяке зображення, що виводиться на екран комп'ютера. Припустимо, що екран являє собою прямокутну матрицю з великою кількістю пікселів з фіксованим числом градацій яскравості. Це зображення є чорно-білим [14].

Зазвичай пікселі перенумеровані послідовно по рядках, які попередньо збудовані один за одним в пряму лінію; таким чином, пікселі набувають номера *0, 1, 2,. . . , N-1*, де $N = M \times K$, де *M* число рядків даної матриці, а *K* – кількість її стовпців.

Для визначеності будемо вважати Н парним; нехай $N = 2L$, де *L* – натуральне число. Кожному пікселю пропонується певна яскравість, що виражається деяким числом; позначимо це число для j-го пікселя через c_j. Таким чином, кодування зображення проводиться за допомогою числового потоку:

$$c_0,c_1,c_2,c_3,c_4,c_5,c_6,c_7,\ldots,c_{2L-1}. \qquad (2.9)$$

Потік (2.9) може бути переданий по лініях зв'язку і при подачі на екран комп'ютера може бути перетворений в вихідне зображення. Якщо вихідне зображення передається з великою точністю, то *H* дуже велике, і передача навіть одного такого зображення представляє значні технічні труднощі (на практиці потрібно передавати мільйони таких зображень з великою швидкістю). Тому виникає необхідність зменшення кількості переданих чисел. Припускаючи, що сусідні числа в (2.9) близькі, можна було б запропонувати передавати, наприклад, тільки числа з непарними номерами в (2.9), тобто числа [14]

$$c_1\ c_3\ c_5\ c_7,\ldots,c_{2L-1}. \qquad (2.10)$$

Таке перетворення називається проріджуванням вихідного числового потоку (англійський термін upsampling – розрідження або розріджується вибірка).

Замість потоку (2.9) передають в два рази коротший потік (2.10); приймальний пристрій розширює отриманий числовий потік (2.10) дублюванням прийнятих значень так, щоб в результаті на місцях з парних і з наступним непарним номером перебували однакові числа. В результаті на

екрані відтворюється зображення, отримане за допомогою числового потоку виду [14]:

$$c_1\ c_1\ c_3\ c_3\ c_5\ c_5\ c_7\ c_7,\ldots,c_{2L-1}\ c_{2L-1}. \quad (2.11)$$

Тим самим "відновлення" (2.11) вихідного потоку (2.9) проводиться з похибкою, причому інформація втрачається незворотнім чином (Тобто без передачі додаткової інформації приймальний пристрій, взагалі кажучи, не в змозі відновити потік (2.9)). Такий прийом (англійська еквівалент downsampling – згущення) виправданий, якщо отримане зображення мало відрізняється від початкового.

Недоліки описаного підходу полягають у наступному.

1. Він застосовується лише до потоку, який повільно змінюється.
2. Відсутній облік характеристик числового потоку (в деяких частинах числовий потік може змінюватися дуже повільно, і можна було б викидати багато чисел поспіль, а в інших частинах при швидкій зміні потоку будь-які викидання чисел можуть істотно зіпсувати зображення, що передається).
3. Немає засобів для уточнення переданого потоку.

Ідея вейвлет-перетворення ілюструється наступним чином. З числового потоку (2.9) формується два числові потоки:

$$a_j = \frac{(c_{2j}+c_{j+1})}{2},\ b_j = \frac{(c_{2j}+c_{2j+1})}{2}, \quad (2.12)$$

де j=0, 1, …, L-1.

Можна побачити, що

$$c_{2j} = a_j + b_j,\ c_{2j+1} = a_j - b_j, \quad (2.13)$$

де j=0, 1, …, L-1.

Таким чином, якщо потік (2.9) замінити двома потоками (2.13), то після їх передачі можна відновити оригінальний потік (2.9), використовуючи формули (2.13).

Таким чином, якщо сусідні числа в (2.9) близькі, то другий з потоків в (2.12) складається з чисел, близьких до нуля, так що може виявитися, що другий потік взагалі не потрібен і його можна відкинути.

Однак, якщо деякі фрагменти першого потоку з (2.12) не дають достатньої точності, то можна використовувати відповідні фрагменти (з тими ж діапазонами індексів) другого потоку, і провести розрахунки за формулами (2.13); це призведе до точного відновлення вихідного потоку (2.9) на відповідних ділянках (подібна технологія передачі використовується, зокрема, при передачі зображень в Інтернет: спочатку з'являються основні контури зображення, що дозволяють оцінити його зміст і перервати передачу, якщо в ній немає необхідності, і лише потім відбувається уточнення, і остаточне завершення передачі зображення) [14].

Потік чисел:

$$a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,\ldots,a_{L-1}. \qquad (2.14)$$

називають основним, а потік чисел:

$$b_0,b_1,b_2,b_3,b_4,b_5,b_6,b_7,\ldots,b_{L-1}. \qquad (2.15)$$

вейвлетним потоком.

Отриманий основний потік (2.14) можна розглядати як ущільнений вихідний потік (2.9), а потік (2.15) як поправку до основного потоку, що дозволяє відновити оригінальний потік.

Якщо потік (2.14) все ще великий для передачі, то аналогічною процедурою його розщеплюють на два потоки: потік, який є основним для потоку (2.14) (він має назву – нульове наближення до вихідного потоку (2.9) або просто нульовий потік) і відповідний вейвлетний потік (його називають першою поправкою до нульового потоку або першим вейвлетним потоком); в цьому випадку потік (2.15) можна назвати другою поправкою (або другим вейвлетним потоком).

Можливе подальше продовження процесу розщеплення; на *k*-му кроці отримаємо розщеплення вихідного потоку на *k + 1* потоків: нульовий потік (основний результат ущільнення) і *k*-вейвлетних потоків, послідовне додавання яких до нульового потоку призводить до послідовного уточнення результату ущільнення аж до повного відновлення вихідного потоку. Представлена методика схожа на розкладання по формулі Тейлора, де похідні замінені відповідними речами [14].

Існують різні види вейвлет-перетворення.

1. Вейвлет Хаара.
2. Вейвлет Добеши.
3. Вейвлет Мейера та інші.

Розглянемо деякі з вейвлет-перетворень.

Вейвлет Хаара.

У 1910 році Альфред Хаар представив першу вейвлет-систему. Вейвлет Хаара (HWT) славиться простотою, прямотою і швидкістю обчислень [14]. Вейвлети Хаара ортогональні, мають компактний носій, добре локалізовані в просторі, але не є гладкими. Отримано два типи коефіцієнтів з перетворення Хаара (рис. 2.14).

1. Грубе наближення (апроксимація).
2. Деталізуюча інформація.

Вейвлет Хаара має як пряме, так і зворотне перетворення (рис. 2.15).

Пряме перетворення.

1. Обчислення елементів масштабування - додавання двох сусідніх зразків і ділення на 2.
2. Обчислення вейвлет-елементів - віднімання два суміжні зразки і ділення на 2.

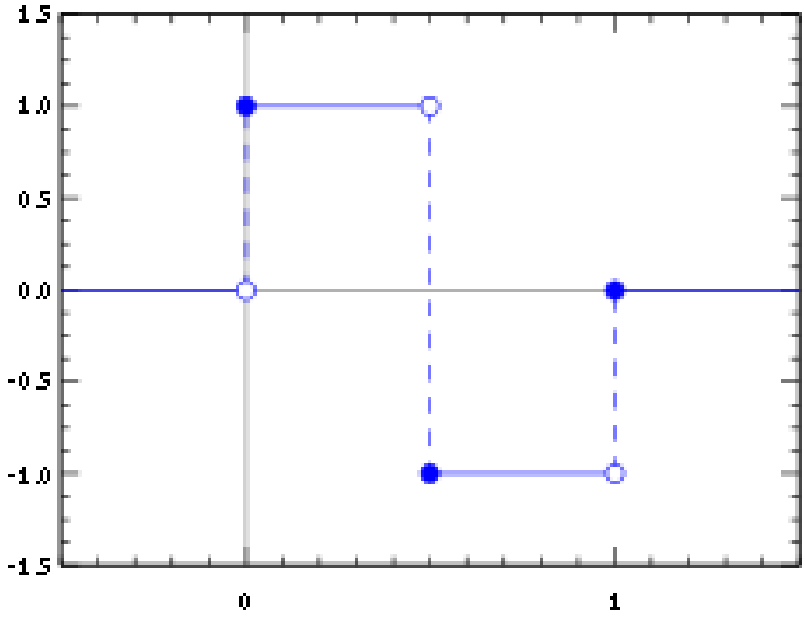


Рисунок 2.14 – Вейвлет Хаара

Зворотне перетворення.

1. Обчислення вимагає просто додавання та віднімання.

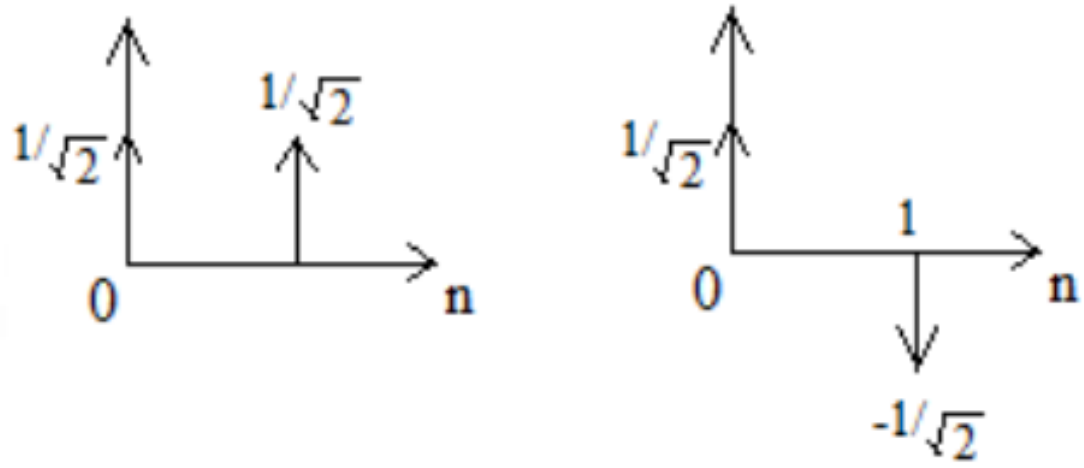


Рисунок 2.15 – Форма хвилі для фільтрів Хаара

Все зображення на першому рівні ділиться на матриці.

1. LL0 (low-low).
2. LH0 (low-high).
3. HL0(high-low).
4. HH0 (high-high).

Далі низькочастотна матриця LL0 піддається вейвлет розкладу. Його результатом є матриці HH1, HL1, LH1, LL1. Таке розкладання повторюється r

раз, як показано на рис. 2.16. Результатом розкладання є набір з *3r + 1* матриць розмірності, що зменшується. Кожна матриця піддається скалярному або векторному квантуванню і подальшому кодуванню. Вибір числа рівнів квантування або кроку квантування виробляється виходячи з потрібного ущільнення і відповідного розподілу бітів між матрицями [15].

Перетворення Хаара використовується для стиснення вхідних сигналів, компресії зображень, в основному кольорових і чорно-білих з плавними переходами.

Ідеально підходить для об'ємних даних типу рентгенівських знімків. Даний вид архівації відомий досить давно і безпосередньо виходить з ідеї використання когерентності областей.

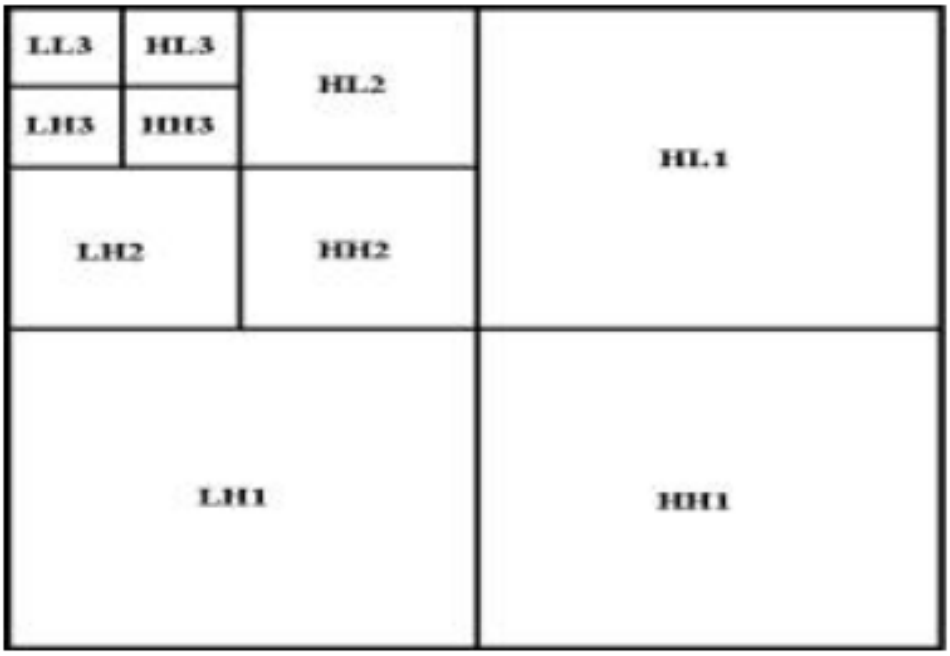


Рисунок 2.16 – Вейвлет перетворення зображення

Ступінь ущільнення задається і варіюється в межах 5-100. При спробі задати більший коефіцієнт на різких межах, особливо тих, що проходять по діагоналі, проявляється «сходовий ефект» - сходинки різної яскравості розміром в кілька пікселів.

Вейвлет Добеши

Вейвлети Добеши - сімейство ортогональних вейвлетів з компактним носієм, який обчислюється ітераційним шляхом. Названі на честь Інгрід

Добеши, математика з США, яка перша побудувала дане сімейство [14].

Припустимо, що маємо зображення розміром N × N (рис. 2.17 а).

Спочатку кожний з N рядків зображення ділиться (фільтрується) на низькочастотну (НЧ) і високочастотну (ВЧ) половини. В результаті виходить два зображення розміром *N × N/2* (рис. 2.17 б). Далі кожен стовпець ділиться точно також, в результаті виходить чотири зображення розміром *N/2 × N/2* (рис. 2.17 а): низькі частоти по горизонталі і вертикалі (НЧНЧ1), високі частоти по горизонталі і вертикалі (ВЧВЧ1), низькі частоти по горизонталі і високі частоти по вертикалі (НЧВЧ1) і високі частоти по горизонталі і низькі частоти по вертикалі (ВЧНЧ1). Перше з зазначених вище зображень ділиться аналогічним чином на наступному кроці (рівні) перетворення (рис. 2.17 г) і так далі [14].

