УДК: 004.056 **DOI 10.33111/mise.103.16**

Серденко Т. В.,
к. фіз. — мат.н., доцент кафедри системного аналізу та кібербезпеки,
КНЕУ ім. В. Гетьмана
Ляшко К. О.,
студентка за освітньо-професійною програмою «Кібербезпека» ННІ
«Інститут нформаційних технологій в економіці»,
КНЕУ ім. В. Гетьмана

Serdenko T. V.,
candidate of Physical and Mathematical Sciences,
Associate Professor of Department of Systems Analysis and Cybersecurity,
KNEU named after V. Hetman
Liashko K. O.,
student of the educational and professional program «Cybersecurity» Institute of Information Technologies in Economics,
KNEU named after V. Hetman

КОДУВАННЯ СИГНАЛІВ НА ОСНОВІ ВЕЙВЛЕТ-АНАЛІЗУ

SIGNAL CODING BASED ON WAWELET ANALYSIS

Анотація. *Стаття присвячена аналізу застосування вейвлет-перетворень у кодуванні сигналів і зображень. Вейвлети визначаються як потужний інструмент у багатьох технічних і наукових дисциплінах, здатний ефективно виділяти й обробляти характеристики сигналу на різних рівнях роздільної здатності. У статті наголошується на значенні вейвлетів у шифруванні зображень і сигналів, зокрема щодо оптимізації часу шифрування та забезпечення захисту від різних атак. У сучасному світі цифровий зв'язок і обробка даних набувають неймовірного значення, вейвлет-аналіз є ключем до успіху в багатьох технічних і наукових дисциплінах. У цій статті про вейвлет-аналіз розглядається значення та застосування вейвлет-аналізу в кодуванні сигналу. Розглянуто історію вейвлет-аналізу, його математичні основи, а також сучасні методи та технології, які використовують цей аналіз для вдосконалення та оптимізації процесів кодування. Цінність вейвлетів у кодуванні сигналу полягає в їх здатності ефективно виділяти та обробляти характеристики сигналу на різних рівнях роздільної здатності. Ця універсальність робить вейвлети надзвичайно корисними в широкому діапазоні застосувань, від стиснення зображень і відео до криптографічного шифрування та обробки медичних сигналів. У цій статті розглядаються різні способи, за допомогою яких вейвлет-перетворення можуть покращити кодування сигналу, забезпечуючи більшу ефективність і безпеку в різноманітних програмах, забезпечує глибше розуміння ролі вейвлет-аналізу в сучасному кодуванні сигналу. Інноваційний підхід до шифрування, який поєднує вейвлет-перетворення Хаара і «золоті» матриці, відкриває нові можливості в криптографічному захисті цифрових сигналів. У статті розглянуто різні підходи до вибору та застосування вейвлетів для конкретних завдань обробки сигналів, підкреслено їх математичні власти-*

вості та практичну ефективність. Цінність вейвлетів у шифруванні зображень і сигналів виражається в необхідності оптимізації часу шифрування та забезпечення захисту від різних атак. Сучасні методи вейвлет-кодування потребують додаткового вдосконалення для вирішення задачі обробки різних типів сигналів з урахуванням шуму, зміни частоти та інших складнощів.
Ключові слова: *аналіз сигналу, вейвлет-перетворення, криптографія, стиснення зображення, цифровий сигнал.*

Abstract. *The article focuses on the analysis of the application of wavelet transforms in signal and image encoding. Wavelets are defined as a powerful tool in numerous technical and scientific disciplines, capable of effectively highlighting and processing signal characteristics at various levels of resolution. The article emphasizes the significance of wavelets in the encryption of images and signals, particularly regarding optimization of the encryption time and providing protection against various attacks. In today's world, digital communication and data processing are gaining incredible importance, wavelet analysis is the key to success in numerous technical and scientific disciplines. This wavelet analysis article considers the meaning and application of wavelet analysis in signal coding. The history of wavelet analysis, its mathematical foundations, as well as modern methods and technologies that use this analysis to improve and optimize coding processes are considered. The value of wavelets in signal coding lies in their ability to efficiently extract and process signal characteristics at different levels of resolution. This versatility makes wavelets extremely useful in a wide range of applications, from image and video compression to cryptographic encryption and medical signal processing. This article examines the various ways in which wavelet transforms can improve signal coding, providing greater efficiency and security in a variety of applications, provides a deeper understanding of the role of wavelet analysis in modern signal coding. An innovative approach to encryption, which combines the Haar wavelet transform and «golden» matrices, opens up new possibilities in the cryptographic protection of digital signals. The article considers various approaches to the selection and application of wavelets for specific signal processing tasks, emphasizing their mathematical properties and practical effectiveness. The value of wavelets in the encryption of images and signals is reflected in the need to optimize encryption time and ensure protection against various attacks. Modern methods of wavelet coding need additional improvement to solve the task of processing different types of signals taking into account noise, frequency changes and other complexities.*
Keywords: *Signal analysis, wavelet transform, cryptography, image compression, digital signal.*

