УДК 681.325

А.Й. Наконечний
Національний університет “Львівська політехніка”,
кафедра “Автоматика і телемеханіка”

НАНЕСЕННЯ САМОПОДІБНИХ ЦИФРОВИХ ПІДПИСІВ НА ОСНОВІ МАЛОХВИЛЬОВОГО ПЕРЕТВОРЕННЯ СИГНАЛІВ

Розглянуто метод нанесення цифрових підписів для захисту зображень. Нанесення і виділення цифрового підпису виконується в малохвильовій області, що забезпечує велику роздільну здатність виділення. В запропонованому методі використовуються самоподібні цифрові підписи, які є стійкими до багатьох видів спотворень, таких, як фільтрування, компресія, масштабування і обрізання.

This paper presents a watermarking method for protection of still images. Embedding and detection are performed in the wavelet domain allowing thus multiresolution detection. The self-similar watermarks are used in suggested method and they are robust against many kinds of distortions, such as filtering, compression, scaling and cropping.

Вступ. Актуальною проблемою сьогодні є захист різних типів державних цінних паперів, копій, фотознімків та авторських прав мультимедійних даних. Така потреба викликала необхідність розробки сучасних методів позначень – цифрових підписів (ЦП) (водяних знаків). Усі методи нанесення ЦП спрямовані на дотримання двох основних вимог: невидимості та невідчутності ЦП та їх стійкості до різних типів модифікацій зображень при збереженні бажаної якості. Більшість сучасних методів базуються на переведенні оригінальних даних і даних ЦП в частотну область, з використанням дискретного перетворення Фур’є або дискретного косинусного перетворення (ДКП), після чого коефіцієнти модифікуються для нанесення цифрового підпису в початкові мультимедійні дані. При застосуванні ДКП псевдовипадкова кількість даних ЦП виділяється легко, в той час як усунення даних ЦП у вигляді коефіцієнтів, що є розкиданими по усій частотній області, є дуже складним. Крім того, наявність ЦП в початкових даних повинна оцінюватися під час виділення підпису при вимірюванні кореляції. За цим принципом працює метод, запропонований Коксом [2]. Згідно з цим методом цифровий підпис, який поміщається в перцептуально важливу компоненту сигналу, під час роботи сильно спотворює загальний сигнал і погано впливає на нього. Фактично модифікація такої компоненти під час зняття цифрового підпису буде викликати істотне спотворення самого зображення. З іншого боку, перцептуально важлива компонента може бути незначно модифікована процедурою нанесення підпису без будь-якої втрати якості зображення. Дещо кращі властивості має метод спектральної дисперсії, який є додатком до частотного методу. Основною відмінністю методу від попереднього є те, що в ньому здійснюється розсіяння перетворених даних ЦП на всьому проміжку частотної області початкових даних. Отже, порівняно зі звичайними частотними методами метод спектральної дисперсії є дещо стійкіший до фільтрування, обрізання країв, компресії з втратами, перевибірки та інших аналогічних перетворень з даними. Однак досягнути високих якісних показників при нанесенні ЦП, модифікації даних зображення з ЦП, а також при виділенні ЦП з маркованого зображення

можна лише при використанні малохвильового перетворення сигналів [1]. Основною властивістю малохвильових функцій є обробка даних у різних масштабах або з різними роздільними здатностями, виділення як великих, так і дрібних деталей.

Залежно від області представлення зображення ЦП, а також його видів і параметрів, існує ряд методів нанесення ЦП на оригінальні зображення, що базуються на малохвильовому перетворенні. Так, найпоширенішим є метод нанесення перетвореного за допомогою ДКП зображення ЦП в чорно-біле зображення та його досконаліший варіант, який включає додаткове малохвильове перетворення ЦП.

Самоподібні цифрові підписи. Різновидом представлених методів є метод вставки самоподібних ЦП у виділені піддіапазони малохвильового перетворення, який приводить до неявного візуального маскування, а, отже, невидимості ЦП.

Для пояснення методу можна використати, наприклад, ЦП у вигляді кола $W_M(r,\theta)$ як у базовому, материнському сигналі (рис.1):

$$W_M(r,\theta)=\begin{cases}0, & r<r_{min}\ \text{або}\ r>r_{max}\\ \pm\alpha, & r_{min}<r<r_{max}\end{cases}, \qquad (1)$$

де $r=\sqrt{n_1^2+n_2^2}$, n_1,n_2 представляють просторові координати, а $\theta=\text{arctg}\left(\frac{n_2}{n_1}\right)$; r_{min},r_{max} відповідно мінімальний і максимальний радіуси, які визначають кругову або колоподібну основу ЦП; α – ціле число, яке показує рівень вставки.