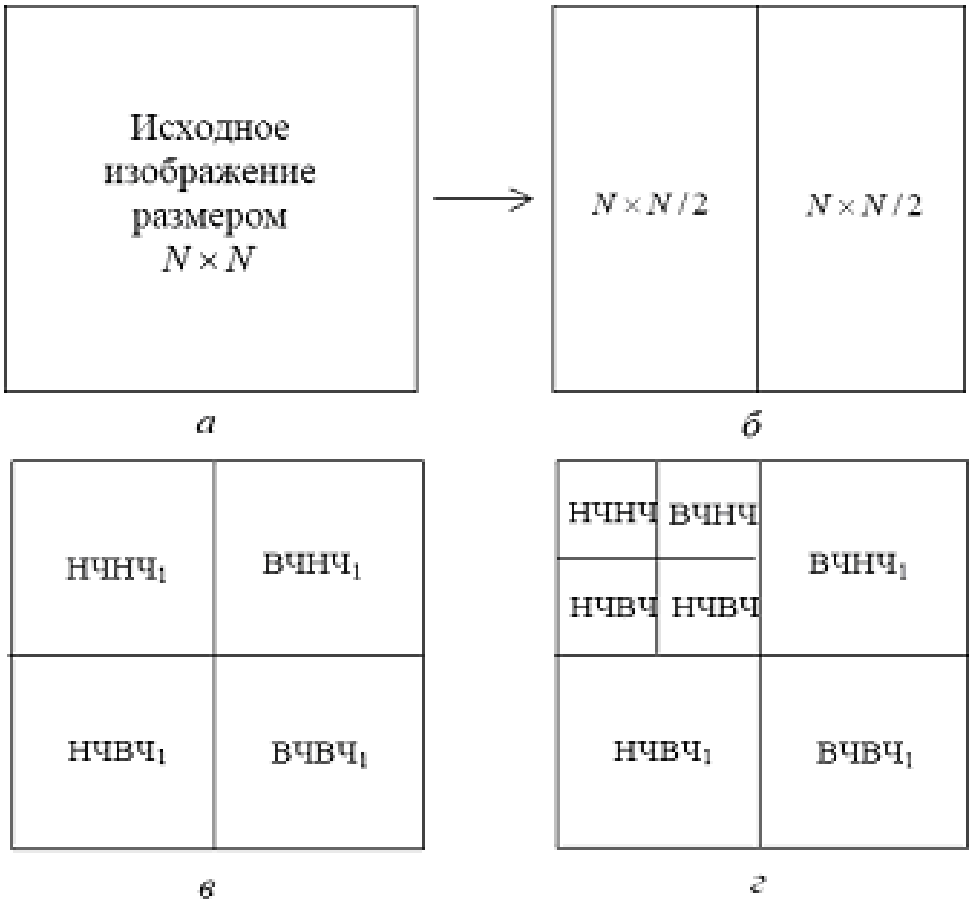


Рисунок 2.17 – Результат вейвлет-перетворення

Вейвлет Мейера

Вейвлет Мейера - ортогональний вейвлет, запропонований Івом Меєром. Як тип неприривного вейвлета, він застосовувався у ряді випадків, наприклад, у адаптивних фільтрах, фрактальних випадкових полях та багатофазні класифікації [16].

Вейвлет Мейєра нескінченно диференційований і визначається в частотній області за функцією ν як:

$$\psi(\omega) := \begin{cases} \frac{1}{\sqrt{2\pi}} \sin\left(\frac{\pi}{2}\nu\left(\frac{3|\omega|}{2\pi} - 1\right)\right) e^{\frac{j\omega}{2}} & \text{якщо } \frac{2\pi}{3} < |\omega| < \frac{4\pi}{3} \\ \frac{1}{\sqrt{2\pi}} \cos\left(\frac{\pi}{2}\nu\left(\frac{3|\omega|}{4\pi} - 1\right)\right) e^{\frac{j\omega}{2}} & \text{якщо } \frac{4\pi}{3} < |\omega| < \frac{8\pi}{3} \end{cases} \quad (16)$$

де:

$$\nu(x) := \begin{cases} 0 \text{ якщо } x < 0, \\ x \text{ якщо } 0 < x < 1, \\ 1 \text{ якщо } x > 1. \end{cases} \quad (17)$$

На рис. 2.18 зображено спектр вевйлета Мейера.

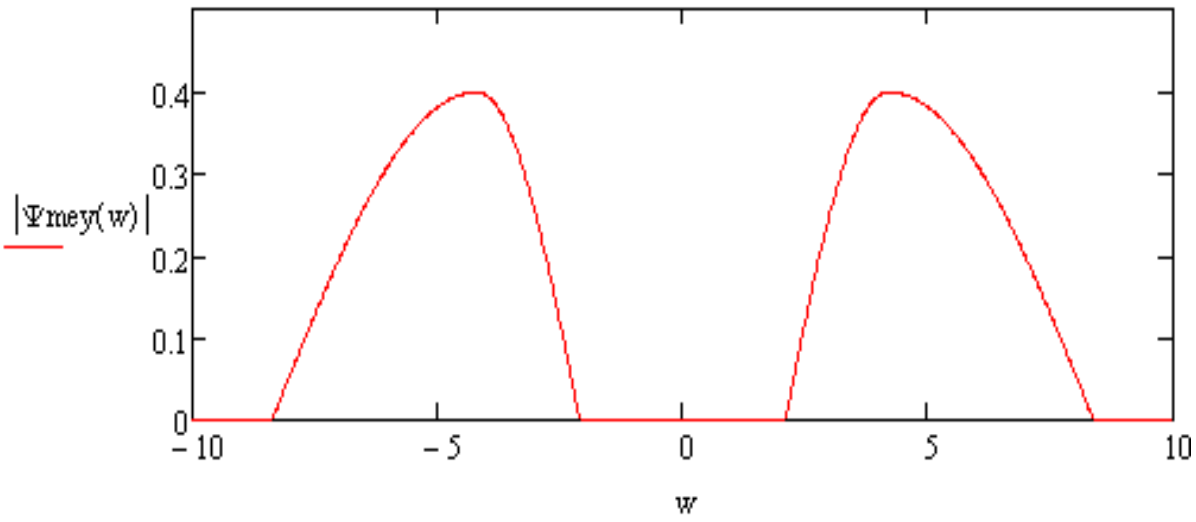


Рисунок 2.18 – Спектр вевйлета Мейера

Існує багато різних способів визначення цієї допоміжної функції, що дає варіанти вейвлета Мейера. Наприклад, прийнята інша стандартна реалізація:

$$\nu(x) := \begin{cases} x^4(35 - 84x + 70x^2 - 20x^3) \text{ якщо } 0 < x < 1, \\ 0 \text{ в інших випадках.} \end{cases} \quad (18)$$

Функція масштабу Мейера (рис. 219) визначається, як:

$$\Phi(\omega) := \begin{cases} \frac{1}{\sqrt{2\pi}} \text{ якщо } |\omega| < \frac{2\pi}{3}, \\ \frac{1}{\sqrt{2\pi}} \cos\left(\frac{\pi}{2}\nu\left(\frac{3|\omega|}{2\pi} - 1\right)\right) \text{ якщо } \frac{2\pi}{3} < |\omega| < \frac{4\pi}{3} \\ 0 \text{ в інших випадках.} \end{cases} \quad (19)$$

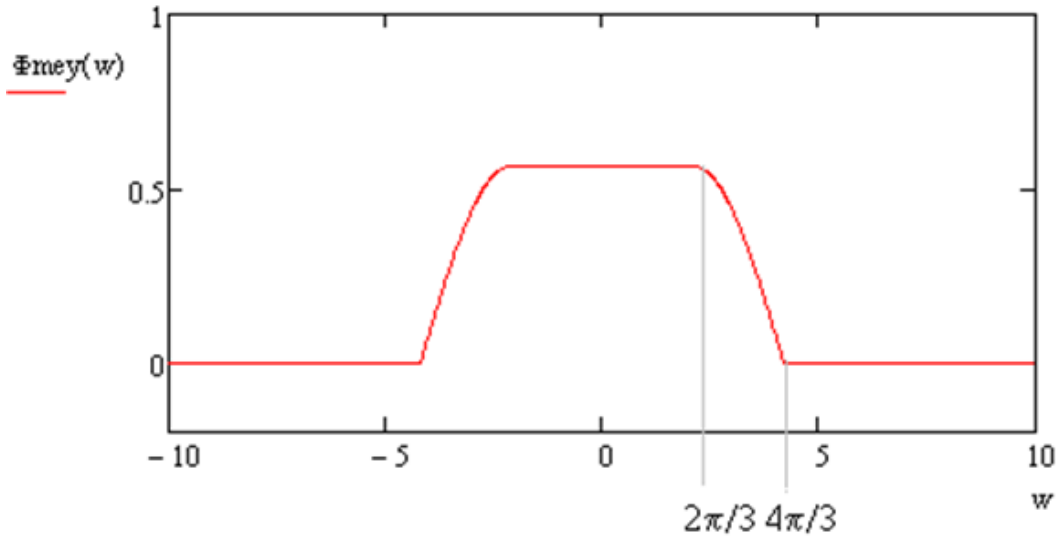


Рисунок 2.19 – Функція масштабу Мейера

У часовій області форма сигналу вейвлету Мейера має форму, як показано на рис. 2.20.

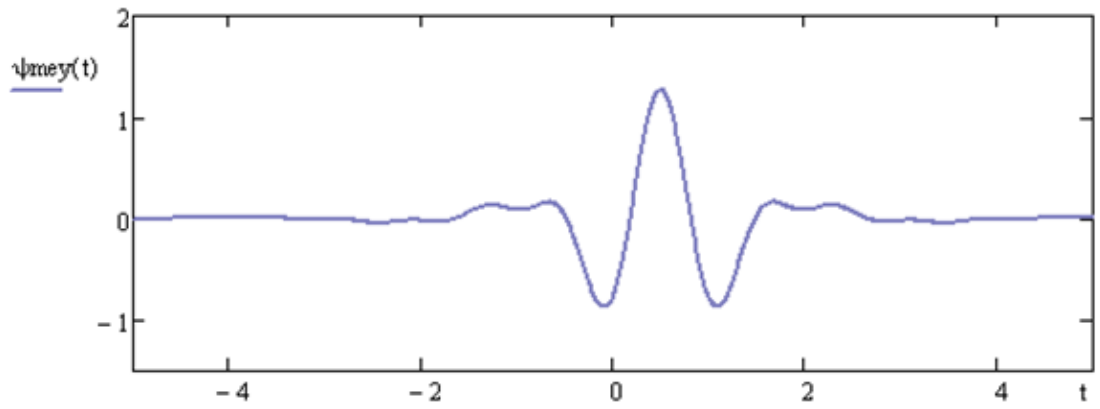


Рисунок 2.20 – Вейвлет Мейера

Висновки до розділу 2

Розглянуто та проаналізовано способи ущільнення двовимірних (2-D) даних з використанням вейвлет-перетворення.

Проаналізовано їх можливості для ущільнення тривимірних (3-D) даних. Показано, що в стандартному вигляді відомі підходи не можуть забезпечити якісного ущільнення. Тому постає актуальна задача ущільнення тривимірних (3-D) даних. Хоча об'ємні зображенні можуть розглядатися як розширення традиційних зображень, методологія кодування таких даних не є тією ж самою, що вимагає проведення додаткових досліджень.

3. МОДИФІКОВАНИЙ СПОСІБ УЩІЛЬНЕННЯ ТРИВИМІРНИХ ДАНИХ

3.1. Загальний опис модифікованого способу ущільнення великих обсягів даних

На сьогоднішній день існує велика кількість способів ущільнення даних. На основі проведеного дослідження розроблено модифікований способі ущільнення тривимірних даних.

Розроблений спосіб продемонстровано на рис. 3.1 у вигляді блок-схеми.

Рисунок 3.1 – Розроблений спосіб

Потреба в ущільнені тривимірних даних у радіології зростає прямо пропорційно зростанню кількісті цифрових методів візуалізації, і використання об’ємних даних стає важливою проблемою. Ущільнення об’ємних даних, які є наборами зображень, дуже важливе в радіології, тому що найбільш часто використовувані цифрові методи візуалізації, включаючи магнітний резонанс (MR), комп'ютерну томографію (CT), позитронну емісійну томографію (PET) та комп'ютерну томографію з однокомпонентним випромінюванням (SPECT), генерують набір слайсів. Один слайс, як правило, являє собою поперечний переріз тіла. Її прилеглі слайси є поперечними перерізами, паралельні розглянутому фрагменту.

Кілька слайсів, сформованих таким чином, зазвичай аналогічно або фізіологічно корелюються один з одним. Інакше кажучи, існує деяка структурна схожість зображення між сусідніми слайсами. Незважаючи на те, що фрагмент набору зображень можна ущільнювати фрагментом, більш ефективне ущільнення можна досягти, вивчаючи зв'язок між слайсами. Вейвлет - це функція, яка виглядає як маленька хвиля, пульсація базової лінії.

Дискретне вейвлет-перетворення (DWT) відносяться до вейвлет-перетворень, в яких вейвлети представлені дискретними сигналами (вибірками). Іншими словами, коефіцієнти дискретного вейвлет-перетворення можуть мати реальні (з плаваючою комою) значення, але значення часу та шкали, які використовуються для індексування цих коефіцієнтів, є цілими числами. У искретного вейвлет-перетворення фільтр піддіапазонів перетворює сигнал дискретного часу у середній сигнал і сигнал деталізації. Вейвлети – це математичні функції, які роздыляють дані на різні частотні компоненти, а потім вивчають кожен компонент з роздільною здатністю, відповідною її масштабу. Вони мають переваги над традиційними перетвореннями Фур'є при аналізі фізичних ситуацій, коли сигнал містить розриви і різкі зубці. Вейвлети були розроблені самостійно в сферах математики, квантової фізики, електротехніки та сейсмічної геології. Взаємозв’язки між цими полями протягом останніх десяти років призвели до

появи багатьох нових вейвлет-додатків, таких як ущільнення зображення, турбулентність, бачення людини, радіолокація та прогнозування землетрусів [17].

Схема ущілнення, як буле зазначено у першому розділі, може бути розділене на дві основні категорії: ущільнення без втрат і з втратами. Ущільнення без втрат тривимірних даних дає змогу отримати оригінальні вхідні дані з ущільнених даних, тоді як ущільнення об'ємних даних з втратами не може відновити вихідні дані. Однак, стиснення втраченого зображення дозволяє зберігати більшість деталей оригінального зображення, корисного для діагностики. Саме тому розроблений спосіб є способом ущільнення без втрат.

3.1.1. Тривимірне вейвлет-перетворення

Ідея модифікованого вейвлет-перетворенняє для тривимірних даних полягає в наступному: тримірні дані розкладаються в декілька блоків, з одним маленьким блоком, що містить більшу частину енергії та решту блоків, що містять інформацію в різних діапазонах частот. Розкладені об'ємні дані забезпечують чудове представлення для подальшого квантування та кодування. Розподілене вейвлет-перетворення тривимірних даних можна обчислити шляхом розширення одновимірного алгоритму. Оскільки набір слайсів медичних зображень можу мати різну товщину між слайсами, то співвідношення пікселів в межах слайсів, як правило, набагато краще, ніж між слайсами.

Алгоритм модифікованого вейвлет-перетворення для тривимірних даних використовує цю властивість за допомогою двох наборів вейвлет-фільтрів замість тільки одного вейвлет-фільтра [18]. Це являє собою координати X та Y у площині зображення та Z у напрямку слайсу, як показано на рис. 3.2.

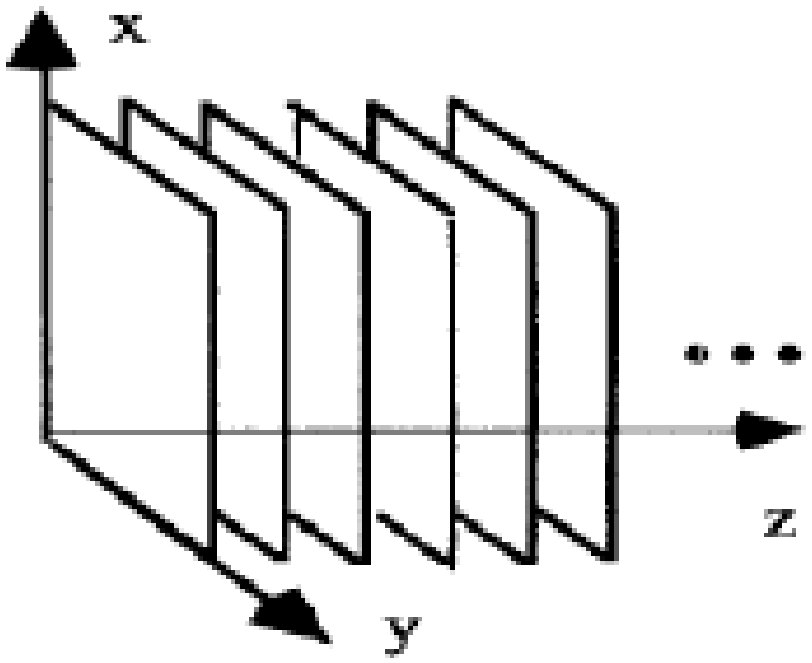


Рисунок 3.2 – Координати набору зображень з декількома слайсами.

