УДК 683.03

О.Ю.Афанасєва, Б.В.Дурняк

РЕАЛІЗАЦІЯ АЛГОРИТМУ ВЕЙВЛЕТ ПЕРЕТВОРЕНЬ ГРАФІЧНИХ ОБРАЗІВ ДЛЯ СТЕГАНОСИСТЕМ

Перетворення Фур'є дозволяє перетворити довільний сигнал у нескінчений спектр, що представляє собою розклад по функціях косинусів і синусів. Це означає, що їх носії є нескінченими. Через це, розклад Фур'є не може забезпечити локалізації в часі. Це означає, що таке перетворення придатне для сигналів, частотні складові яких не змінюються в часі. Сигнали, що мають такі властивості, називаються стаціонарними. У випадку перетворень сигналу образу, для задач стеганографії необхідно мати змогу аналізувати не тільки його структуру представлену його спектром, а й місця, в котрих є особливості. Для того, щоб можна було забезпечити таку можливість, необхідно замість функцій косинуса і синуса використовувати функцію, яка мала б свій початок і кінець. Таким функціями є вейвлети. Завдяки цьому, існує можливість виявити в окремих місцях образу різного роду особливості. Досить вейвлет функцію розтягнути, чи стиснути, щоб досягнути зменшення, чи збільшення частоти. Розтягнута функція займає багато місця, тому її придатність до локалізації є менша. Стиснута функція займає мало місця, тому її роздільна здатність є висока. При вейвлет перетвореннях (DWT) немає необхідності ділити образ на частини. Такий поділ реалізується автоматично самими вейвлетами. Якщо реалізовувати сам алгоритм апроксимації сигналу вейвлетами, то можна його роботу продемонструвати на простому прикладі, в якому розглядається сигнал представлений восьма дискретними значеннями. Для цього групуються послідовні вартості сигналу парами і для кожної пари визначається середнє значення сигналу і отримуємо послідовність, що апроксимує сигнал кількістю дискретних значень, яких є в два рази менше ніж у попередньому його представленні. Аналогічно обчислюємо середнє значення різниці дискретних значень цих пар і отримуємо другу послідовність сигналу, яка також є в два рази менша початкової послідовності. Перша послідовність представляє собою ілюстрацію згладжування сигналу при його апроксимації, а друга послідовність відображає тенденцію в сигналі, або апроксимацією сигналу і деталізацією, відповідно. Оскільки в послідовності втрачається кожне друге значення, то отримані значення у нових послідовностях необхідно помножити на $\sqrt{2}$. Повторення описаної процедури приводить до скорочення кожної чергової послідовності в два рази і на кінець можна отримати послідовності з одним елементом. Кожна з отриманих пар послідовностей відповідає певному рівню апроксимації.

Аналогічно можна проілюструвати реалізацію оберненого алгоритму відновлення сигналу. Слід зауважити, що відновлення сигналу можливе лише послідовно переходячи з нижніх рівнів на верхні і тільки з першого рівня можна перейти до відновленого сигналу. Природно, що процес відновлення можна починати з будь якого рівня, оскільки в результату перетворення зберігаються послідовності всіх рівнів. Якщо прийняти, що відновлення сигналу реалізується з першого рівня, то практична реалізація такого відновлення полягає у наступному. Непарні місця двох послідовностей заповнюються нулями, завдяки чому, кількість елементів послідовностей подвоюється. Значення «0» позначимо x і із співвідношення, по якому обраховувались середні значення пар, визначимо x. Якщо текуче значення одного елемента послідовності першого рівня рівне y, то, для послідовності середнього значення від суми елементів, можна записати:

$$x = 2y - y \tag{1}$$

і, для послідовності середніх значень різниці елементів, можна записати:

$$x = y - 2y\,. \tag{2}$$

Після цього, кожний елемент послідовності ділиться на $\sqrt{2}$ і отримаємо дві нові послідовності, в яких в яких додаються члени двох послідовностей, що знаходяться на однакових позиціях. В результаті, отримуємо дискретні значення сигналу, якщо відповідні операції виконувались з послідовностями розкладу першого рівня. Якщо відповідні перетворення виконувались з послідовностями рівня n, то отримуємо послідовності рівня $n-1$, при цьому, не виконується додавання двох різних послідовностей. Якщо в результаті модифікації сигналу, при представленні його на останньому рівні, проводиться модифікація, що обумовлена вбудовуванням елемента повідомлення, то така модифікація проводиться по відношенню до всього сигналу в цілому.

З приведеної ілюстрації реалізації перетворення DWT видно, що кожний крок апроксимації приводить до декомпозиції сигналу, а кожний елемент послідовності, що відображає деталі, являється коефіцієнтом вейвлет перетворення. По приведеній ілюстрації видно, що чим вищий номер рівня декомпозиції, тим з більшої кількості дискретних значень сигналу вміщає коефіцієнт. Це означає, що вейвлети, які відповідають цим коефіцієнтам, займають більше місця в області часу. Тому, роздільність в області часу падає з ростом номеру рівня декомпозиції. Відповідно. Роздільність в області частоти росте із збільшенням рівня декомпозиції.

Більш гнучка реалізація вейвлет перетворень ґрунтується на використанні уявлень про цифрові фільтри. В даному випадку, використовуються фільтри з скінченою імпульсною відповіддю (FIR). Це означає, що фільтр вміщає скінчену послідовність коефіцієнтів. Практично, фільтр витинає з сигналу певні смуги частот. Найбільш простими фільтрами є низько і високо смугові фільтри. Використання фільтру реалізує в області частот множення характеристики фільтру на спектр сигналу, що по суті, в області частот означає суперпозицію в області часу. Оскільки фільтр є цифровий, то операція, яка виконує суперпозицію, ґрунтується на використанні суми добутків коефіцієнтів фільтру і вартості дискретних величин сигналу. Співвідношення (1) і (2) можна записати у наступному вигляді:

$$a_i = 0,5x_i + 0,5x_{i-1} \qquad \text{і} \qquad d_i = 0,5x_i - 0,5x_{i-1}.$$

Якщо x_i є дискретне значення сигналу, то стала 0,5 є коефіцієнтом фільтру. Фільтри, що використовуються, з точки зору частотних смуг, діляться на фільтри низького пасма частот (H) і фільтри високого пасма частот (G). Оскільки, в процесі перетворень величини середніх і різниць множились на $\sqrt{2}$, то коефіцієнтами фільтрів будуть:

$$H = [\sqrt{2}/2];\sqrt{2}/2]; \qquad G = [-\sqrt{2}/2;\sqrt{2}/2].$$

Величини деталей, що відповідають коефіцієнтам вейвлет функцій означають, у скільки раз величина складової сигналу є більша від вейвлету. Характеристика фільтру покриває спектр, тому відповідь фільтру G на одиничний імпульс має структуру вейвлету. Зміну масштабу для вейвлету, або його розтягування реалізується з допомогою функції зміни масштабу і визначається низько смуговим фільтром H. Систему перетворень, що ґрунтується на використанні фільтрів, називають деревом Малла [1]. У відповідності з таким деревом, можна стверджувати, що вейвлет аналіз проходить в двох областях одночасно. Можемо переміщатися вздовж дерева, щоб оперувати в нижніх пасмах частот, або у верхніх пасмах частот. Одночасно маємо можливість переміщатися по деталях вздовж осі часу. Принцип неозначеності, в даному випадку, означає, що чим нижчий рівень декомпозиції по дереву Малла, тим менша можливість руху по осі часу. Таким чином, розподіл сигналу на фрагменти, при використанні вейвлет перетворень, реалізується автоматично. Приймаючи до уваги, що фрагменти сигналу не є сталими, а залежать від співвідношення роздільності в області часу і частоти, то автоматичний розподіл сигналу забезпечує еластичність обробки сигналів. Технічна реалізація такої еластичності забезпечується за рахунок використання фільтрів FIR. Більш того, якщо необхідно поміняти один тип вейвлет функцій на інший, до досить поміняти фільтри.

Проектування фільтрів є досить складним завданням, особливо, складним є проектування системи фільтрів. Тому, сформульовано ряд умов, яким повинні задовольняти системи фільтрів, які використовуються для реалізації вейвлет аналізу сигналів.

Умова 1. Коефіцієнти низько смугових фільтрів H повинні задовольняти наступному співвідношенню:

$$\sum_{n=0}^{L-1} (h_n)^2 = 1,$$

де h_n коефіцієнт фільтру, L - довжина фільтру, n - номер коефіцієнта фільтру, що означає, що норма фільтру повинна бути рівна 1.

Умова 2. Сума добутків коефіцієнтів фільтру H, при пересуванні їх на паристу кількість позицій, повинна бути рівна нулю.

$$\sum_{n=0}^{L-1} h_{2k+n} h_n = 0 ,$$

де k - ціле число.

Ця умова рівнозначна наступній умові, що описується співвідношенням:

$$\sum_{n=0}^{L-1} h_n = \sqrt{2} .$$

Приведені умови визначають вимоги для фільтрів типу H. Коефіцієнти фільтрів високо смугових формуються на основі наступних співвідношень. Для коефіцієнта високо смугового фільтру аналізу, використовується наступне співвідношення:

$$g_n = (-1)^n h_{L-1-n}$$

Це співвідношення означає, що коефіцієнти високо смугового фільтру формується, як обернений до коефіцієнта фільтру H, при цьому, при парних коефіцієнтах, знак міняється на протилежний. Для коефіцієнтів низько смугового фільтру синтезу виконується співвідношення: $h_n^* = h_{L-1-n}$. Після цього, фільтр синтезу H^* формується з фільтру H шляхом переставлення послідовності його коефіцієнтів в оберненій послідовності.

Для коефіцієнтів високо смугового фільтру синтезу, має місце співвідношення:

$$g_n^* = g_{L-1-n} = (-1)^{n-1} h_n .$$

Це означає, що цей фільтр можна утворити або з фільтру G міняючи послідовність розміщення коефіцієнтів на протилежну, або з фільтра H.

В практиці часто використовується, для формування фільтрів, операція дзеркального відображення ($MIRROR$) [2]. Вона полягає у наступному. Спочатку формуються коефіцієнти фільтрів H і H^*, а решта коефіцієнтів формується на основі дзеркального перетворення, що реалізується у відповідності з наступними співвідношеннями:

$$G = MIRROR(H^*); G^* = MIRROR(H) .$$

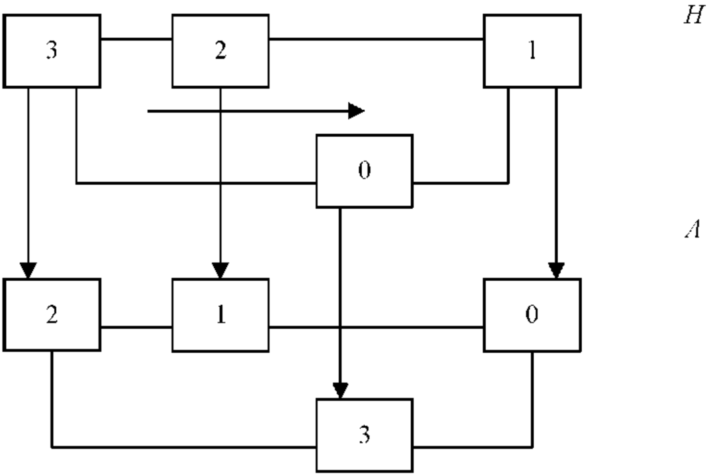
Операція $MIRROR$ полягає у заміні послідовності розміщення всіх коефіцієнтів на протилежну послідовність розміщення і зміні знаку коефіцієнтів. Що розміщаються на парних позиція. Нумерація коефіцієнтів починається з нуля і починаючи з нульового коефіцієнту змінюємо знак на протилежний.