Щоби досягнути для $W_M(r,\theta)$ необхідних низькосмугових характеристик і, отже, збільшити стійкість при компресії чи фільтруванні, круговий базовий сигнал або колоподібну просторову основу додатково розділяють на цілу кількість секторів s, які мають розмір $\frac{s}{360}$. Усі пікселі всередині сектора для постійних радіусів дорівнюють $-\alpha$ або $+\alpha$ згідно з ініціалізацією псевдовипадкового генератора. W_M вибирають, щоб забезпечити можливість операції повертання. Виділення при кутах, менших, ніж $\frac{s}{360}$, є можливим без повертання ЦП. Коли кути повороту є більшими, то виділення виконується швидше, оскільки поворот ЦП потребує тільки багатократного $\frac{s}{360}$.

Наступним кроком є включення просторової самоподібності щодо декартової площини. На рис.1 наведені основні етапи виконання цього процесу. $W_M(n_1,n_2)$ є змасштабовані і зміщені відносно свого центра у 4 рази, отже, дають можливість виділяти ЦП для масштабованих факторів. Кінцевий ЦП $W_M(n_1,n_2)$ (рис. 1) складається з чотирьох шарів і визначається так:

$$W_M(n_1,n_2)=\sum_{f=0}^{3}\sum_{i=0}^{2^f-1}\sum_{j=0}^{2^f-1}W_M\left(2^f n_1+i\left\lceil\frac{r_{max}}{2^f}\right\rceil,2^f n_2+j\left\lceil\frac{r_{max}}{2^f}\right\rceil\right) \qquad (2)$$

Очевидно, що розміри ЦП становлять $2r_{max}\times 2r_{max}$ і не залежать від розміру зображення. Центр ЦП на етапі виявлення використовується як опорна точка.

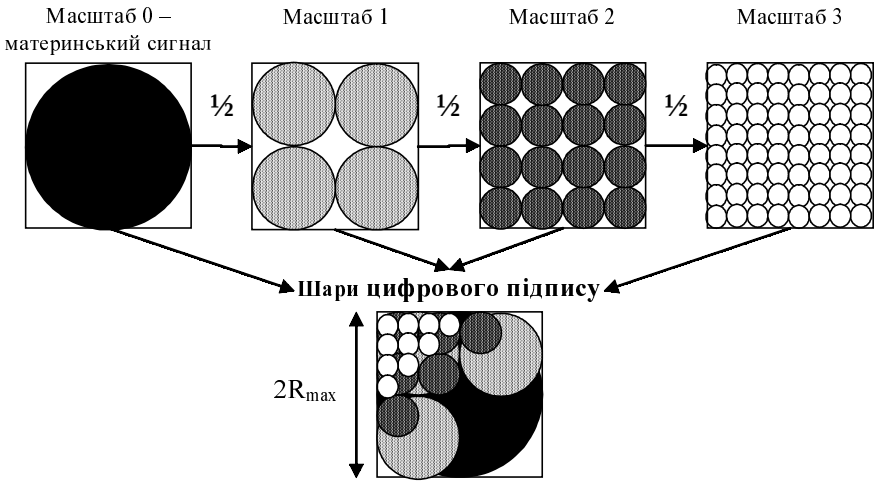

Рис. 1. Ілюстрація самоподібності в процесі генерації цифрового підпису

Нанесення цифрового підпису. Цей процес реалізується у малохвильовій області адитивним способом. Зображення розкладають за допомогою малохвильового перетворення на чотири рівні, використовуючи базові функції Гаара. ЦП $W_M(n_1, n_2)$ накладається на деталі підсмуг найвищого та інших вищих рівнів розкладеного оригінального зображення $I(n_1, n_2)$ (рис. 2). Аналітично зображення з ЦП може бути подано так:

$$I'_{f_l} = I_{f_l} \oplus W\left(2^{l-1} n_1, 2^{l-1} n_2\right), f \in \{HB, BH, BB\}, l \in \{1,2\}$$

де $\oplus$ – оператор суперпозиції, f визначає індекс піддіапазону, а l – індекс рівня малохвильового розкладу, де виконується встановлення.