Реалізація одного рівня тривимірного вейвлет-перетворення представлено на рис. 3.3. Кожен рядок в координатах *X* згортається за допомогою фільтрів H0 і H1, відповідно, з подальшою підвибіркою будь-якого іншого пікселя. Отримані сигнали потім згортаються з H0 і H1 у координатах *Y*, з наступним підвибіркою, після цього застосовується другий набір вейвлет-фільтрів H'0 і H'1 в *Z*-координатах з наступною підвибіркою.

Отриманий сигнал має вісім компонент f_{m+1}, містить низькочастотну інформацію, тому що вона отримана шляхом згортки з фільтрами низьких частот H0 і H'0.

Решта компонентів отримуються шляхом згортки з принаймні одним фільтром високих частот, H1 або H'1, і тому містять докладний сигнал у координатах *X, Y* та *Z* та різних діагональних напрямках. Той самий процес можна повторити для низькочастотного сигналу, f_{m+1}, доки не буде досягнутий бажаний рівень. H0, H1, H'0 та H'1 - два різні набори фільтрів [19].

На рис. 3.4 показано два рівня тривимірного вейвлет-перетворення об’ємних даних. Перший рівень розбиває дані на вісім блоків. Для кожного

блоку даних використовуються трибуквені мітки, які означають тип фільтра в напрямках *X*, *Y* та *Z*.

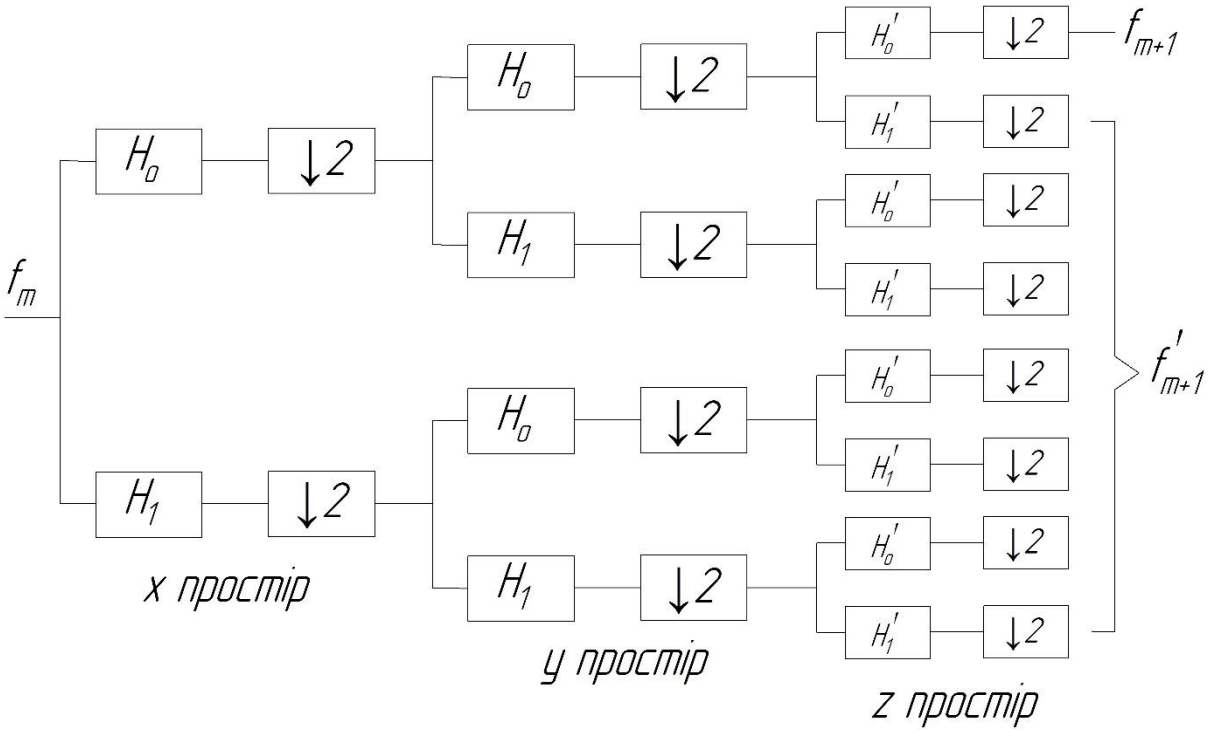


Рисунок 3.3 – Реалізація одного рівня вейвлет-перетворення тривимірних даних

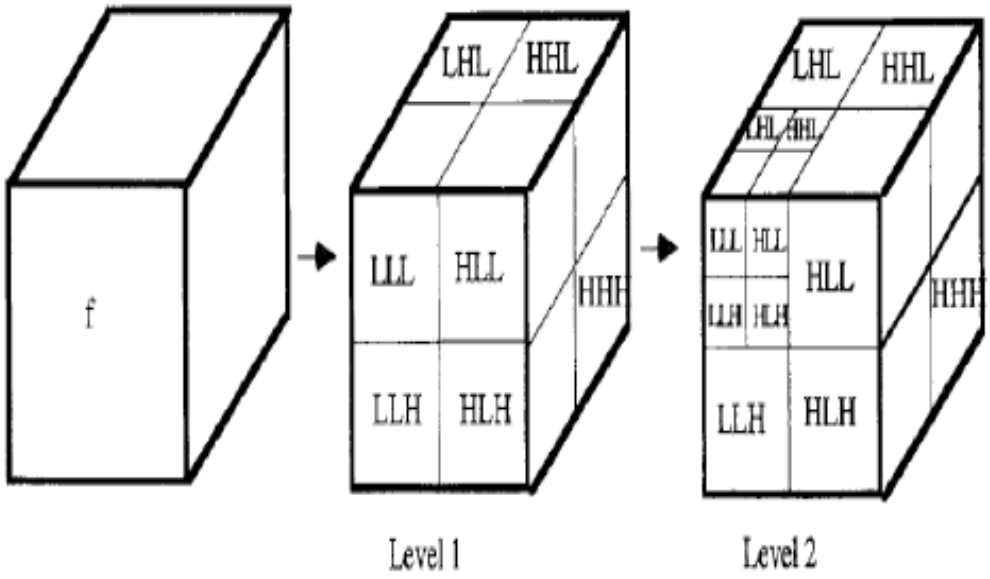


Рисунок 3.4 – Результат двох рівнів тривимірного вейвлет-перетворення двох.

L означає фільтр низьких частот, а H - фільтр високих частот. Верхній лівий кутовий блок - це частина з низькою частотою об’ємних даних, а інші

залишкові блоки фільтруються принаймні один раз з фільтром високих частот і тому містять компоненти високої частоти в одному з напрямків. Низькочастотний блок може бути додатково розбитий на вісім інших блоків. Блоки другого рівня містять більш високі частотні компоненти, ніж блоки першого рівня.

Як було зазначено раніше, модифіковане вейвлет-перетворення тривимірних даних розкладає тривимірні дані в декілька блоків, з одним маленьким блоком, що містить більшу частину енергії та решту блоків, що містять інформацію в різних діапазонах частот. Розкладене зображення забезпечує відмінне представлення для подальшого квантування та кодування. А модифіковане вейвлет-перетворення тривимірних даних можна обчислити шляхом розширення одновимірного пірамідального алгоритму. Набори медичних даних з декількома слайсами можуть мати різну товщину між слайсами. А кореляція між пікселями всередині слайсів, як правило, набагато краща, ніж між слайсами.

Другий шаг вейвлет-перетворення тривимірних даних – квантування.

Метою квантування є зниження ентропії даних за рахунок зниження точності даних. Зменшення ентропії дозволяє збільшити ущільнення. Крок квантування вказує велику кількість вхідних значень на менший набір вихідних значень. Шаг квантування відображає велику кількість вхідних значень в менший набір вихідних значень. Оригінальні дані не можуть бути відновлені відразу після квантування. Тому дуже важливо розробляти стратегію квантування, яка вибірково квантує вейвлет-коефіцієнти та зберігає якість оригінальних даних.

Вейвлет-перетворення даних представлено значеннями з плаваючою комою і складаються з двох типів даних: одного компонента з низьким дозволом, що містить більшу частину енергії; і кілька компонентів високої роздільної здатності, які містять інформацію про гострих краях. Оскільки компонент із низькою роздільною здатністю має більшу частину енергії, ці дані повинні зберігатись такими, якими є. Щоб мінімізувати втрату даних у

цій частині, кожне значення з плаваючою комою відображається, як найближче ціле число. Компоненти з високою роздільною здатністю містять в основному інформацію з високою частотою [20].

Оскільки гладкі області в оригінальних даних мають меншу частотну інформацію, компоненти з високою роздільною здатністю в цих областях переважно з невеликими коефіцієнтами амплітуди. Ці коефіцієнти містять дуже мало енергії. І можливо усунути ці коефіцієнти, не створюючи значні спотворення у відновлених оригінальних даних. Порогове число T_m вибирається так, щоб коефіцієнти, менші за T_m, були рівні нулю. Ti, що вище T_m використовуються однорідним скалярним квантуванням для відображення діапазону значень з плаваючою комою, як цілі числа.

3.2. Детальний опис запропонованого вейвлет-перетворення тривимірних даних та наступні кроки модифікованого способу ущільнення

Існує велика кількість методів вирішення проблеми втрат інформації медичних тривимірних даних під час ущільнення, підвищення рівня ущільнення, але кожен з них має власні переваги та недоліки.

Наприклад, дискретне косинусне перетворення (DCT) має такі недоліки.

1. Дуже добре підходить для відео- та аудіосигналів, але не підходить для медичних об’ємних даних, оскільки втрачається частина даних.
2. Розглядається лише просторова кореляція пікселів всередині одиночного 2-D блоку, і нехтується кореляція пікселів сусідніх блоків.
3. Неможливо повністю декорелювати межі блоків, використовуючи дискретне косинусне перетворення.

Розглядаючи ще один приклад, можна сказати, що ущільнення медичних тривимірних даних використовує цілочисельне вейвлет-

перетворення. Первинний широкосмуговий звуковий сигнал спочатку розкладається у вейвлет-піддіапазоні. Результуючі коефіцієнти повинні бути цілими, і вони можуть бути передані за допомогою адаптивного контекстного методу, без втрати даних, декодер, здатний відновити звукову форму сигналу. Недоліком цієї техніки є.

1. Він працює лише для аудіосигналів.
2. Зберігання та обробка даних призводить до більших витрат.

Після аналізу усі цих аспекти розроблено модифіковане вейвлет-перетворення для медичних зображень, які є тривимірними даними.

Запропоновано метод тривимірного (3-D) ущільнення медичного зображення для даних отриманих методами комп'ютерної томографії (CT) та магнітного резонансу (MP), який використовує модифіковане вейвлет-перетворення для тривимірних даних та ентропійне кодування.

Запропоноване вейвлет-перетворення тривимірних даних використовує, як вже було зазначено раніше, один фільтр в межах двовимірних (2-D) слайсів, а потім другий фільтр в напрямку нарізу. Необхідно зазначити, що набори зображень отриманих методами комп'ютерної томографії (CT) та магнітного резонансу (MP), як правило, мають різну роздільну здатність всередині слайса та між слайсами. Відстані пікселів в межах слайсів, як правило, менше 1 мм, а відстань між слайсами може коливатися від 1 мм до 10 мм.

Запропоноване модифіковане вейвлет-перетворення тривимірних даних має наступні переваги.

1. Висока якість зображення з високим показником пікового співвідношення сигналу до шуму (PSNR). Пікове співвідношення сигналу до шуму позначає співвідношення між максимумом можливого значення сигналу та потужністю шуму, що спотворює значення сигналу. Оскільки більшість сигналів мають широкий динамічний діапазон, PSNR зазвичай вимірюється логарифмічною шкалою в децибелах.
2. Швидке кодування та декодування.

3. Може використовуватись для ущільнення без втрат.

Модифіковане вейвлет-перетворення тривимірних даних повинно бути роздільним, саме тому воно буде здійснюватися у кожному просторі. Як і в оригінальному вейвлет-перетворені в основі розробленого будуть лежати дві функції.

1. Вейвлет-функція psi (ψ(t)), яка визначає деталі сигналу і породжує деталізуючи коефіцієнти.
2. Масштабуюча функція phi (φ(t)), яка визначає грубе наближення (апроксимацію) сигналу і породжує коефіцієнти апроксимації.

Вейвлет функція та функція масштабування (*Psi (x)* та *Phi (x)*) для вейвлет-перетворення тривимірних даних наведені нижче.

$$\varphi(x,y,z) = \varphi(x)\varphi(y)\varphi(z) \quad (3.1)$$

$$\psi 1(x,y,z) = \varphi(x)\varphi(y)\psi(z) \quad (3.2)$$

$$\psi 2(x,y,z) = \varphi(x)\psi(y)\varphi(z) \quad (3.3)$$

$$\psi 3(x,y,z) = \psi(x)\varphi(y)\varphi(z) \quad (3.4)$$

$$\psi 4(x,y,z) = \varphi(x)\psi(y)\psi(z) \quad (3.5)$$

$$\psi 5(x,y,z) = \psi(x)\varphi(y)\psi(z) \quad (3.6)$$

$$\psi 6(x,y,z) = \psi(x)\psi(y)\varphi(z) \quad (3.7)$$

$$\psi 7(x,y,z) = \psi(x)\psi(y)\psi(z) \quad (3.8)$$

Розроблене вейвлет-перетворення тривимірних даних виглядає як одновимірне вейвлет-перетворення у напрямках трьох координат (рис. 3.5).

Процес вейвлет-перетворення тривимірних даних виглядає наступним чином.

Першим йде процес перетворення даних на координатній прямі *X*. Далі отримані вихідні сигнали низького та високого рівнів, подаються на наступні

пари фільтрів, і йде перетворення даних на координатній прямій *Y*. Отримані чотири вихідні потоки йдуть до наступних чотирьох пар фільтрів, виконуючи остаточне перетворення на координатній прямій *Z*. Результатом процесу є отримання 8 потоків даних.

Апроксимований сигнал, який є результатом операцій масштабування, переходить до наступної октави тривимірного вейвлет-перетворення. Це приблизно 90% від загальної енергії. А 7 інших потоках містяться деталі сигналу.