Вступ. У сучасному світі, де цифрова комунікація та обробка даних набувають неймовірної ваги, вейвлет-аналіз відіграє ключову роль у численних технічних та наукових дисциплінах. Від теорії обробки сигналів до практичного застосування в цифровому кодуванні та шифруванні, вейвлети надають потужний інструментарій для ефективного аналізу та представлення сигналів. Ця стаття вейвлет-аналізу розкриває значення та застосування вейвлет-аналізу у кодуванні сигналів. Розглядається історію вейвлет-аналізу, його математичні основи, а також сучасні методи та технології, що використовують цей аналіз для покращення та оптимізації процесів кодування.

Значення вейвлетів у кодуванні сигналів полягає в їх здатності ефективно виділяти та обробляти характеристики сигналів на різних рівнях роздільної здатності. Ця універсальність робить вейвлети надзвичайно корисними в широкому спектрі застосувань, від стиснення зображень та відео до криптографічного шифрування та обробки медичних сигналів [8]. У цій статті розглядаються різні способи, якими вейвлет-перетворення можуть покращувати кодування сигналів, забезпечуючи більшу ефективність і безпеку в різних випадках.

Постановка проблеми. Вейвлет-аналіз відіграє значну роль у кодуванні сигналів, але зіштовхується з рядом викликів у різних сферах цифрової обробки даних. Від шифрування ЕКГ сигналів до обробки зображень і захисту конфіденційної інформації, потреба в ефективному кодуванні залишається важливою, але водночас складною задачею [1-9].

Значення вейвлетів у шифруванні зображень та сигналів відображається в необхідності оптимізації часу шифрування та забезпечення захисту від різноманітних атак. Сучасні методики вейвлет-кодування потребують додаткового вдосконалення, щоб вирішувати завдання обробки різних типів сигналів з урахуванням шумів, зміни частоти та інших складнощів.

Поряд з цим, важливим є вибір оптимального вейвлета для конкретного типу сигналу, з огляду на їх характерні особливості у часовому та частотному просторах. Вибір вейвлетів є вирішальним, оскільки невірний вибір може призвести до несподіваних результатів у аналізі та обробці сигналів. Проблема ускладнюється тим, що дослідження вейвлетів часто обмежується вивченням їх математичних властивостей, без зосередження на практичному застосуванні у конкретних сценаріях обробки сигналів.

Важливість інтерпретації результатів, отриманих вейвлет-перетворенням, не може бути недооцінена, оскільки вона дозволяє розуміти взаємозв'язок між вейвлет-спектрограмами та характеристиками сигналу [8]. Аналіз чутливості вейвлет-перетворень до різних параметрів сигналів є ключовим для забезпечення точності та надійності при їх обробці.

Враховуючи ці виклики, завданням статті є аналіз різноманітні аспекти вейвлет-аналізу та його застосування у кодуванні сигналів, з акцентом на вибір оптимальних вейвлетів для конкретних сигналів та забезпечення їх ефективної обробки та безпеки.

Метою статті є аналіз та оцінка вейвлет-аналізу як фундаментального інструменту в кодуванні сигналів. Розглянуто як теоретичні аспекти вейвлет-перетворень, так і їх практичне застосу-

вання в різних областях, таких як цифрове шифрування, обробка медичних сигналів, стиснення зображень та відео.

Ця стаття має на меті виявити та розглянути ключові виклики та обмеження існуючих методів вейвлет-кодування, зокрема в контексті обробки різноманітних типів сигналів та забезпечення безпеки у шифруванні. Проаналізовано різні підходи до вибору та застосування вейвлетів для конкретних задач обробки сигналів, включаючи врахування їх математичних властивостей та практичної ефективності.

Ця стаття покликана надати читачам розуміння ролі вейвлет-аналізу у сучасному кодуванні сигналів та вказати на шляхи подальшого вдосконалення в цій області.