Необхідно пам'ятати ряд базових властивостей вейвлетів Хаара, про які йдеться, що полягають у наступному. Середнє значення величини вейвлета є рівне 0, тому, спектр вейвлета має величину 0 для частоти 0 Hz. Такий спектр складається з великої кількості порогів. З цього випливає, що вейвлет аналіз не надає такої точної і однозначної відповіді на питання "з чого складається сигнал?", а аналіз Фур'є таку відповідь дає [3]. Пояснюється це тим, що у вейвлет аналізі маємо справу не з окремими частотами а з пасмами частот. Деталі у вейвлет аналізі відповідають за енергію сигналу, що сконцентрований у пасмі частот, а не за конкретну складову. Середнє значення масштабної функції відрізняється від нуля. Масштабна функція виводиться з вейвлет функції і пов'язана тільки з одним типом вейвлет функцій. Вейвлет функції в цифровому середовищі є дискретними в часі і, тому, зміна її вартості наступає тільки в момент вимірювання її значення. Якщо вейвлети створюють ортогональну базу, то зміна величини вужчого вейвлета може наступити тільки в границях часу, в яких ширший вейвлет має постійну величину. Для забезпечення умови нормалізації, необхідно, щоб стиснення вейвлета приводило до збільшення його амплітуди. Розтягування вейвлета повинно приводити до зменшення його амплітуди. Тому, норма вейвлет функції повинна завжди бути рівною одиниці. В протилежному випадку, не можливо було би стверджувати на різних рівнях декомпозиції в скільки раз коефіцієнти вейвлетів є більшими від складової сигналу.

Ціллю використання вейвлет перетворень, у нашому випадку, є аналіз растрових образів одночасно в часі і частоті. Фільтри вейвлет аналізу на основі вейвлетів Хаара є короткими і мають лише два коефіцієнти. У випадку, коли сигнал має багато дискретних значень, наприклад 100 дискретних значень, а фільтр має тільки 4 коефіцієнти, то очевидно, щоб реалізувати суперпозицію коефіцієнтів фільтра з сигналом, необхідно пересувати фільтр вздовж сигналу, після кожної операції сумування, на одну позицію. Кожний раз буде зменшуватися кількість дискретних значень сигналу і в кінці кінців виникне ситуація, коли сигнал буде коротшим від фільтру. В таких випадках, при практичній реалізації розв'язування використовується огортання фільтру навкруги сигналу. Для прикладу розглянемо фільтр H з чотирма коефіцієнтами а апроксимацію A з 4 дискретними значеннями. Щоб перейти на нижчий рівень, мусимо відкинути одночасно 2 дискретні значення. Виконаємо це наступним чином:

$$H : 0 \quad 1 \quad 2 \quad 3$$
$$A : 0 \quad 1 \quad 2 \quad 3$$

Обчислення суперпозиції фільтру з сигналом, якщо сигнал складається з такої самої кількості дискретних значень що і кількість коефіцієнтів у фільтру реалізується наступним способом. Обраховуються добуток коефіцієнтів, що виділені стрілками і підраховується їх сума. Ця сума складає першу величину дискретного значення сигналу на виході фільтра. Після запам'ятовування цієї величини, повертаємо всі коефіцієнти H у напрямку, який вказується стрілкою на дві позиції. Завдяки цьому виконуємо операцію редукування кожної другої вартості сигналу, які позначатимемо 92. Знову обраховуємо добуток коефіцієнтів, що позначені стрілками і обраховуємо їх суму. Дістанемо другий і останній елемент вихідного сигналу з фільтра. Для підвищення еластичності алгоритму, впроваджується поняття пересування (*OFFSET*). Пересування означає «ситуацію початкову» з якої розпочинається обраховування суперпозиції. Якщо пересування буде рівне 1, то обчислення буде виглядати наступним чином.



Результати обчислень приведено в таблиці 1.

Табл. 1.

Сума 1

	Множник 1	Множник 2	Множник 3	Множник 4
H	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3
A	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3

Сума 2

	Множник 1	Множник 2	Множник 3	Множник 4
H	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3
A	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3

Якщо пересування буде рівне 2, то обрахунок суперпозиції реалізується відповідно до схеми, що представлена на рис. 3.

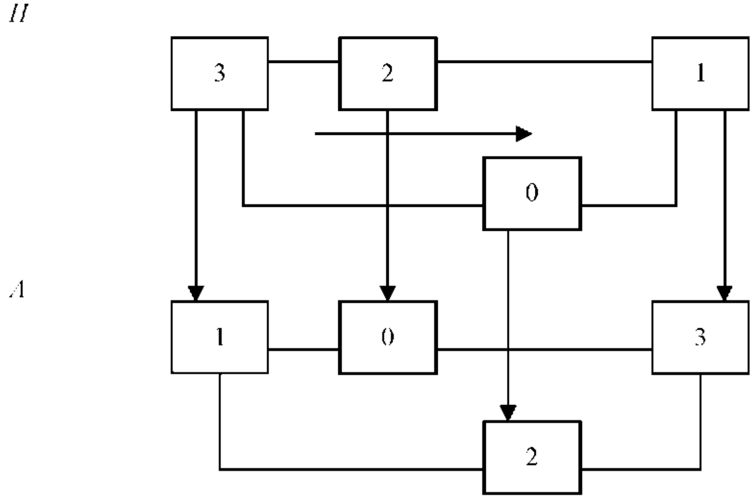


Рис. 3. Обчислення суперпозиції з пересуванням рівним 2.

Результати обчислень приведені в таблиці 2:

Табл.2.

Сума 1

	Множник 1	Множник 2	Множник 3	Множник 4
H	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3
A	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3

Сума 2

	Множник 1	Множник 2	Множник 3	Множник 4
H	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3
A	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3

З приведеного виходить, що пересування полягає у повороті фільтру H на певну кількість позицій назад по відношенню до обороту, або на повороті сигналу у відповідності з напрямком обертання.

Приведемо приклад, в якому фільтр є довшим від сигналу. Приймемо, що у цьому прикладі фільтр має 6 коефіцієнтів, а сигнал тільки 4 дискретні значення. приймемо, що пересування буде рівно 3.

H : 0 1 2 3 4 5 ; A : 0 1 2 3.

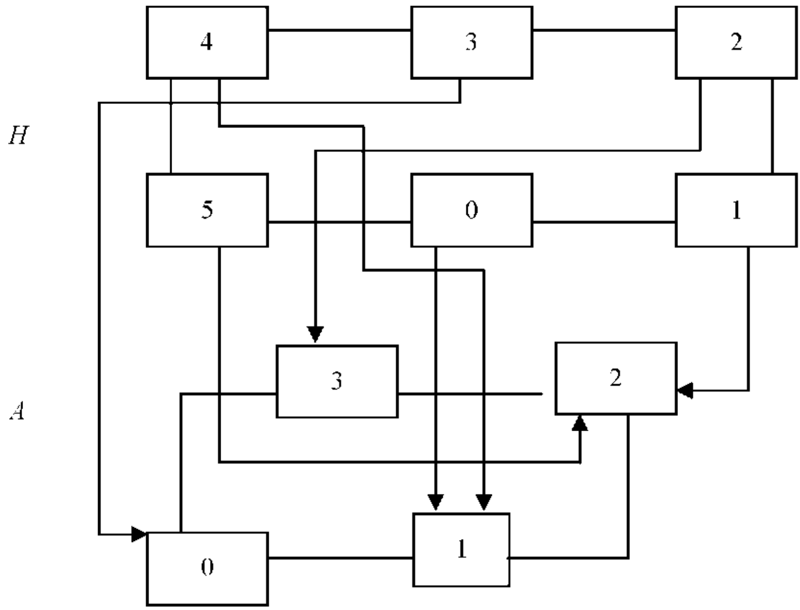


Рис.3. Схема проведення обрахунків з фільтром, що має 6 коефіцієнтів, сигналом, що має 3 дискретні точки.

Результати обчислень приведено в таблиці 3.

Табл..3.

Сума 1

Множ. 1 Множ. 2 Множ. 3 Множ. 4 Множ. 5 Множ. 6
H 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5

A 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3

Сума 2

Множ. 1 Множ. 2 Множ. 3 Множ. 4 Множ. 5 Множ. 6
H 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5

A 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3

З точки зору потреб стеганографії [4], вейвлет перетворення надають можливість використовувати різні рівні роздільності в часі і частотах. Завдяки цьому, можна вибирати можливі найкращі місця для впровадження елементів повідомлення, що укривається.

1. *Малла С.* Вейвлеты в обработке сигналов. М.: Мир, 2005.
2. *Дьяконов Ю.К.* Вейвлеты. От теории к практике. М.: СОЛОН-Р, 2002.
3. *Барри Н.К.* Тригонометрические ряды М.: Физматгиз, 1961.
4. Information Hiding Techniques for Steganography and Digital Watermarking.\ Editors *Stefan Katzenbeisser, Fabien A.P. Petitcolas*, London: Artech House, 2000.

Поступила 26.01.2009р.