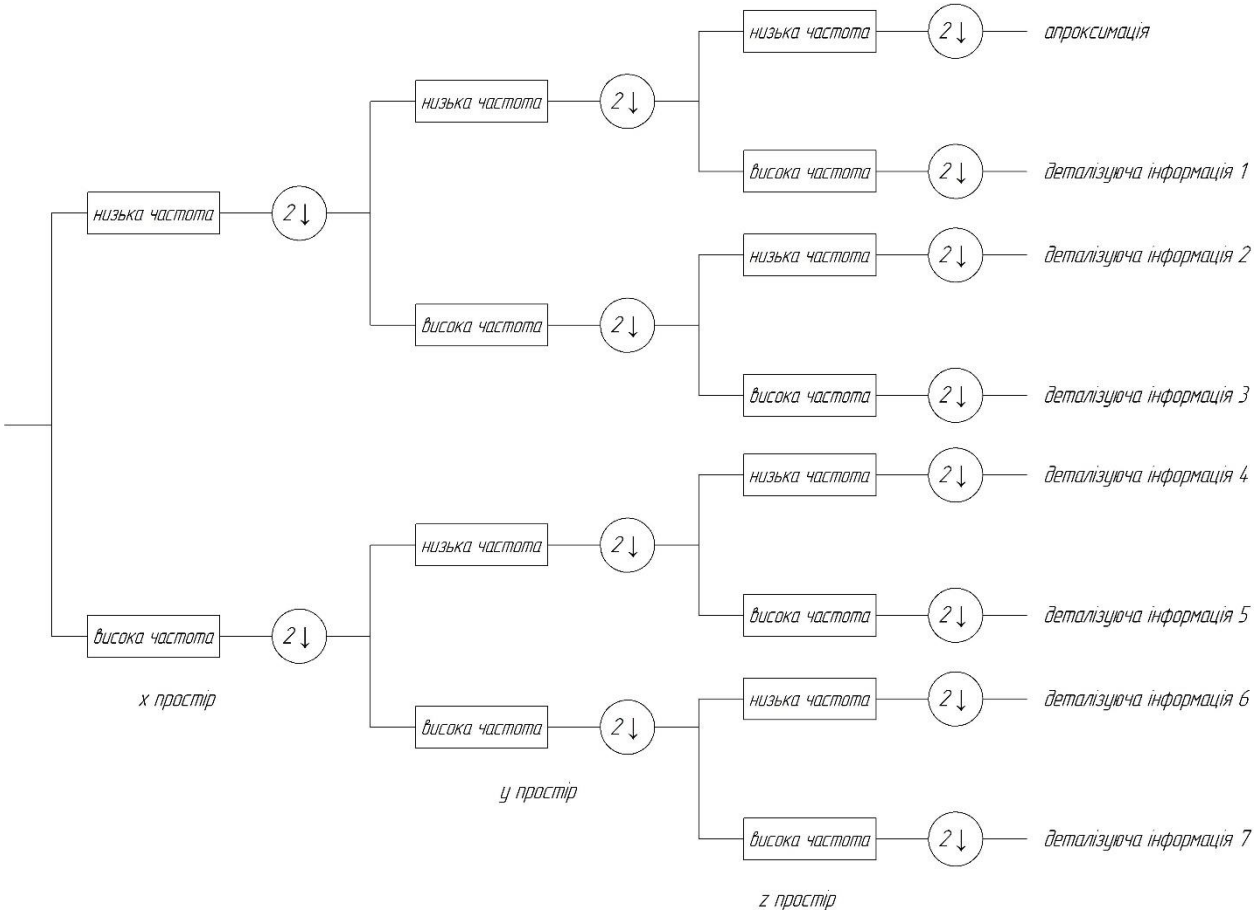


Рисунок 3.5 – Схема вейвлет-перетворення тривимірних даних

Концепція і реалізація тривимірного вейвлет-перетворення показано на рисунку 3.6, для нього 14 фільтрів. Проте фільтри в просторі *Y* можуть бути активні в два рази частіше, ніж фільтри простору *X*. Аналогічно, фільтри простору *Z* будуть чвертю від фільтрів простору *X*.

Процес роботи вейвлет-перетворення тривимірних даних продемонстровано на рис. 3.6, процес йде зліва на право. Після роботи вейвлет-перетворення вихідний розмір даних – 4x4x4.

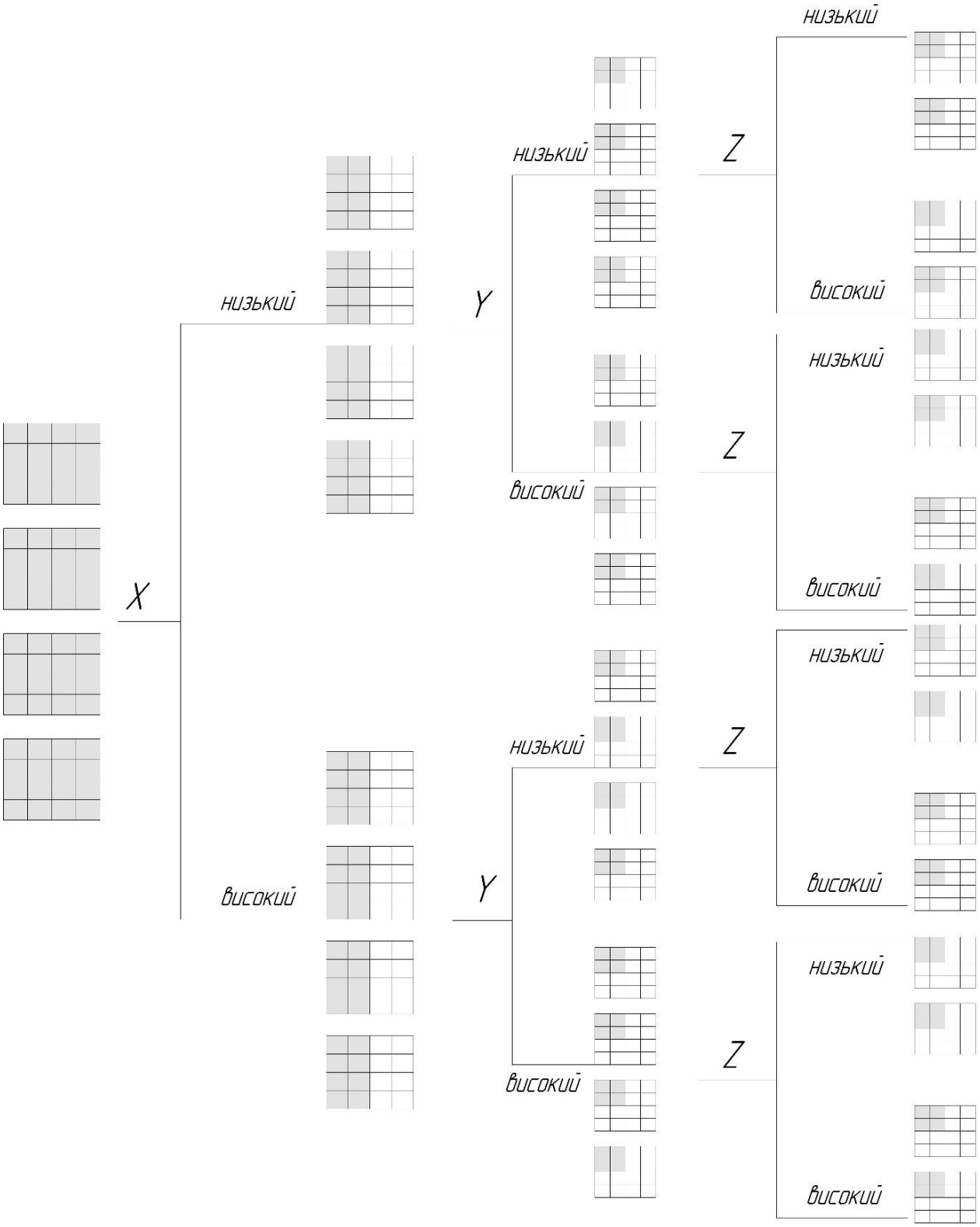


Рисунок 3.6 – Процес роботи запропонованого вейвлет-перетворення тривимірних даних

Вейвлет-перетворення тривимірних даних застосовується до значень пікселів, які зберігаються в текстовому файлі. Воно працює як звичайне одновимірне вейвлет-перетворення але в трьох просторах. Спочатку йде процес перетворювання даних у просторі *X*. Далі отримані вихідні низькочастотні та високочастотні сигнали подаються на наступні пари фільтрів, які перетворюють дані у просторі *Y*. Отримані чотири вихідні потоки сигналів йдуть до наступних чотирьох пар фільтрів, виконуючи остаточне перетворення в у просторі *Z*, цей процес продемонстровано на рис. 3.6.

Результатом усього процесу є 8 потоків даних. Апроксимований сигнал, який є результатом функції масштабування, переходить до наступної октави вейвлет-перетворення тривимірних даних. Це складає приблизно 90% від загальної енергії. Тим часом 7 інших потоків містять деталізуючи дані сигналів.

Вейвлет-перетворення тривимірних даних є дуже ефективною методикою для ущільнення медичних тривимірних зображень. Воно дає значно кращі результати, ніж стандартний алгоритм JPEG в порівнюванні з обчислювальною ефективністю. Стандартними кроками такого ущільнення є виконання дискретного вейвлет-перетворення (DWT), квантування отриманих вейвлет-коефіцієнтів і кодування квантованих коефіцієнтів. Ці коефіцієнти, як правило, кодуються растровую розгорткою.

Далі до отриманих вихідних потоків застосовується кодування Хаффмана.

Ущільнення методом Хаффмана – дає мінімальне кодування надмірності, а також потребує менше об’ємів обчислень. Воно призначає менше значення до бітів з більш високою частотою виникнення та більше значення до бітів з меншою частотою виникнення. Після першого визначення частоти появи кожного рівня сірого, кодування Хаффмана дозволить подати дані в меншому обсязі в порівнянні з оригінальними даними [19, 20].

Процедура кодування Хаффмана ґрунтується на двох основних підходах.

1. Символи, які більш часто зустрічаються мають коротші кодові слова, ніж символи, що зустрічаються рідше.
2. Два символи, що зустрічаються найменш часто, матимуть однакову довжину.

Ущільнення методом Хаффмана розроблено шляхом злиття найменших вірогідних символів, і цей процес повторюється, доки не залишиться тільки дві ймовірності двох складових символів. Таким чином, створюється дерево кодів і коди Хаффмана отримуються з маркування дерева кодів.

3.3. Оцінка результатів модифікованого способу ущільнення

3.3.1. Параметри оцінки модифікованого способу ущільнення

Неможливо загалом оцінити способи ущільнення. Для цього використовують деякі параметри. Будь-які способи ущільнення оцінюються за трьома наступними параметрами.

1. Пікове співвідношення сигналу до шуму (PSNR).
2. Коефіцієнт ущільнення.
3. Середньо-квадратична похибка (MSE).

Пікове співвідношення сигналу до шуму та середньо квадратична похибка.

Пікове співвідношення сигналу до шуму (PSNR) інженерний термін, який визначає співвідношення між максимальною можливістю сили сигналу та потужністю шуму, що впливає на вірність його подання. Пікове співвідношення сигналу до шуму найчастіше використовується як показник якості реконструкції кодеків ущільнення.

У випадку даної магістерської роботи, сигнал є оригінальним даними, а шум – це помилка, яка була введена шляхом ущільнення. При порівнянні

способів ущільнення показник пікового співвідношення сигналу до шуму використовується як наближення до сприйняття людей якості відновлення, тому в деяких випадках одна реконструкція може виявитися ближчою до оригіналу, ніж інша, навіть якщо вона має значення PSNR нижче. Загалом значення пікового співвідношення сигналу до шуму визначає значення якості віднровлення ущільнених даних.

Найчастіше цей показник можна визначити за допомогою середньо-квадратної похибки (MSE).

Середньо-квадратична похибка – сукупний квадратична похибка між ущільненими та оригінальними даними, тоді як пікове співвідношення сигналу до шуму – це показник пікової похибки.

Коли обидва зображення однакові, значення середньо-квадратичної похибки дорівнює нулю. Пікове співвідношення сигналу до шуму в такому випадку невизначене або дорівнює нескінченності.

Середньо-квадратична похибка визначається за формулою (3.9), а пікове співвідношення сигналу до шуму – (3.10).

$$MSE = \frac{1}{M*N}\sum\sum[I(x,y) - I'(x,y)], \tag{3.9}$$

де: *I(x, y)* є оригінальними даними, а *I '(x, y)* - це аппроксимована версія даних, *M* та *N* – розміри зображень.

$$PSNR = 20 * \log_{10}\frac{MAX_i}{\sqrt{MSE}}, \tag{3.10}$$

де MAX_i – це максимальне значення даних, яке приймається пікселем зображення. Для пікселів розярдності 8 біт, MAX_i дорівнює 255.

Невелике значення середньо-квадратичної похибки означає меншу помилку, і, як видно з зворотного зв'язку між *MSE* і *PSNR*, це означає, що у пікового значення сигналу до шуму буде велике значення. Логічно, що більш високе значення *PSNR* це добре, тому що це означає, що співвідношення сигналу до шуму вище.

У данні магістерській роботі сигналом є оригінальні об’ємні дані, а шум – це помилка, яка з’являється під час ущільнення. Отже, якщо спосіб ущільнення має низьке значення середньо квадратичної похибки та високе пікове значення сигналу до шуму, то це означає, що спосіб ущільнення є гарним та підходить для зменшення розмірів тривимірних даних.

Коефіцієнт ущільнення

Коефіцієнт ущільнення – це наступний основний показник, який використовується для оцінки ефективності способів ущільнення. Це термін, який використовується для кількісного визначення ущільнення оригінальних даних.

Коефіцієнт ущільнення даних визначається як відношення розміру оригінальних даних до розміру ущільнених даних (3.11).

$$k_{\text{ущ}} = \frac{I_0}{I_{\text{ущ}}} * 100\%, \qquad (3.11)$$

де: I_0 – розмір оригінальних даних, а $I_{ущ}$ – розмір даних після ущільнення.

Таким чином, якщо чим вище коефіцієнт ущільнення, тим спосіб ущільнення ефективніше. Також варто відмітити:

1. Якщо коефіцієнт ущільнення дорівнює 1, то ущільнення не було проведено. Тобто розмір ущільнених даних дорівнює розміру оригінальних даних.
2. Якщо коефіцієнт ущільнення менше 1, то розмір ущільнених даних більше ніж розмір оригінальних даних. Тобто було проведена неякісна робота.

3.3.2. Результати оцінки модифікованого способу ущільнення

Для оцінки роботи модифікованого способу ущільнення тривимірних даних було вирішено використовувати набір зображень з розширенням .dicom головного мозку, які були отримані методом комп’ютерної томографії. Один з слайсів продемонстровано на рис. 3.7.

Використаний набір зображень був завантажений з Інтернет ресурсу National Institutes of Health, де медичні зображення знаходяться в вільному доступі.

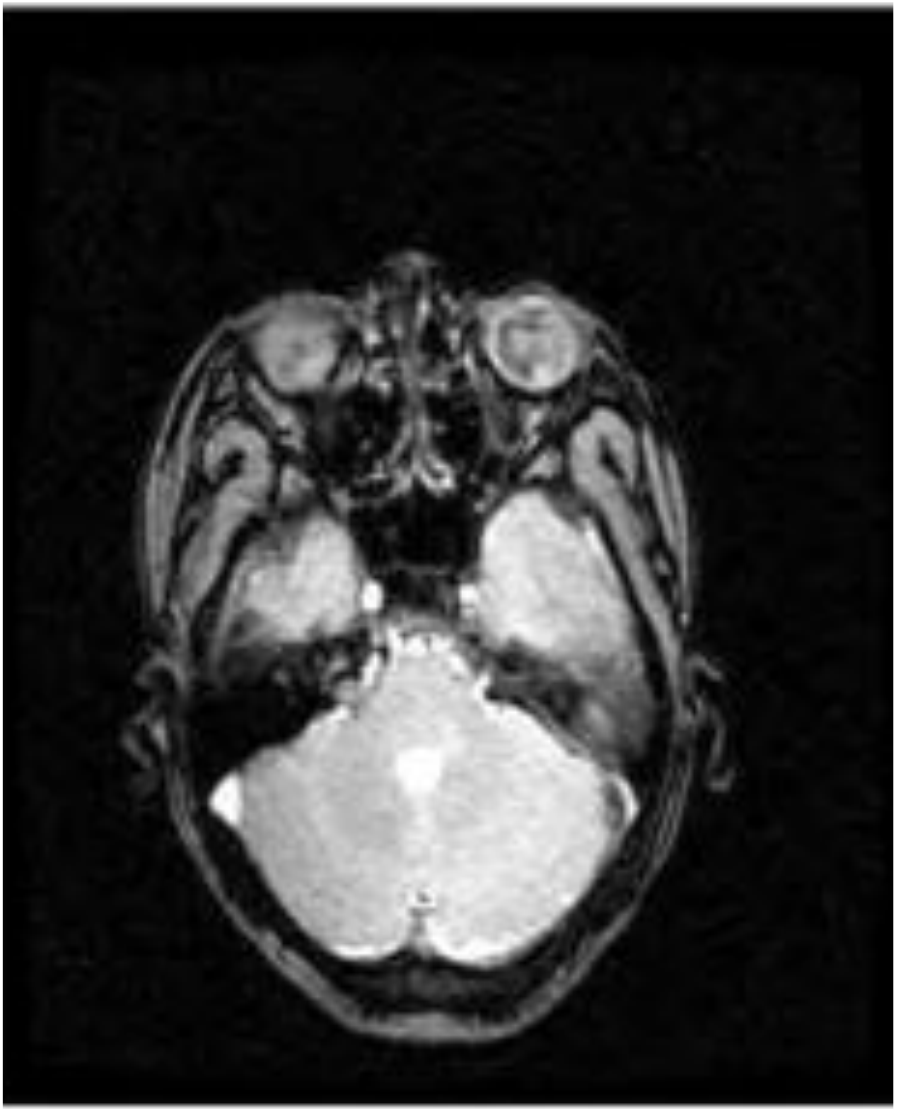


Рисунок 3.7 – Комп’ютерна томографія головного мозку

Розмір оригінальних тривимірних даних дорівнює 150 МБайт. Розширення зображення 512x512x300 з глибиною пікселей 12-16 байт на піксель.