Виклад основного матеріалу. Вейвлет-аналіз став незамінним інструментом у обробці сигналів завдяки своїй унікальній здатності одночасно видобувати часову та частотну інформацію з сигналів. Ця характеристика робить його особливо корисним у різноманітних областях, від аналізу електроенергії до обробки медичних зображень.

Вейвлет-перетворення може бути неперервним (CWT) або дискретним (DWT). Неперервне вейвлет-перетворення (CWT) особливо придатне для аналізу гармонік у сигналах через його здатність зберігати інформацію про фазу сигналу. Ця особливість дозволяє детально аналізувати локальні особливості сигналу, такі як раптові зміни або нестабільності [9].

Вейвлет-перетворення сигналу f(t) визначається через інтегральне перетворення, де вейвлет-функція ψ(t),служить як основа для перетворення. Формула вейвлет-перетворення виглядає так:

$$W_f(u,s) = \int_{-\infty}^{+\infty} f(t)\frac{1}{\sqrt{s}}\psi * (\frac{t-u}{s})dt,$$

де ψ*(t) є комплексно-спряженою вейвлет-функцією, s — параметр розтягнення (масштаб), а u — параметр зсуву (положення) [9].

Вейвлет-функція має задовольняти певним математичним критеріям: вона має мати скінченну енергію і середнє значення, що дорівнює нулю. Остання умова означає, що вейвлет не містить компоненту нульової частоти.

У розглянутому у статті [9] алгоритмі для гармонічного аналізу використовується спрощений комплексний вейвлет Морле (CMW):

$$\psi(\mathrm{sf}) = \sqrt{s}e^{-\pi^2 f_b(sf-f_c)^2},$$

який є, по суті, модульованою гауссівською функцією. Він добре підходить для гармонічного аналізу через свою гладкість та хвильоподібну форму. CMW дозволяє окремо аналізувати амплітуду та фазу сигналу. Його середнє значення можна зробити дуже малим, обираючи відповідні параметри f_b і f_c, що робить його практично придатним для аналізу.

Вейвлет-аналіз, завдяки своїй здатності ефективно аналізувати сигнали в часово-частотному просторі, відкриває широкі можливості для досліджень та практичного використання в різних галузях науки та техніки.

Детекція гармонік є значущим завданням у сфері обробки сигналів, особливо в контексті криптографічних алгоритмів, де точність є критичною. У цьому контексті, вейвлет-перетворення, особливо з використанням Max-Plus алгебри, пропонують ефективний підхід. Вейвлет-перетворення включає два основних процеси: аналіз та синтез. Під час аналізу сигнал з високою роздільною здатністю розкладається на складові наближення та деталізації, де наближення представляє сигнал у нижчій роздільній здатності, а деталізація допомагає відновити даний сигнал у процесі синтезу. Max-Plus алгебра, яка використовує операції максимізації та додавання над множиною дійсних чисел, стала важливою у таких застосуваннях, як криптографія та вейвлет-перетворення. Ця алгебра допомогла створити вейвлет-перетворення, засновані на Max-Plus алгебрі (MP-Wavelets), які характеризуються ефективністю обчислень та відсутністю проблем з округленням [3].

У криптографії вейвлет-перетворення на основі Max-Plus алгебри використовуються для шифрування та дешифрування. Процес шифрування включає перетворення початкового тексту в послідовність ASCII кодів, яка потім обробляється за допомогою вейвлет-аналізу. Після визначення ключа шифрування проводиться аналіз вейвлетів, який включає кодування деталізованих сигналів у бінарний формат. Зашифрований текст (Ciphertext) представляє собою послідовність ASCII кодів, яка визначається як наближення сигналу на рівні m і абсолютні значення деталізованих сигналів, доданих до нього [3].

Процес дешифрування полягає у перетворенні зашифрованого тексту назад у вихідний текст. Це досягається шляхом використання ключа дешифрування, який складається з ключа шифрування та бінарного кодування деталей сигналу. Потім виконується синтез вейвлетів для відновлення початкового сигналу. Використання вейвлет-перетворень на основі Max-Plus алгебри в

криптографії демонструє важливість та ефективність цих методів у детекції та обробці гармонік сигналів. Цей підхід відіграє ключову роль у забезпеченні безпеки та надійності у застосуваннях в області криптографії.

Ефективність, простота обчислень та відсутність проблем з округленням роблять MP-Wavelets особливо привабливими для сучасних криптографічних рішень, відкриваючи шлях для розвитку нових та більш ефективних методів шифрування та дешифрування.