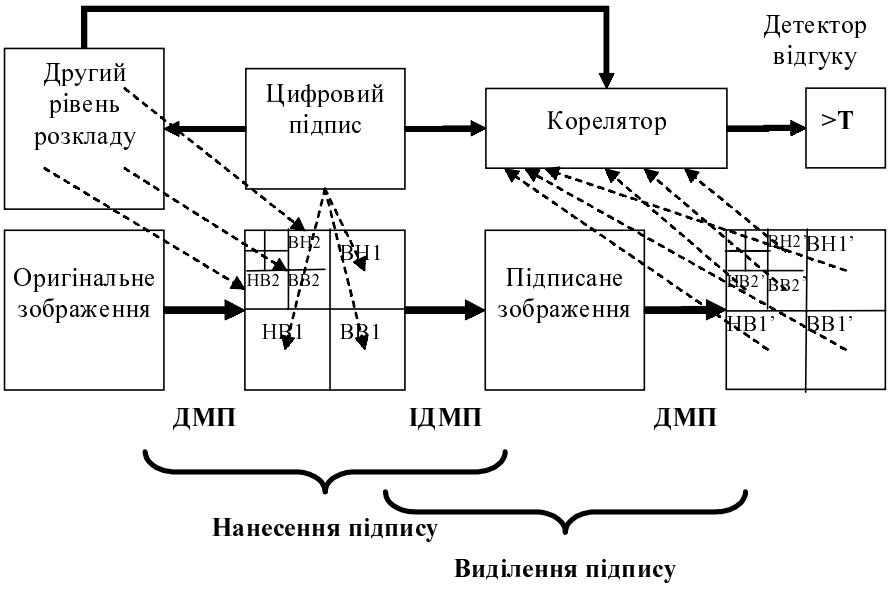

Рис. 2. Способи нанесення та виділення цифрового підпису в малохвильовій області

Необхідно відзначити, що розмір ЦП мусить бути меншим або дорівнювати половині розміру зображення, що маркується. Якщо він є меншим, то він додається всередину компоненти підсмуги деталі. Крім того, щоби зробити вставку в другий найвищий рівень малохвильового розкладу, виконують першочергово масштабування ЦП з коефіцієнтом S, використовуючи лінійну інтерполяцію. Вставка в нижні рівні розкладу дискретного малохвильового перетворення не виконується, оскільки вони розглядаються як особливо

ненадійні при дослідженні виділення помилкових ЦП. Після нанесення ЦП виконується зворотне дискретне малохвильове перетворення і отримується підписане зображення $I'(n_1, n_2)$. Завдяки наявній просторовій локалізації і частотному поширенню дискретного малохвильового перетворення відбувається неявне візуальне маскування невидимого ЦП.

Для забезпечення виділення ЦП після таких спотворень, як фільтрування або компресія, які мають схильність до усунення високочастотних компонент зображення (перший рівень ДМП), додатково здійснюється вставка в другий найвищий рівень перетворення. Така мультиплікативна вставка звичайно покращує характеристики ЦП.

Виділення цифрового підпису. Забезпечується статистичним способом без використання оригінального зображення. Спочатку підписане зображення $I'(n_1, n_2)$ перетворюється за допомогою малохвильового перетворення і обчислюються кореляції між ЦП (або масштабованим ЦП) і деталізованими частотними компонентами 1-го і 2-го рівнів (рис. 2). Отже, наступні нормалізовані кореляційні вирази оцінюються:

$$\rho(l, f) = \frac{I'_{f_l} \cdot W_{2^{l-1}}}{W_{2^{l-1}} \cdot W_{2^{l-1}}}, \quad l \in \{1,2\}, f \in \{HB, BH, BB\} \tag{3}$$

для кожної частотної орієнтації f (компоненти підсмуги) і кожного рівня l. $W_1(n_1, n_2) = W(n_1, n_2)$ і $W_2(n_1, n_2) = W(2n_1, 2n_2)$ Оскільки I_{f_l} і W є статистично незалежними і некорельованими, можна стверджувати, що $\rho(l, f)$ буде дорівнювати 1 за наявності ЦП і дорівнювати 0 за його відсутності. Для того, щоби оцінити повну кореляційну характеристику (відгук), спочатку оцінюється середнє значення по кожній частотній орієнтації f, а потім – максимальне значення з усіх частотно-орієнтованих f:

$$\rho = \max_f \{E_l[\rho(l, f)]\} \tag{4}$$

Середні значення по кожній частотній орієнтації допомагають підвищити кореляційне значення особливо після фільтрування або компресії, де вищі рівні розкладу мають схильність до більшого впливу. Для використання будь-якої стійкої існуючої структури в зображенні (наприклад, багатьох вертикальних країв), де ЦП краще зберігається, кінцевий кореляційний відгук вибирається як максимальне значення усіх підсмуг.