У таблиці 3.1. наведено отримані результати. Оцінка роботи модифікованого способу ущільнення виконується за наступними показниками: пікове значення сигналу до шуму, середньо-квадратична

похибка, коефіцієнт ущільнення. У таблиці наведені отримані значення після процесу ущільнення.

Також було проведено ущільнення набору зображень з розширенням .dicom головного мозку, які були отримані методом магнітного резонансу. Один з слайсів продемонстровано на рис. 3.8.

Розмір оригінальних тривимірних даних дорівнює 100 МБайт. Розширення зображення 512x512x300 з глибиною пікселей 12-16 байт на піксель.

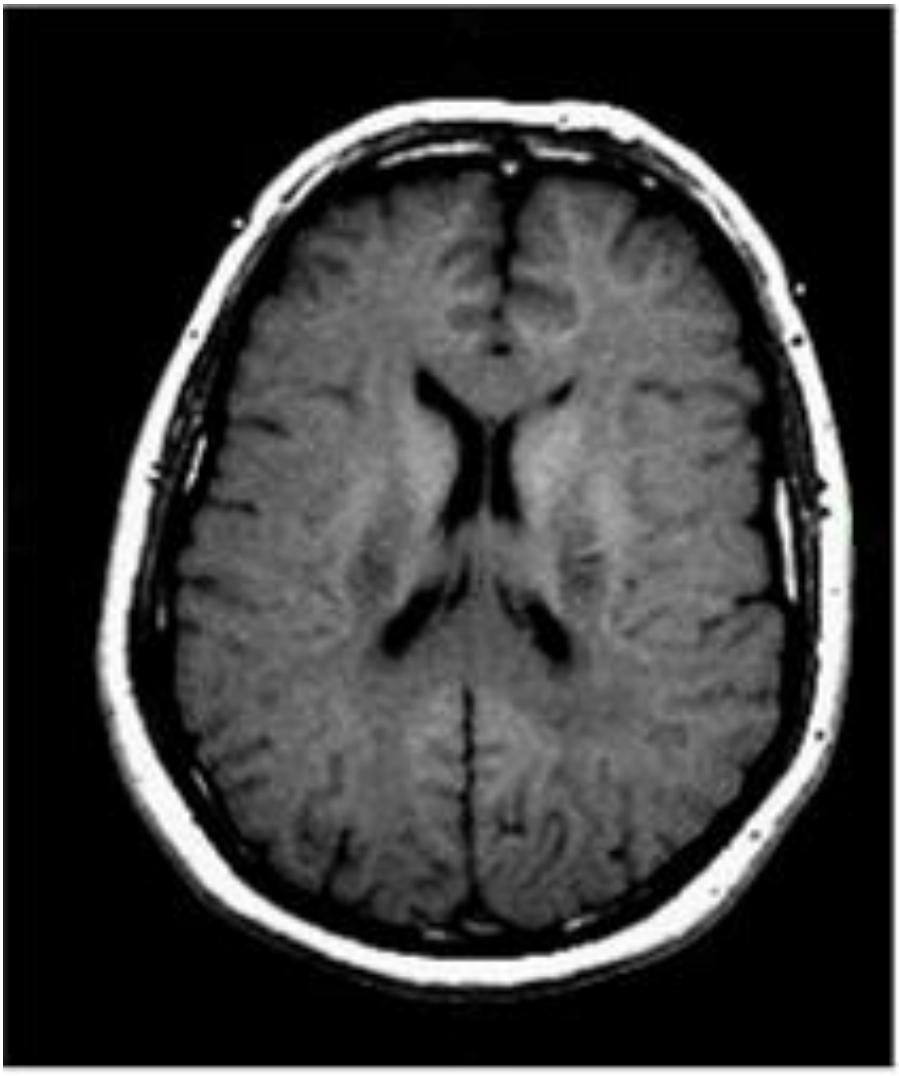


Рисунок 3.8 – Магнітний резонанс головного мозку

У таблиці 3.2. наведено отримані результати. Оцінка роботи модифікованого способу ущільнення виконується за наступними показниками: пікове значення сигналу до шуму, середньо-квадратична

похибка, коефіцієнт ущільнення. У таблиці наведені отримані значення після процесу ущільнення.

Таблиця 3.1 – Результат ущільнення CT-скану головного мозку модифікованим способом ущільнення

	CT-скан головного мозку
Пікове значення сигналу до шуму (ДБ)	39.56
Середньо-квадратична похибка (%)	7.19
Коефіцієнт ущільнення (%)	9.29

Таблиця 3.2 – Результат ущільнення MRI-скану головного мозку модифікованим способом ущільнення

	MRI-скан головного мозгу
Пікове значення сигналу до шуму (ДБ)	23.14
Середньо-квадратична похибка (%)	11.82
Коефіцієнт ущільнення (%)	10.36

3.4. Порівняння модифікованого способу ущільнення з існуючими алгоритмами ущільнення

Для порівняння отриманих результатів було обрано існуючі алгоритми JPEG200 та ROI.

JPEG 2000 — це спосіб ущільнення даних, при якому зображення описуються у всій сукупності, а не діляться на окремі блоки. JPEG 2000 може працювати з різною роздільною здатністю.

Основною метою алгоритму ущільнення ROI є ущільнення регіону інтересів з більш високою якістю ніж в порівнянні з іншим регіоном, який називається «Фон».

Результати цих алгоритмів наведено у таблиці 3.3 та таблиці 3.4. У таблицях наведені показники пікового значення сигналу до шуму, середньо-квадратичної похибки та коефіцієнта ущільнення.

Таблиця 3.3 – Результати роботи алгоритмів JPEG200 та ROI CT-скану головного мозку модифікованим способом ущільнення

	Коефіцієнт ущільнення (%)	Середньо-квадратична похибка (%)	Пікове значення сигналу до шуму (ДБ)
JPEG2000	10.35	29.09	33.49
ROI	15.69	21.16	34.88

Таблиця 3.4 – Результати роботи алгоритмів JPEG200 та ROI MRI-скану головного мозку модифікованим способом ущільнення

	Коефіцієнт ущільнення (%)	Середньо-квадратична похибка (%)	Пікове значення сигналу до шуму (ДБ)
JPEG2000	10.57	24.09	21.55
ROI	12.34	26.43	20.67

Як видно з наведених у таблиці результатів, ці алгоритми дають гарні результати. Але модифікований спосіб ущільнення має більш оптимальні значення по всім показникам.

Показник пікового значення сигналу до шуму вище в середньому на 6.07, а середньо-квадратична похибка нижче в середньому на 13.97 під час ущільнення CT-скану головного мозку. Та для ущільнення MRI-скану головного мозку показник пікового значення сигналу до шуму вище в середньому на 1.56, а середньо-квадратична похибка нижче в середньому на 12.27

Модифікований спосіб ущільнення великих обсягів даних має низький показник середньо-квадратичної похибки та високий показник пікове значення сигналу до шуму. Це означає, що спосіб ущільнення є оптимальним та підходить для зменшення розмірів тривимірних даних.

Висновки до розділу 3

Розроблено та проаналізовано модифікований способі ущільнення тривимірних даних.

Розроблений метод протестовано на наборі зображень головного мозку, отриманих методом комп’ютерної томографії та наборі зображень головного мозку отриманих методом магнітного резонансу. Запропонований модифікований способі ущільнення тривимірних даних дозволяє отримати показники пікового значення сигналу до шуму, яке дорівнює 39.56 ДБ, та середньо-квадратичної похибки, яка дорівнює 7.09 під час ущільнення CT-скану головного мозку, та для ущільнення MRI-скану головного мозку отримати показники пікового значення сигналу до шуму, яке дорівнює 23.14 ДБ, та середньо-квадратичної похибки, яка дорівнює 11.82.

У порівняння з існуючими алгоритмами він дає оптимальні показники (в середньому пікове значення сигналу до шуму вище на 6.07, а середньо-квадратична похибка нижче на 13.97 під час ущільнення CT-скану головного мозку, для ущільнення MRI-скану головного мозку показник пікового значення сигналу до шуму вище в середньому на 1.56, а середньо-квадратична похибка нижче в середньому на 12.27). Це доводить, що запропонований спосіб доречний при ущільнені тривимірних даних.

ВИСНОВКИ

У даній магістерській дисертації розглянута проблема надмірності даних та основні алгоритми ущільнення. Представлено варіанти зменшення розміру даних двома методами – з втратами та без втрат. Відомі алгоритми ущільнення, можуть використовуватися для ущільнення одномірних даних.

Розглянуто та проаналізовано основні існуючі алгоритми ущільнення даних. Розглянуто процес ущільнення різними варіантами алгоритмів, показані їх переваги та недоліки.

Проведене дослідження існуючих алгоритмів ущільнення показало, що для того, щоб блок даних, який зберігається, займав менший обсяг, необхідно елементи, які часто використовуються, заміняти короткими кодами, а ті, які рідко використовуються – довгими кодами.

Показано, що всі відомі алгоритми ущільнення на сьогоднішній день використовуються тільки для одномірних даних і не підходять для ущільнення тривимірних даних (особливо для медичних 3-D зображень), оскільки такі дані представлені у трьох площинах. Особливо важливо, щоб тривимірні дані були ущільнені без втрати якості.

Розглянуто та проаналізовано способи ущільнення двовимірних (2-D) даних з використанням вейвлет-перетворення.

Проаналізовано їх можливості для ущільнення тривимірних (3-D) даних. Показано, що в стандартному вигляді відомі підходи не можуть забезпечити якісного ущільнення. Тому постає актуальна задача ущільнення тривимірних (3-D) даних.

Розроблено та проаналізовано модифікований способі ущільнення тривимірних даних.

Розроблений метод протестовано на наборі зображень головного мозку, отриманих методом комп’ютерної томографії та наборі зображень головного мозку отриманих методом магнітного резонансу. Запропонований модифікований способі ущільнення тривимірних даних дозволяє отримати показники пікового значення сигналу до шуму, яке дорівнює 39.56 ДБ, та

середньо-квадратичної похибки, яка дорівнює 7.09 під час ущільнення CT-скану головного мозку, та для ущільнення MRI-скану головного мозку отримати показники пікового значення сигналу до шуму, яке дорівнює 23.14 ДБ, та середньо-квадратичної похибки, яка дорівнює 11.82.

У порівняння з існуючими алгоритмами він дає оптимальні показники (в середньому пікове значення сигналу до шуму вище на 6.07, а середньо-квадратична похибка нижче на 13.97 під час ущільнення CT-скану головного мозку, для ущільнення MRI-скану головного мозку показник пікового значення сигналу до шуму вище в середньому на 1.56, а середньо-квадратична похибка нижче в середньому на 12.27). Це доводить, що запропонований спосіб доречний при ущільнені тривимірних даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ватолин Д. П. Методы сжатия данных / Д. П. Ватолин, А. О. Ратушняк, М. М. Смирнов, В. А. Юкин – М.: ДИАЛОГ – МИФИ, 2002. – С. 384.

2. Mark Nelson «The Data Compression Book 2nd edition». – Wiley, 1995. – p. 576.

3. Andreas Uhl «Lecture Notes Compression Technologies and Multimedia Data Formats». – Department of Computer Sciences University of Salzburg, 2011. – p. 120.

4. Joe Celko «Complete Guide to NoSQL: What Every SQL Professional Needs to Know about Non-Relational Databases». – Morgan Kaufmann; 1 edition, 2013. – p. 244.

5. Shannon, C.E. «A Mathematical Theory of Communication», – Bell System Technical Journal 27, 1948. – p. 423.

6. Ayushi «Symmetric Key Cryptographic Algorithm», – International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15, 2010. – p. 4.

7. Taubman, David S. «W. JPEG 2000: Image Compression Fundamentals, Standards and Practice», – Kluwer Academic Publishers, 2001. – p. 776.

8. Moser, Robin A., «A constructive proof of the Lovász local lemma», STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing, New York: ACM, 2009. – p. 350.

9. Красильников Н.Н. Цифровая обработка 2D и 3D изображений – СПб: «БХВ-Петербург», 2011. – с. 602.

10. William A. «Digital Signal Compression: Principles and Practice», – Chapter 4 "Entropy coding techniques", 2010. – p. 76

11. Гонсалес Р., Вудс Р. Цифровая обработка изображений / Перев. с англ. — М.: Техносфера, 2006. — 1070 с.

12. Michel Misiti «Wavelets and their Applications», – First published in Great Britain and the United States in 2007 by ISTE Ltd, 2007. – p. 352.

13. Демьянович Ю.К. Введение в теорию вейвлетов Курс лекций Петербургский государственный университет путей сообщения / Ю.К. Демьянович, В.А. Ходаковский. – СПб, 2007. – с. 487.

14. Тропченко А.Ю. Методы сжатия изображений, аудиосигналов и видео / А.Ю. Тропченко, А.А. Тропченко. – Учебное пособие по дисциплине «Теоретическая информатика» Санкт-Петербург 2009. – с.105.

15. Xu, L. «Wavelet-based cascaded adaptive filter for removing baseline drift in pulse waveforms». IEEE Transactions on Biomedical Engineering. 52.11: 1973–1975. doi:10.1109/tbme.2005.856296, 2005. – p. 3.

16. K. K. Chan, «Three-dimensional transform compression of images from dynamic studies», – SPIE med. Image. IV: Image Capture and Display, vol.1232, 1990. – p. 326.

17. S. Lewis, «Image compression using the 2-D wavelet transform», – IEEE Trans. Image Process., vol. 1, no. 3, 1992. – p. 250.

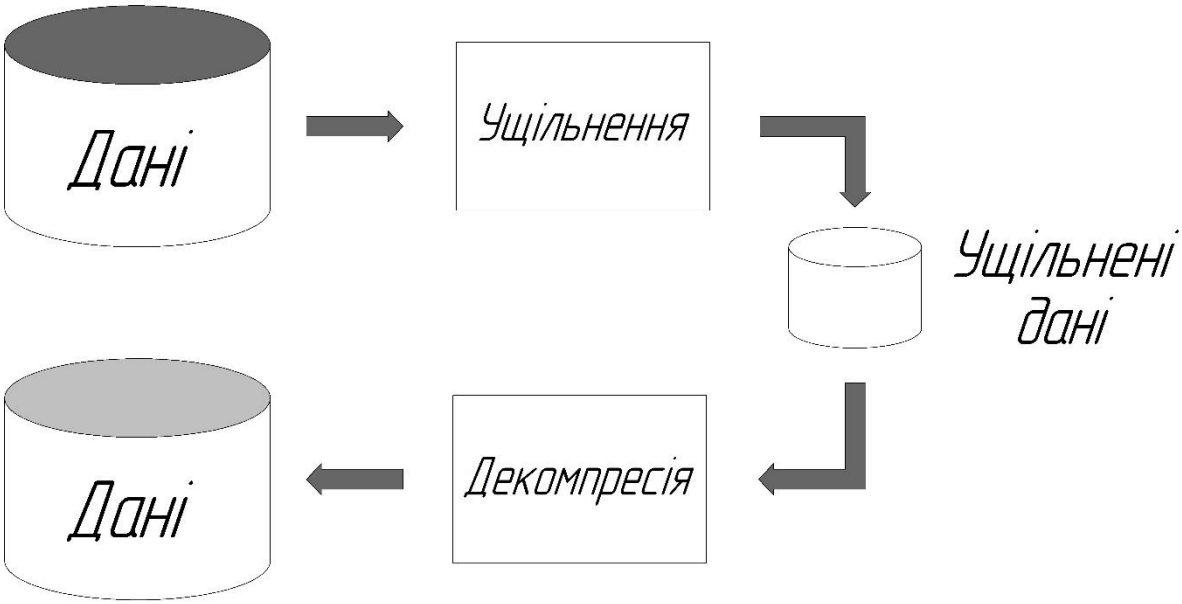
18. M. Ohta, «Wavelet picture coding with transform coding approach», – IEICE Trans. Fundamentals, vol. E75-A, no. 7, 1992. – p. 785.

19. T. Vijayaraghavan and K. Rajan, «Image coding of 3D volume using wavelet transform for fast retrieval of 2D images», – IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 4, 2006. – p. 5.

20. S.M.Ramesh, «Medical image compression using wavelet decomposition for prediction method», – (IJCSIS) Internationa Journal of Computer Science and Information Security, Vol. 7, No.1, 2010. – p. 4.

Додаток 1

Процес ущільнення даних

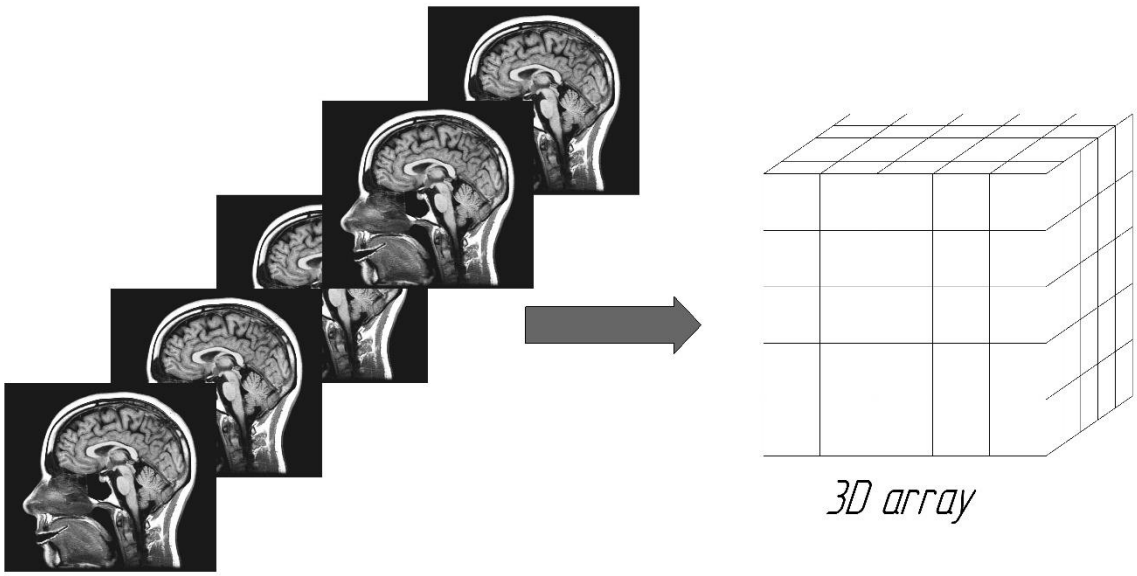


Щербакова Г.В.

Алгоритми ущільнення даних

Щербакова Г.В.

Представлення тривимірних даних у медицині



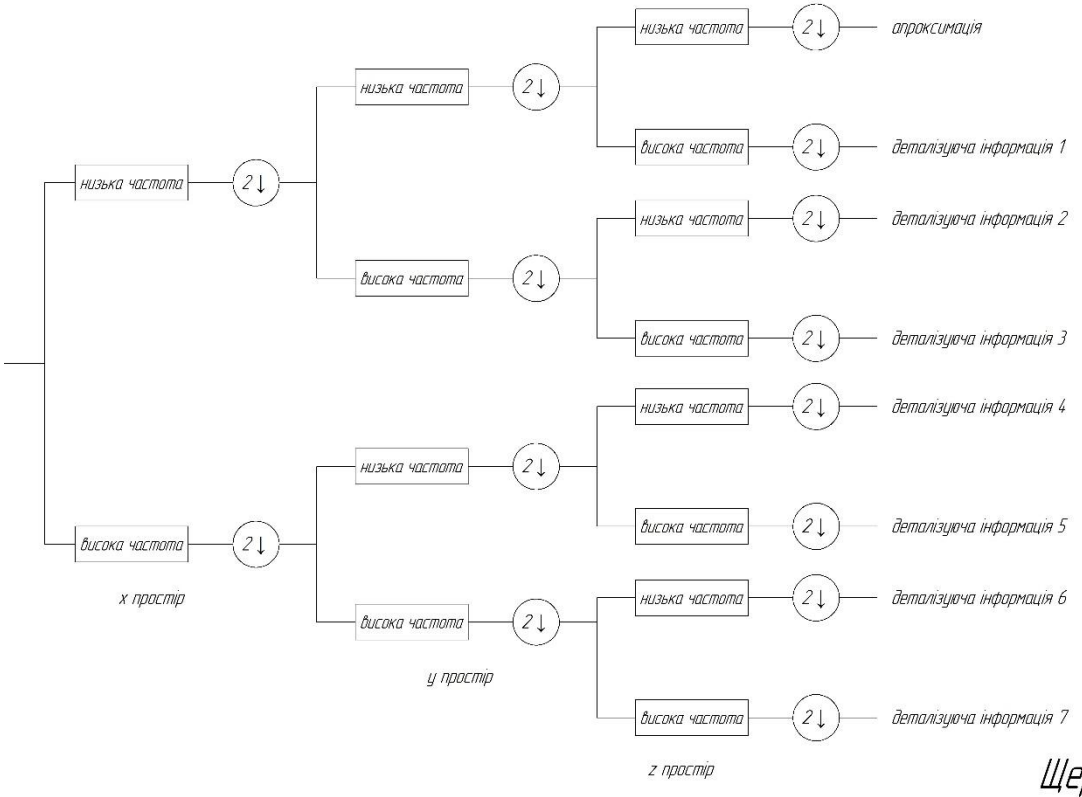
Nx2D Arraies

Щербакова Г.В.

Розроблений спосіб

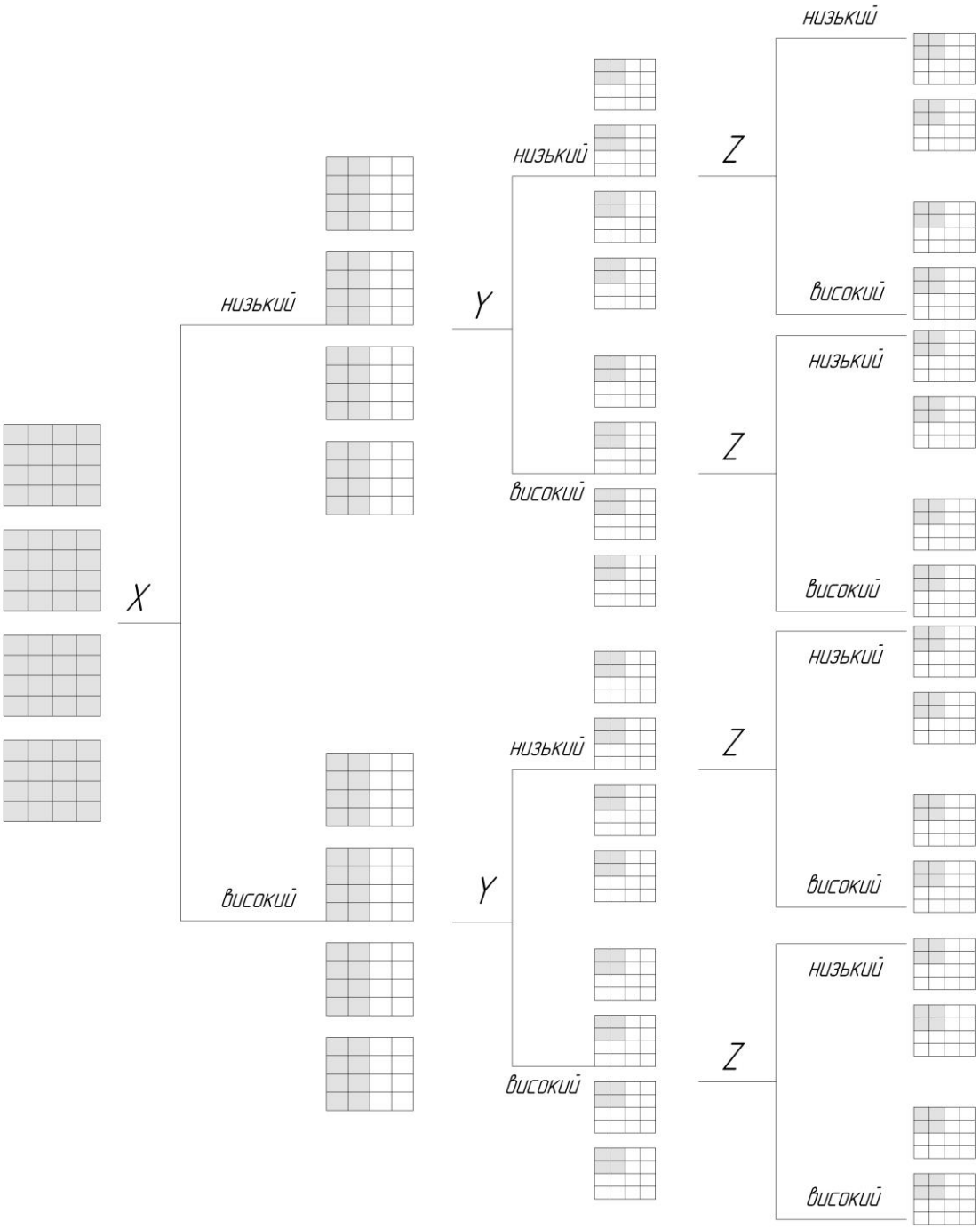
Щербакова Г.В.

Схема вейвлет-перетворення тривимірних даних



Щербакова Г.В.

Процес роботи вейвлет-перетворення тривимірних даних



Щербакова Г.В.

Додаток 2

ISSN 2520-2057

МІЖНАРОДНИЙ НАУКОВИЙ ЖУРНАЛ «ІНТЕРНАУКА»

INTERNATIONAL SCIETIFIC JOURNAL «INTERNAUKA»

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ «ИНТЕРНАУКА»

№ 7 (47) / 2018
2 том

Технічні науки

УДК 044.77

Орлова Марія Миколаївна

кандидат технічних наук, доцент кафедри

системного програмування і спеціалізованих комп'ютерних систем

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Орлова Мария Николаевна

кандидат технических наук, доцент кафедры

системного программирования и специализированных компьютерных стистем

Национальный технический университет Украины

«Киевский политехнический институт имени Игоря Сикорского»

Mariia Orlova

PhD, Assistant Professor of Department of

System Programming and Specialized Computer Systems

National Technical University of Ukraine

"Igor Sikorsky Kyiv Polytechnic Institute"

Щербакова Галина В'ячеславівна

магістрант

Національного технічного університету України

«Київський політехнічний інститут імені Ігоря Сікорського»

Щербакова Галина Вячеславовна

магистрант

Национального технического университета Украины

«Киевский политехнический институт имени Игоря Сикорского»

Shcherbakova Halyna

Student of the

National Technical University of Ukraine

"Igor Sikorsky Kyiv Polytechnic Institute"

МОДИФІКОВАНИЙ СПОСІБ УЩІЛЬНЕННЯ ВЕЛИКИХ ОБСЯГІВ ДАНИХ

МОДИФИЦИРОВАНИЙ СПОСОБ СЖАТИЯ БОЛЬШИХ ОБЪЕМОВ ДАННЫХ

MODIFIED METHOD OF VOLUMES DATA COMPRESSION

Анотація. *Проведено дослідження алгоритмів ущільнення без втрат та запропоновано модифікований спосіб ущільнення великих обсягів даних на основі отриманих результатів.*

Ключові слова: *алгоритм, ущільнення, спосіб, дані, вейвлет-перетворення, кодування.*

Аннотация. *Проведено исследование сжатия без потерь и предложено модифицированный способ сжатия больших объемов данных на основе полученных результатов.*

Ключевые слова: *алгоритм, сжатие, способ, данные, вейвлет-преобразование, кодирование.*

Summary. *The research lossless compression algorithms and proposed a modified method of volume data compression based on the results obtained.*

Key words: *algorithm, compression, method, data, wavelet transform, coding.*

Характерною особливістю більшості типів даних є їх надлишковість. При передачі та збереженні великих обсягів інформації надмірність відіграє негативну роль, оскільки вона не тільки призводить до збільшення часу передачі і функціональної надійності передачі інформації та її зберігання, а й до зростання сукупної вартості. В зв'язку з цим на сьогоднішній день для

забезпечення ефективності передачі великих обсягів інформації та зберігання широко використовуються алгоритми ущільнення.

Метою даної роботи є дослідження та алгоритмів ущільнення великих обсягів інформації без втрат та розробка на цій основі модифікованого способу ущільнення великих обсягів даних.

Ущільнення даних засновано на усунені надмірності інформації. В основі всіх методів ущільнення лежить проста ідея: якщо уявляти часто використовувані елементи короткими кодами, а рідко використовувані довгими кодами, то для зберігання блоку даних потрібно менший обсяг пам'яті, ніж якби всі елементи представлялися кодами однакової довжини [1, с.17; 3, с. 200].

Виходячи з вимог реконструкції, схеми ущільнення даних можна розділити на два широких класи: схеми ущільнення без втрат, в яких Y є ідентичним X, і схеми ущільнення з втратами, які зазвичай забезпечують набагато вище ущільнення, ніж ущільнення з втратами, але дозволяють Y бути різними з X [2, с.3-4].

Алгоритми ущільнення без втрат діляться на дві великі групи.

1. Потокові та словникові алгоритми. До них відносять алгоритми сімейств RLE (Run-Length Encoding), LZ (Lempel-Ziv).
2. Алгоритми статистичного (ентропійного) ущільнення. До алгоритмів цієї групи відносяться алгоритми Шеннона-Фанно та Хаффмана [4, с. 55].

Спочатку оригінальні дані знаходяться в просторовому обласному значенні, який потрібно перетворити в частотну область, щоб витягнути ознаки або значущу інформацію про дані. Таким чином, перед ущільненням будь-яких даних необхідно перетворити дані з часового домену до частотного домену. Для цього використовується дискретне вейвлет-перетворення для досягнення високої якості даних, а також кращої ефективності ущільнення [5, с. 26].