У сфері шифрування сигналів та зображень вейвлет-перетворення та алгоритм перестановок виявилися ефективним інструментом. Використовуючи дискретне вейвлет-перетворення (DWT), можна аналізувати характерні особливості сигналів і зображень, після чого застосовувати алгоритм перестановок для їх шифрування.

Квантизація відіграє важливу роль у стисненні зображень, оскільки вона дозволяє представити безперервний ряд значень за допомогою обмеженого, зазвичай малого, обсягу інформації. Цей процес передбачає втрату деякої частини інформації, що призводить до використання так званих процедур «lossy coding», які спрямовані на зменшення обсягу даних, необхідних для зберігання зображення. При цьому важливо підтримувати прийнятний баланс між якістю зображення та його розміром.

Щоб усунути кореляції між пікселями, використовують ортогональне лінійне перетворення, відоме як трансформація Карунена-Лоева або трансформація Хотеллінга. Таке перетворення дозволяє отримати некорельовані компоненти зображення, що сприяє ефективному кодуванню та подальшій обробці цифрових зображень, що практично показано у статті [2].

Основна ідея методу полягає у тому, щоб не шифрувати весь сигнал чи зображення, а спочатку аналізувати їх за допомогою вейвлет-перетворення, а потім застосовувати алгоритм перестановок до отриманих коефіцієнтів, що дозволяє зменшити розмір даних, які потребують шифрування, і відповідно, знижує обчислювальне навантаження. Цей підхід сприяє покращенню ефективності шифрування, одночасно забезпечуючи надійний захист інформації [1].

Вейвлет-перетворення Хаара [4] є першим відомим видом вейвлетів, який був запропонований у 1909 році Альфредом Хааром. Вейвлет-перетворення Хаара має ряд переваг: простота, швидкість, ефективне використання пам’яті, оскільки можна проводити обчислення без тимчасового масиву.

Новаторський підхід до шифрування, який об'єднує вейвлет-перетворення Haar і «золоті» матриці, відкриває нові можливості у криптографічному захисті цифрових сигналів. Haar wavelet transform відрізняється простотою, швидкістю та ефективністю використання пам'яті, оскільки ця трансформація може бути виконана без використання тимчасових масивів (temporary arrays). Процес шифрування включає кілька етапів: спочатку дані піддаються стисненню, потім оброблюються за допомогою адаптивного коду Гаффмана, який видаляє зайві дані, зменшує розмір даних. Техніка MAC (Message Authentication Code) створює цифровий підпис схеми для надання конфіденційності та цілісності інформації. У цій схемі цифровий підпис спочатку створюється шляхом обчислення MAC стислого повідомлення, а потім підписується відправником за допомогою приватного ключа, створеного будь-яким алгоритмом шифрування. Нарешті, підписаний MAC і шифр відправляються в кіберпростір. На боці отримувача після розшифрування цифровий підпис зі стислого повідомлення може бути використаний для перевірки цілісності повідомлення та аутентифікації відправника, а потім вже розпакувати повідомлення, щоб отримати початкові дані. Запропонована криптосистема [4] має високі властивості розсіювання (confusion) та перемішування (diffusion), вона має високий рівень безпеки і підходить для забезпечення безпеки комунікацій.

Вейвлет-аналіз являє собою потужний та універсальний математичний інструмент, що має широке застосування у різних галузях науки та техніки. Стаття [5] оглядає історію розвитку теорії вейвлетів, методи їх побудови, обговорення властивостей вейвлетів та зосереджується на перевагах раціонального вейвлет-перетворення (RWT — Rational Wavelet Transformation). Також обговорюються комбінації вейвлет-теорії та нейронних мереж, охоплюючи еволюцію вейвлетних нейронних мереж (WNN — Wavelet Neural Network), їх системну архітектуру та реалізацію алгоритмів. Дискретне вейвлет-перетворення (DWT — Discrete Wavelet Transformation) є найбільш базовим і широко використовується методом вейвлетного аналізу. Наприклад, RWT може досягти більшої точності в частотному домені. Це покращує локалізацію частот в сигналі та є потужним інструментом обробки сигналів. З розвитком нейронних мереж також активно розвивається поєднання нейронних мереж і вейвлетного аналізу. WNN, сигнал якого передається попередньо обробленим вейвлетним аналізом, поєднує переваги штучних нейронних мереж та вейвлетного аналізу. WNN може уникнути недоліків традиційного про-

ектування нейронної мережі. Він має вищу можливість навчання, більшу точність, просту структуру та швидкість збіжності. Але в статті [5] зазначено, що, хоч RWT може гнучко та швидко налаштовувати часово-частотні характеристики, кількість обчислень, навантаження на процесор та використання пам'яті значно збільшилося, тому RWT не застосовується широко, тільки в традиційній обробці сигналів.

Стаття [7] описує новий алгоритм шифрування цифрових зображень. Цей алгоритм інтегрує хвильовий, хаотичний та циклічний алгоритми шифрування, комбінуючи шифрування в частотному та просторовому доменах. Основні особливості та переваги цього методу включають підвищену адаптивність завдяки використанню оптимізації за допомогою методу рою часток (PSO — Particle Swarm Optimization), застосування хаотичної карти для замішування низькочастотних коефіцієнтів із застосуванням логістичної хаотичної системи, циклічний підхід до шифрування з використанням алгоритму SHA-1 для генерації ключових послідовностей, ефективне приховування первісної інформації зображення в зашифрованих виходах, міцний ключовий простір із багатокомпонентною структурою, який стійкий до вичерпних атак, висока чутливість до ключових параметрів, висока інформаційна ентропія зашифрованих зображень, що вказує на дуже випадковий розподіл піксельних значень, високий піковий сигнал до шуму (PSNR) у розшифрованих зображеннях у порівнянні з іншими алгоритмами, підтвердження псевдовипадковості алгоритму через тести на випадковість NIST STS2.1.

Загалом, цей алгоритм шифрування вирізняється завдяки своїм особливостям забезпечення безпеки, адаптивності та ефективності в збереженні цілісності зашифрованих зображень.

Висновки. Стаття надає більш глибоке розуміння ролі вейвлет-аналізу у сучасному кодуванні сигналів. Вейвлет-перетворення демонструє значну ефективність у обробці сигналів та зображень. Новаторський підхід до шифрування, який об'єднує вейвлет-перетворення Haar та «золоті» матриці, відкриває нові можливості у криптографічному захисті цифрових сигналів. У статті розглядаються різні підходи до вибору та застосування вейвлетів для конкретних задач обробки сигналів, підкреслюючи їхні математичні властивості та практичну ефективність. Вейвлет-перетворення залишають великий простір для подальших досліджень в багатьох напрямках, пов'язаних з кодуванням та аналізуванням даних.

Бібліографічні посилання

1. Aljazaery Ibtisam A. Encryption of Images and Signals Using Wavelet Transform and Permutation Algorithm. / College of Engineering, Elect. Eng. Dep. Babylon University Hilla, July 2014

2. Davis, G.M., Nosratinia, A. Wavelet-Based Image Coding: An Overview. / Datta, B.N. Applied and Computational Control, Signals, and Circuits, 1999.

3. Subiono Joko Cahyono, Dieky Adzkiya, Bijan Davvaz A cryptographic algorithm using wavelet transforms over max-plus algebra. / Journal of King Saud University — Computer and Information Sciences, Vol. 34, 2022, Pages 627-635.

4. Confidential Algorithm for Golden Cryptography Using Haar Wavelet. / Marghny H. Mohamed, Yousef B. Mahdy, Wafaa Abd El-Wahed Shaban // (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 8, August 2014.

5. A Review of Wavelet Analysis and Its Applications: Challenges and Opportunities. / Tiantian Guo, Tongpo Zhang, Enggee Lim, Miguel Lopez-Benitez, Fei Ma, And Limin Yu // IEEE Access, Vol. 10, 2022, Pages 58869-58903.

6. Ситніков В. С., Біленко А. О. Класифікація вейвлет-функцій. / Праці Одеського політехнічного університету, 2008, вид. 1(29), стор. 168-171

7. Feng-Ping An, Jun-e Liu Image Encryption Algorithm Based on Adaptive Wavelet Chaos. /Journal of Sensors, Vol. 2019, Article ID 2768121, 12 pages.

8. Аносов А. О., Проценко М. М., Дубинко О. Л., Павлунько М. Я. Застосування вейвлет-перетворення для аналізу цифрових сигналів. / Сучасний захист інформації №1(33), 2018, стор. 38-42.

9. Tse, Norman C. F.; Lai, L. L. **Wavelet-based algorithm for signal analysis** / Journal on Advances in Signal Processing, Vol. 2007, 38916, 2007.

Статтю подано до редакції: 21.11.2023