Кореляція (3) задовольняється при спотворенні таких зображень, як фільтрування або компресія, де просторова підтримка не змінюється. Щоби виявити ЦП при геометричних перетвореннях, ця кореляція повинна визначати, де використовується базовий сигнал $W_M(n_1, n_2)$ замість повного ЦП для застосування його самоподібної структури:

$$\rho_M(l, f) = \frac{I'_{f_l} \cdot W_{M, 2^{l-1}, \lceil r_{max} / 2^{l-1} \rceil}}{W_{M, 2^{l-1}, \lceil r_{max} / 2^{l-1} \rceil} W_{M, 2^{l-1}, \lceil r_{max} / 2^{l-1} \rceil}}. \tag{5}$$

$W_{M, 2^{l-1}, \lceil r_{max} / 2^{l-1} \rceil}$ визначає базовий сигнал, який є масштабованим до рівня $1/2^{l-1}$ і зміщений щодо центра ЦП в обох вимірах на величину $\lfloor r_{max} / 2^{l-1} \rfloor$. Ця кореляція веде себе в такий самий спосіб, як і в (3), навіть для інших видів спотворень. Легко довести, що коли ЦП існує, рівень кореляції дорівнює 1, а коли ЦП відсутній, його значення дорівнює 0.

Детектування виконують, порівнюючи кінцевий нормалізований корельований відгук ρ відносно визначеного порогу. Останній визначають, досягаючи дуже малої ймовірності виявлення ЦП за його відсутності в зображенні.

Експериментальне дослідження самоподібних ЦП. Дослідження виконувались для мультиплікативних нанесень ЦП у найвищі рівні перетворення. Виділення ЦП обчислювалися за відсутності спотворень або коли різні спотворення накладалися на підписане зображення. Коли спотворення були відсутні, ЦП виділявся у всіх випадках (100%). Виконувались також тестування численних випадкових ЦП. Так, дев'ять різних ЦП вносилися в зображення і намагалися виділити їх із 1000 підписаних зображень, які містили ці дев'ять ЦП. Як показують результати, наведені на рис. 3, виділялися усі дев'ять ЦП.

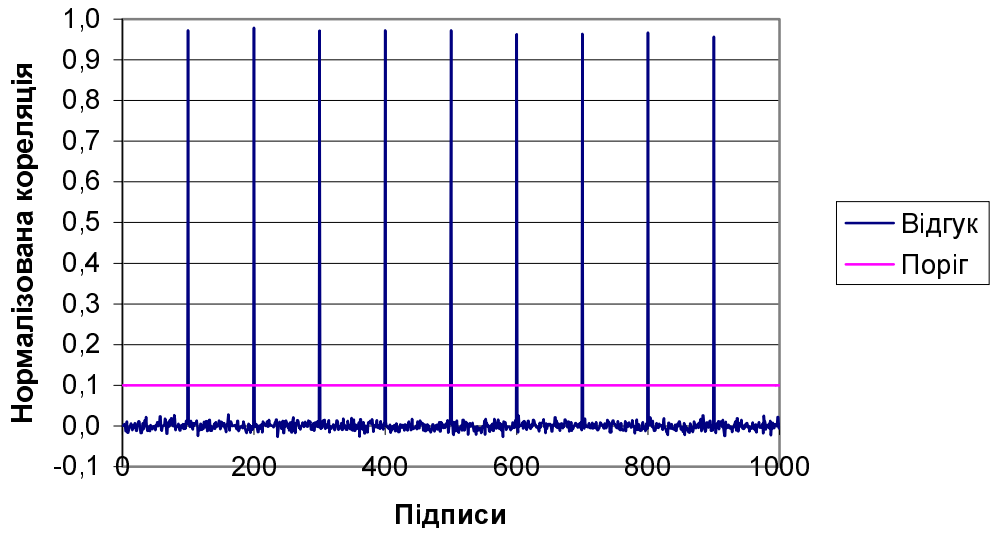

Рис. 3 Детектування 9 унікальних підписів з 1000 нанесених

Цей метод показав значну стійкість для слабких ЦП (40dB), які можуть витримати ступінь компресії 1:30. Нерівномірне обрізання кінців приводило, практично, до 100% детектування; розмір оригінального зображення зберігався.