Однак, для тривимірних даних звичайне вейвлет-перетворення не підходить. Тому розроблено модифіковане вейвлет-перетворення тривимірних даних.

У цій роботі запропоновано модифікований спосіб ущільнення великих обсягів даних. Під великими обсягами даних розуміються тривимірні дані. Оцінка результатів роботи проводиться за наступними показниками: показниками: пікове значення сигналу до шуму, середньо-квадратична похибка, коефіцієнт ущільнення.

Модифікований спосіб ущільнення складається з двох етапів.

1. Вейвлет-перетворення тривимірних даних.
2. Ентропійне кодування.

Ідея модифікованого вейвлет-перетворенняє для тривимірних даних полягає в наступному: тривимірні дані розкладаються в декілька блоків, з одним маленьким блоком, що містить більшу частину енергії та решту блоків, що містять інформацію в різних діапазонах частот. Розкладені об’ємні дані забезпечують оптимальне представлення для подальшого квантування та кодування. Розподілене вейвлет-перетворення тривимірних даних можна обчислити шляхом розширення одновимірного алгоритму.

Реалізація одного рівня тривимірного вейвлет-перетворення представлено на рис. 1. Кожен рядок в координатах *X* згортається за допомогою фільтрів H0 і H1, відповідно, з подальшою підвибіркою будь-якого іншого пікселя. Отримані сигнали потім згортаються з H0 і H1 у координатах *Y*, з наступною підвибіркою, після цього застосовується другий набір вейвлет-фільтрів H'0 і H'1 в *Z*-координатах з наступною підвибіркою.

Решта компонентів отримуються шляхом згортки з принаймні одним фільтром високих частот, H1 або H'1, і тому містять докладний сигнал у координатах *X*, *Y* та *Z* та різних діагональних напрямках. Той самий процес можна повторити для низькочастотного сигналу, f_{m+1}, доки не буде досягнутий бажаний рівень. H0, H1, H'0 та H'1 - два різні набори фільтрів.

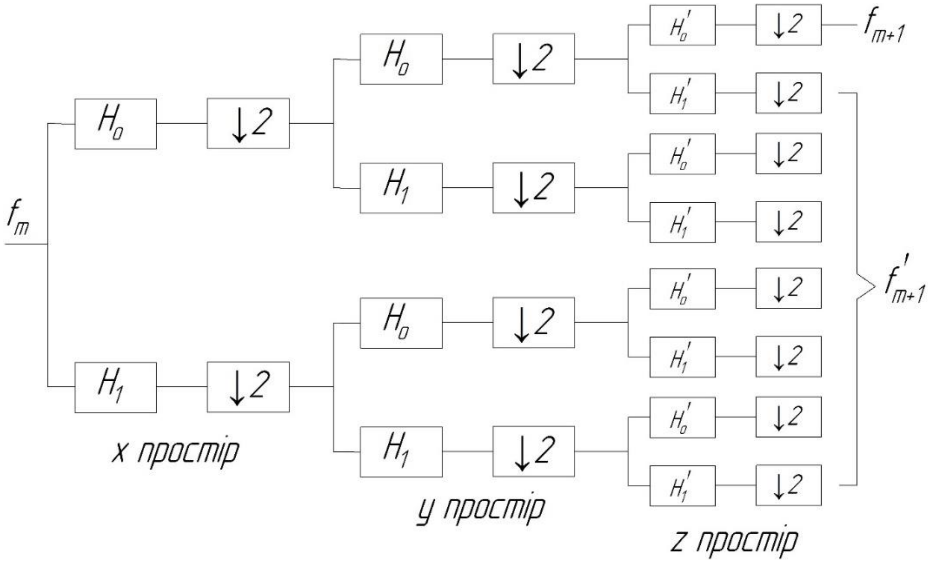


Рис. 1. Реалізація одного рівня вейвлет-перетворення тривимірних даних

Результатом усього процесу є 8 потоків даних. Апроксимований сигнал, який є результатом функції масштабування, переходить до наступної октави вейвлет-перетворення тривимырних даних. Це складає приблизно 90% від загальної енергії. Тим часом 7 інших потоків містять деталізуючи дані сигналів.

Далі до отриманих вихідних потоків застосовується кодування Хаффмана.

У таблиці 1 наведено отримані результати.

Таблиця 1

	СТ-скан головного мозгу
Пікове значення сигналу до шуму (ДБ)	39.56
Середньо-квадратична похибка (%)	7.19
Коефіцієнт ущільнення (%)	9.29

Представленій дані у таблиці показують, що запропонований спосіб дає низький показник середньо-квадратичної похибки та високий показник

пікового значення сигналу до шуму. Це означає, що спосіб ущільнення є оптимальним та підходить для зменшення розмірів тривимірних даних.

Таким чином, запропоновано новий модифікований спосіб ущільнення тривимірних даних. Представлений спосіб також може бути використаний для ущільнення кольорових зображень. Модифікований спосіб ущільнення в середньому дає покращений результат пікового значення сигналу до шуму на 6.07 ДБ, а середньо-квадратичної похибки на 13.97 %. Значить, він дає оптимальні показники.

Література

1. Ватолин В. Методы сжатия данных / В. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ – МИФИ, 2002. – с. 17.
2. Khalid Sayood “Introduction to Data Compression, Third Edition”, Series Editor, Edward A. Fox, Virginia Polytechnic University, 2005. - pp. 3-4.
3. Ватолин Д.С. Алгоритмы сжатия изображений. Методическое пособие. / Д.С. Ватолин. – М.: Издательство МГУ, 1999. – 200 с.
4. Зив Дж. Алгоритм универсального сжатия данных / Дж. Зив // Проблемы передачи информации. – 1996. – № 2. – С.55.
5. Michel Misiti “Wavelets and their Applications” First published in Great Britain and the United States in 2007 by ISTE Ltd. – pp. 26.

УДК 044.77

К.т.н., доцент Орлова М.М., студентка Щербакова Г.В.

Національний технічний університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

АНАЛІЗ АЛГОРИТМІВ СТИСНЕННЯ ВЕЛИКИХ ОБСЯГІВ ІНФОРМАЦІЇ БЕЗ ВТРАТ

Abstract

Maria Orlova, assoc. prof., PhD; Galina Shcherbakova, student
Lossless data compression algorithms for large amounts of information

A characteristic feature of most types of data is their redundancy. When it comes to storage and transmission of large amounts of information, redundancy plays a negative role, since it leads to an increase in the cost of storing and transmitting information. In this regard, there is always a problem of reducing the redundancy or compression of data.

Вступ

Характерною особливістю більшості типів даних є їх надлишковість. При зберіганні та передачі великих обсягів інформації надмірність відіграє негативну роль, оскільки вона призводить до зростання не тільки вартості зберігання, а й часу передачі інформації. В зв'язку з цим на сьогоднішній день для забезпечення ефективності зберігання, передачі великих обсягів інформації широко використовуються алгоритми стиснення.

Постановка проблеми

Метою роботи є дослідження та порівняння алгоритмів стиснення великих обсягів інформації без втрат та розробка модифікованої версії алгоритму на основі отриманих результатів.

Методи вирішення проблем

Стиснення даних засновано на усунені надмірності інформації. При виявлені у тексті повторень, надмірність усувається заміною повторювальної послідовності коротшим значенням чи кодом [1].

На поточний час існує велика кількість алгоритмів стиснення без втрат, які умовно можна розділити на дві великі групи.

4. Потокові і словникові алгоритми. До цієї групи належать алгоритми сімейств RLE (Run-Length Encoding), LZ (Lempel-Ziv). Особливістю всіх алгоритмів цієї групи є те, що при кодуванні використовується не

інформація про частоти символів в повідомленні, а інформація про послідовності, що зустрічалися раніше [2].

5. Алгоритми статистичного (ентропійного) стиснення. Ця група алгоритмів стискає інформацію, використовуючи нерівномірність частот, з якими різні символи зустрічаються в повідомленні. До алгоритмів цієї групи відносяться алгоритми арифметичного і префіксного кодування (з використанням дерев Шеннона-Фанно, Хаффмана, січних) [2].

Кодування довжин серій – це один з найпростіших і розповсюджених алгоритмів стиснення даних. У цьому алгоритмі послідовність символів, що повторюються замінюється символом і кількістю його повторів [3].

Група словникових алгоритмів, на відміну від алгоритмів групи RLE, кодує не кількість повторів символів, а послідовності, які раніше зустрічались. Під час роботи розглянутих алгоритмів динамічно створюється таблиця зі списком послідовностей, які вже зустрічалися, і відповідних їм кодів. Цю таблицю часто називають словником, а відповідну групу алгоритмів називають словниковими [3].

Алгоритм Шеннона-Фано – один з перших розроблених алгоритмів стиснення. В основі алгоритму лежить ідея представлення більш частих символів за допомогою більш коротких кодів. При цьому коди, отримані за допомогою алгоритму Шеннона-Фано, мають властивість префіксності: тобто жоден код не є початком будь-якого іншого коду. Властивість префіксності гарантує, що кодування буде взаємно-однозначним [3].

Алгоритм кодування Хаффмана також має властивість префіксності, а, крім того, доведеною мінімальною надмірністю, саме цим обумовлено його вкрай широке поширення. Для отримання кодів Хаффмана використовують наступний алгоритм.

1. Всі символи алфавіту представляються у вигляді вільних вузлів, при цьому вага вузла пропорційний частоті символу в повідомленні.
2. З безлічі вільних вузлів вибираються два вузла з мінімальною вагою і створюється новий (батьківський) вузол з вагою, рівною сумі ваг обраних вузлів.
3. Вибрані вузли видаляються зі списку вільних, а створений на їх основі батьківський вузол додається в цей список.
4. Кроки 2-3 повторюються до тих пір, поки в списку вільних більше одного вузла.
5. На основі побудованого дерева кожному символу алфавіту присвоюється префіксний код.
6. Повідомлення кодується отриманими кодами.

Порівняння алгоритмів стиснення

Існують різні критерії для вимірювання продуктивності алгоритмів стиснення. Одним з головних факторів є час та пропускна спроможність. Неможливо виміряти загальну ефективність алгоритмів,

оскільки поведінка стиснення залежить від об’єму інформації, продуктивність стиснення також залежить від типу даних [4].

У цій роботі будуть використовуватися наступні критерії для визначення ефективності алгоритмів стиснення без втрат.

1. Коефіцієнт стиснення: визначається, як відношення розміру стиснутого файл до розміру вхідного файлу.
2. Фактор стиснення: визначається, як відношення між розміром вхідного файлу та розміром стиснутого файлу.
3. Коефіцієнт збереження: він обчислює зменшення вихідного файлу у відсотках.

У таблиці 1 наведено порівняння алгоритмів.

Відповідно до отриманих результатів алгоритм кодування довжин серій має коефіцієнт стиснення більший за сто відсотків. Така ситуація виникає через наявність меншої кількості прогонів у джерелі, у результаті чого розмір стиснутого файлу майже не змінюється. Алгоритм LZ дає хороші коефіцієнти стиснення та збереження. Але він має значний недолік: при збільшені розміру файлу, збільшується розмір словника. Алгоритми Хаффмана и Шеннона-Фано показали найкращі результати.

Модифікована версія алгоритму

На основі отриманих результатів було вирішено розробити модифіковану версію алгоритму Хаффмана.

Отримана версія алгоритму буде працювати наступним чином.

1. Дані стискаються за допомогою динамічного методу зменшення біт.
2. Виявлення унікальних слів.
3. Використання кодування Хаффмана для отримання кінцевого результату.

Таблиця 1

Порівняння алгоритмів стиснення інформації

	RLE	LZ	Алгоритм Хаффмана	Алгоритм Шеннона-Фано
Розмір даних до стиснення (байт)	188 223	188 223	188 223	188 223
Коефіцієнт стиснення (%)	100.45	49.61	62.62	63.76
Коефіцієнт збереження (%)	0.45	50.39	42.24	40.51
Час стиснення (с)	344	517739	134281	15386

Висновки

Таким чином було проведено дослідження та порівняння чотирьох алгоритмів стиснення без втрат. Аналіз проведено за критеріями: коефіцієнт стиснення, час стиснення, коефіцієнт збереження. На основі цих показників можна зробити висновок, що алгоритми Шеннона-Фано та Хаффмана показали себе як найбільш ефективні. Значення показників цих алгоритмів потрапили в оптимальний діапазон. На основі отриманих результатів було запропоновано модифіковану версію алгоритму, яка дозволяє отримати покращені результати порівняно з існуючими алгоритмами.

Літератури

6. *Ватолин Д.С.* Алгоритмы сжатия изображений. Методическое пособие. / Д.С. Ватолин. – М.: Издательство МГУ, 1999. – 200 с.
7. *Д. Сэломон Д.* Сжатие данных, изображения и звука. / Д. Сэломон. — М.: Техносфера, 2004. — С. 368.
8. *Ватолин В.* Методы сжатия данных / В. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ – МИФИ, 2002. – 384 с.
9. *Зив Дж.* Алгоритм универсального сжатия данных / Дж. Зив // Проблемы передачи информации. – 1996. – № 2. – С.55.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Національний авіаційний університет
Навчально-науковий інститут комп'ютерних інформаційних технологій

CSNT 2018

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

XI Міжнародної науково-практичної конференції

КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ

19-21 квітня 2018 року

Київ 2018

Маковець О.С.
МЕТОД ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ ЗА ОЦІНКОЮ СКЛАДНОСТІ БІНАРНОГО КОДУ.....49

Орлова М.М., Щербакова Г.В.
ПОРІВНЯННЯ ТА АНАЛІЗ АЛГОРИТМІВ УЩІЛЬНЕННЯ ВЕЛИКИХ ОБСЯГІВ ДАНИХ.....51

Панасенко М.С., Тюрменко І.О., Боровик В.М.
СИСТЕМА ОБЛІКУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ СТУДЕНТІВ STUDFUTURE.....53

Пащенко Н.В., Самойліченко О.В.
РИЗИК-ОРІЄНТОВАНА ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ПРОЦЕСАМИ ЛАБОРАТОРІЇ.....55

Полухін А.В.
ПРО ВПЛИВ НА БЕЗПЕКУ ПОЛЬОТІВ ЗСУВУ ВІТРУ НА МАЛИХ ВИСОТАХ.....57

Рибасова Н.О.
ОСОБЛИВОСТІ ПРОЕКТУВАНЯ З SPARX ENTERPRISE ARCHITECT.....59

Русанова О.В., Корочкін О.В., Любарська Л.В.
СПОСІБ ПЛАНУВАННЯ ОБЧИСЛЕНЬ ДЛЯ ГЕТЕРОГЕННИХ МУЛЬТИЯДЕРНИХ КОМП'ЮТЕРНИХ СИСТЕМ.....61

Сидоров Є.О., Галата Л.П.
МЕТОД АНАЛІЗУ ТА КЛАСИФІКАЦІЇ SIEM СИСТЕМ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ.....63

Сінько Ю.І.
СТІЙКІСТЬ WINDOWS 10 ДО ШКІДЛИВОГО ПРОГРАМНО-МАТЕМАТИЧНОГО ВПЛИВУ.....66

Толстікова О.В., Ушаков К.С., Нестеренко А.О.
АГЕНТНИЙ ПІДХІД ДО МОДЕЛЮВАННЯ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ.....69

Трембовецька О.І.
МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ SOC.....71

УДК 004.77

М.М. Орлова, к.т.н.,
Г.В. Щербакова, студент,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ

ПОРІВНЯННЯ АЛГОРИТМІВ УЩІЛЬНЕННЯ БЕЗ ВТРАТ

Характерною особливістю більшості типів даних є їх надлишковість. При передачі та збереженні великих обсягів інформації надмірність відіграє негативну роль, оскільки вона не тільки призводить до збільшення часу передачі та її зберігання, а й до зростання сукупної вартості. В зв'язку з цим на сьогоднішній день для забезпечення ефективності передачі великих обсягів інформації широко використовуються алгоритми ущільнення.

Метою роботи є дослідження та аналітичне порівняння алгоритмів ущільнення великих обсягів інформації та розробка модифікованої версії алгоритму на основі отриманих результатів.

На поточний час алгоритми ущільнення без втрат, умовно можна розділити на дві великі групи.

6. Потокові і словникові алгоритми. До цієї групи належать алгоритми сімейств RLE (Run-Length Encoding), LZ (Lempel-Ziv). Особливістю всіх алгоритмів цієї групи є те, що при кодуванні використовується інформація про послідовності, що зустрічалися раніше [1].

7. Алгоритми статистичного (ентропійного) ущільнення. Ця група алгоритмів стискає інформацію, використовуючи нерівномірність частот, з якими різні символи зустрічаються в повідомленні. До алгоритмів цієї групи відносяться алгоритми Шеннона-Фанно та Хаффмана [1].

У цій роботі представлено аналітичне порівняння чотирьох алгоритмів: RLE, LZ, Шеннона-Фанно та Хаффмана. Для порівняння будуть використовуватися наступні критерії: коефіцієнт ущільнення та коефіцієнт збереження.

У таблиці 1 наведено порівняння алгоритмів.

Таблиця 1

Порівняння алгоритмів ущільнення інформації

	RLE	LZ	Алгоритм Хаффмана	Алгоритм Шеннона-Фано
Розмір оригінальних даних (байт)	188 223	188 223	188 223	188 223
Коефіцієнт ущільнення (%)	100.45	49.61	62.62	63.76
Коефіцієнт збереження (%)	0.45	50.39	42.24	40.51

Відповідно до отриманих результатів алгоритми Хаффмана и Шеннона-Фано показали найкращі результати.

На основі отриманих результатів було вирішено розробити модифікований спосіб алгоритму Хаффмана.

Отримана версія алгоритму буде працювати наступним чином.

4. Дані стискаються за допомогою динамічного методу зменшення біт.
5. Виявлення унікальних слів.
6. Використання кодування Хаффмана для отримання кінцевого результату.

Дослідження показали, що в середньому досягається збільшення коефіцієнту збереження на 11%.

Таким чином було проведено дослідження та порівняння чотирьох алгоритмів ущільнення без втрат. Алгоритм Хаффмана показав себе як найбільш ефективні. На основі отриманих результатів було запропоновано модифіковану версію алгоритму, яка дозволяє отримати покращені результати порівняно з існуючими алгоритмами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Ватолин Д.С. Алгоритмы сжатия изображений. Методическое пособие. / Д.С. Ватолин. – М.: Издательство МГУ, 1999. – 200 с*

УДК 004.738

К.т.н., доцент Орлова М.М., студент Щербакова Г.В.
Національний технічний університет України
«Київський політехнічний інститут»

Алгоритми шифрування у комп’ютерних мережах

Abstract

Marija Orlova, assoc. prof., PhD; Galina Shcherbakova, student

Encryption algorithms in computer networks

This paper concerns the protection task of computer network. There were researched and analyzed symmetric and asymmetric algorithms of encryption. After that we could conclude advantages and disadvantages.

Вступ

Задачі захисту комп’ютерних мереж мають велике значення. Під захистом інформації розуміють комплекс дій, які проводять з метою запобігання витоку, крадіжки, втрати, несанкціонованого знищення, спотворення, підробки, копіювання інформації та використання ресурсів комп’ютерної мережі. Через небезпеку несанкціонованого втручання зовнішніх зловмисників у роботу організацій, необхідно забезпечити захист комп’ютерної мережі. Для цього потрібно використовувати комплексний підхід.

Один з методів захисту – шифрування. Розглянемо його у цій статті більш детально, а саме криптографічні методи та їх застосування в даній області.

Постановка задачі

Метою роботи є дослідження та аналіз методів захисту ресурсів комп’ютерної мережі за допомогою алгоритмів шифрування, розглянути та порівняти основні алгоритми, та виділити переваги і недоліки.

Термінологія

Шифрування – це процес перетворення відкритої інформації в закриту чи зашифровану. Це перетворення виконується за спеціальними математичними алгоритмами, в них крім даних бере участь додатковий елемент – «ключ».

Розшифрування – процес перетворення закритої інформації в відкриту чи розшифровану.

Ключ – це унікальний елемент, що дозволяє зашифрувати інформацію таким чином, щоб отримати відкриту інформацію за закритої може тільки певний користувач чи група користувачів, які мають на це право [1].

Опис алгоритму

Для захисту інформації, що передається у комп'ютерній мережі, існують наступні криптографічні методи:

1. Шифрування інформації;
2. Електронний цифровий підпис (ЕЦП).

Шифрування та розшифрування виражаються відповідно наступним формулами:

$$C = Ek_1(M)$$

$$M' = Dk_2(C),$$

де: функція Е виконує шифрування інформації; D – розшифрування; k_1,k_2 – криптографічні ключі відповідно для шифрування та дешифрування; М – інформація, яка буде шифруватися; М´- змінена інформація.

В такому разі, якщо ключ k_2 відповідає ключу k_1, який був використаний при шифруванні, вдається отримати відкриту інформацію, тобто отримати відповідність М´ = М.

Якщо відповідний k_2 – відсутній, то отримати розшифроване повідомлення практично неможливо [2].

Існують наступні алгоритми шифрування:

1. Симетричне шифрування: коли $k_1 = k_2$. Під час процесу шифрування та розшифрування використовується один і той же криптографічний ключ. Ключ такого алгоритму повинен триматися у таємниці обома сторонами, а сам алгоритм шифрування обирається ще до початку обміну повідомленням. Загальній приклад представлений на рис. 1.

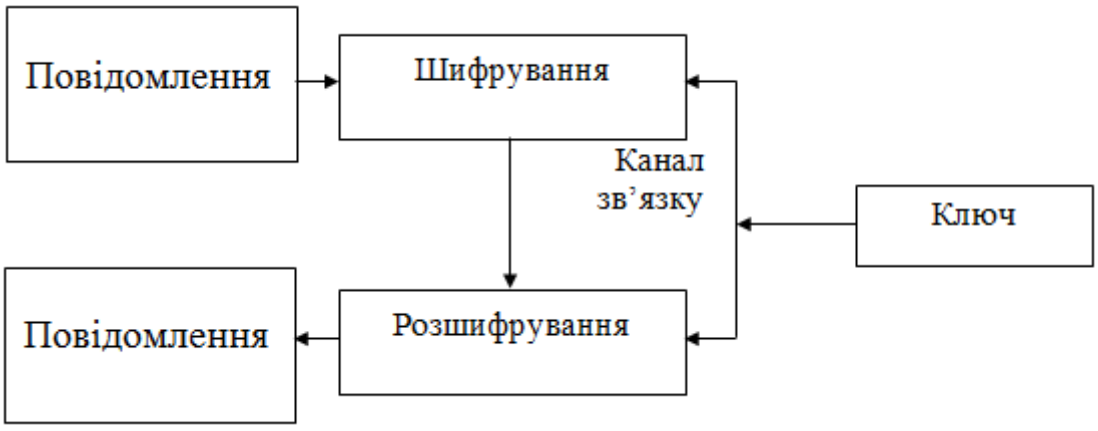


Рис. 1. Загальний приклад симетричного шифрування та розшифрування

2. Асиметричне шифрування: коли k_1 – «відкритий», а k_2 – «таємний». В такому разі криптографічний ключ k_1, відомий усім користувачам, передається відкритим каналом зв'язку, а ключ k_2 повинен не

розголошуватися, та використовуватися для розшифрування. Загальний приклад асиметричного алгоритму представлений на рис. 2.

Рис. 2. Загальний приклад асиметричного алгоритму шифрування

Криптографічні ключі повинні бути випадковими, інакше зловмисник буде мати змогу визначити значення ключа [3].

Порівняємо симетричний та асиметричний алгоритми шифрування:

1. Переваги симетричного шифрування полягають в тому, що у них більша швидкодія, вони більш прості у реалізації, мають меншу довжину ключа і вже більш вивчені.
2. Переваги асиметричних алгоритмів у тому, що не треба передавати таємний ключ по приватному каналу, не має необхідності у більшій кількості ключем, як у симетричних.

Симетричні алгоритми діляться на блочні та потокові шифри. Серед блочних найвідоміші AES – американський стандарт шифрування, DES – стандарт шифрування в США, IDEA – міжнародний алгоритм шифрування даних. До потокових відносяться RC4 – алгоритм з ключем змінної довжини, SEAL – програмно-ефективний алгоритм, WAKE – всесвітній алгоритм на автоматичному ключі.

Серед асиметричних алгоритмів існують таки: RSA – алгоритм, який базується на обчислювальній складності задачі факторизації великих цілих чисел, DSA – алгоритм з використанням відкритого ключа для створення електронного підпису, але не для шифрування, Elgamal – шифросистема Ель-Гамаля та інші.

При написанні цих алгоритмів на якійсь об'єктно-орієнтованій мові програмування майже існують стандартні бібліотеки.

Так, наприклад, у мові програмування Java, є пакети стандартних бібліотек javax.crypto, java.security. У собі вони містять вже готові алгоритми шифрування, генератори ключей, шифрувальники та дешифрувальники.

Ключ генеруються наступною конструкцією:

```
SecretKey key =
 KeyGenerator.getInstance("Назва_Алгоритму").generateKey().
```

Приклад функції шифрування виглядає наступним чином:

```
String encrypt(String str) throws UnsupportedEncodingException,
IllegalBlockSizeException, BadPaddingException {
byte[] utf8 = str.getBytes("UTF8");
byte[] enc = ecipher.doFinal(utf8);
return new sun.misc.BASE64Encoder().encode(enc); }
```

Порівняння симетричного та асиметричного алгоритмів

Для порівняння використовується криптографічний пакет OpenSSL. Для цього необхідно створити пару відкритий-таємний ключ, далі створити необхідну кількість файлів різного розміру. Для порівняння було створено 7 файлів. Їх розміри у діапазоні від 100 MB до 1000 MB. Наступним кроком буде запуск симетричного та асиметричного алгоритмів. Після цього, використовуючи утиліту gnuplot, можна побудувати графік (рис. 3).

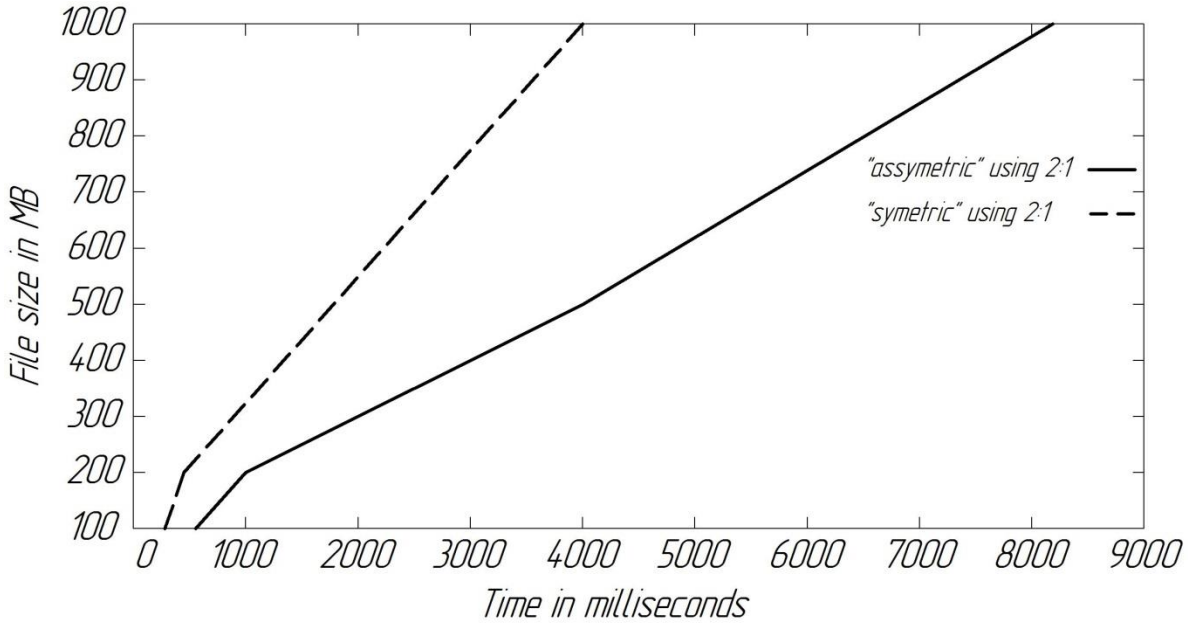


Рис. 3. Графік залежності розміру фалу від часу під час шифрування

З цього графіку можна зробити висновок, що симетричне шифрування займає менше часу ніж асиметричне.

Висновки

Звичайно, за допомогою самого тільки шифрування неможливо захистити мережу. Але воно є необхідною складовою. Саме тому до цього питання необхідно підійти з усією уважністю.

При порівняні асиметричного алгоритму з симетричним можна сказати, що в асиметричних системах проходить вже більш складне шифрування. Кодуються дані відкритим криптографічних ключем, а декодуються – таємним. І користувач може спокійно розповсюджувати свій відкритий ключ, не боячись, що його дані зможе прочитати стороння людина.

Такий алгоритм має більші переваги у використанні.

Література

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2002. — 816 с.
2. *К. Шеннон.* Теория связи в секретных системах // Работы по теории информации и кибернетике – М.: ИЛ, 1963. — С. 243-322. — 830 с.
3. *Гатчин Ю.А., Коробейников А.Г.* Основы криптографических алгоритмов. Учебное пособие - СПб.: СПбГИТМО(ТУ), 2002.

IX Міжнародна науково-технічна конференція «Комп’ютерні системи та мережні технології»

УДК 004.738

Г.В. Щербакова *(НТУУ "КПІ", Україна)*

Порівняння способів шифрування у комп’ютерних мережах

У сьогоденні проблема захисту ресурсів комп’ютерних мереж має велике значення. Одним з необхідних, але не єдиним, методом захисту є шифрування. Воно існує двох типів – симетричне та асиметричне. Метою цієї роботи є порівняння цих двох методів та виявлення переваг і недоліків.

При симетричному шифруванні використовується один ключ. За допомогою ключа проводиться як шифрування, так і розшифрування. Ключ повинен залишатися у таємниці. Цей метод також називають методологією з таємним ключем [1].

При асиметричному шифруванні створюються два взаємопов'язаних асиметричних ключа. Один повинен бути безпечно переданий його власнику, а інший - тій особі, яка відповідає за зберігання цих ключів, до початку їх використання. Незважаючи на те, що ключі створюються разом, вони різні [2]. У таблиці 1 наведено порівняння симетричного та асиметричного методів шифрування.

Таблиця 1

Показник	Симетричний метод	Асиметричний метод
Ключі	Один ключ, використовується двома, або більше, користувачами	Один відкритий ключ, інший – таємний, який відповідає відкритому
Обмін ключами	Захищеним каналом	Відкритий ключ передається загальнодоступним каналом, а таємний зберігає власник не розголошуючи
Швидкість	Метод шифрування має меншу складність, а тому швидкий	Метод складний, а тому повільний
Спосіб використання	Комплексне шифрування (шифрування файлів та комунікаційних каналів)	Розповсюдження ключів та цифровий підпис

Порівняльний аналіз алгоритмів шифрування показує, що асиметричне шифрування передбачає більш складні процедури, що призводить до значних часових затрат. Симетричне шифрування призводить до значно менших витрат часу, що особливо відчутно при збільшенні об’єму переданих даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2002. — 816 с.

2. Гатчин Ю.А.Основы криптографических алгоритмов. Учебное пособие / Коробейников А.Г. - СПб.: СПбГИТМО(ТУ), 2002. – 29 с.