Висновки. Нанесення самоподібних ЦП у виділені піддіапазони малохвильового перетворення забезпечує неявне візуальне маскування і невидимість ЦП.

Вставка самоподібних ЦП у нижні рівні розкладу дискретного малохвильового перетворення є недоцільною, оскільки вони розглядаються як особливо ненадійні і призводять до виділення помилкових ЦП.

Для забезпечення якісного виділення самоподібних ЦП після фільтрування або компресії сигналів, які мають схильність до усунення високочастотних компонент зображення, ЦП доцільно вставляти у вищі (високочастотні) рівні малохвильового розкладу, які мають порівняно невисоку енергетичну ємність, причому одночасно в декілька рівнів. Така мультиплікативна вставка забезпечує підвищення стійкості ЦП і покращання його характеристик.

Тестування виділення унікальних ЦП серед численних випадкових ЦП показали високу ефективність такого методу.

Дослідження доводять значну стійкість цифрового підпису до геометричних спотворень. Навіть нерівномірне обрізання кінців приводить до 100% детектування. Зберігається розмір оригінального зображення. Масштабовані з коефіцієнтом 1,2 підписані зображення також приводять до 100% виділення підпису.

Дослідження довели, що самоподібні цифрові підписи мають підвищену стійкість до багатьох видів спотворень, таких, як фільтрування, компресія, масштабування і обрізання.

1. Наконечний А.Й. Теорія малохвильового перетворення та її застосування. – Львів, 2001. 2. Cox I, Miller M.L.. "A review of watermarking and the importance of perceptual modeling". In Proc. of SPIE Human Vision and electronic imaging 11. V. 3016, P. 92 – 99. – 1997.

УДК 532.536

П.І. Скоропад, С.П. Яцишин, Р.П. Гамула
Національний університет "Львівська політехніка",
кафедра "Інформаційно-вимірювальна техніка"

АНАЛІЗ РАДІАЦІЙНОЇ СТАБІЛЬНОСТІ ЕЛЕКТРОФІЗИЧНИХ ПАРАМЕТРІВ МЕТАЛЕВИХ АМОРФНИХ СТОПІВ

Аналізується радіаційна стабільність термоелектродів з металевих аморфних стопів.

Radiation stability of metallic amorphous alloys thermoelectrodes is investigated.

Відомо, що при бомбардуванні твердих тіл іонами виникають такі явища, як пружні та недружні співударяння зі зв'язаними електронами речовини; пружні та недружні співударяння з ядрами, а також різного роду випромінювання, що супроводжують рух частинок в речовині. Через неістотність, в діапазоні енергій, що нас цікавлять, впливу процесів недружного співударяння з ядрами речовини та процесів пружного розсіювання на зв'язаних електронах, обмежимося аналізом лише двох процесів: недружнього співударяння зі зв'язаними електронами досліджуваних матеріалів та пружного співударяння з ядрами.

Отже, швидкі іони, розсіюючись на атомах речовини, що опромінюється, під час ядерного гальмування віддають їм частину своєї кінетичної енергії. Якщо передана енергія незначна, то в матриці досліджуваних металевих аморфних стопів (МАС) виникають локальні неоднорідності (аналоги точкових дефектів). Якщо ж передана енергія значно перевищує енергетичний поріг зміщення атома E_d, то атом, що його було вибито на початку, рухаючись, сам стає джерелом неоднорідностей на своєму шляху, котрі можуть змінюватися в часі внаслідок відпалу, скупчення тощо.

Гальмуючись, розсіяні іоном електрони передають свою енергію електронам провідності в області, що обмежується радіусом близько десятка міжатомних віддалей відносно траєкторії руху (треку). Густина енергії електронів тут, за оцінками, приблизно 100 кДж/см^3, а це орієнтовно відповідає тискові в 10^{11} Па, що і викликає, мабуть, стійкі напруження в матриці поблизу треку.

Для нас важливо знати не лише як зміняться властивості опромінених МАС, але й товщину модифікованого шару. Згідно з [1] глибина проникнення іонів у матеріал може бути встановлена через їх середній пробіг: