Список використаної літератури: ***1.*** *National Institute of Standards and Technology: The Advanced Encryption Standard (AES) – Режим доступа: http://csrc.nist.gov/aes/* ***2.*** *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989. – 28с.* ***3.*** *Горбенко И. Д., Тоцький О. С., Казьміна С. В. Перспективний блоковий шифр "Калина" – основні положення та специфікація // Прикладна радіоелектроніка. – 2007. - т.6, №2. – С.195-208.* ***4.*** *Горбенко И. Д., Бондаренко М. Ф. та ін. Перспективний блоковий шифр "Мухомор" – основні положення та специфікація // Прикладна радіоелектроніка. – 2007. – т.6. №2. – С.147-157.* ***5.*** *Kovalchuk L., Alekseyshuk A., Upper Bounds of Maximum Value of Average Differential and Linear Characteristic Probabilities of Feistel Cipher with Adder Modulo 2^n, // Theory of Stochastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32.* ***6.*** *Ковальчук Л. Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений // Труды Четвёртой Общероссийской научной Конференции "Математика и безопасность информационных технологий" (МаБИТ-05), 2-3 ноября 2005. – С.163-167.* ***7.*** *Ковальчук Л. Обобщённые марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа // Труды Пятой Общероссийской научной Конференции "Математика и безопасность информационных технологий" – (МаБИТ-06), 25-27 октября 2006. – С. 595-599.* ***8.*** *Олексійчук А. Н., Ковальчук Л. В., Пальченко С. В. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу // Захист інформації. – 2007. – № 2. – С. 12 – 23* ***9.*** *Алексейчук А., Ковальчук Л., Шевцов А., Скрыпник Л. Оценки практической стойкости блочного шифра «Калина» относительно разностного, линейного билинейного методов криптоанализа. // Труды Седьмой Общероссийской научной Конференции "Математика и безопасность информационных технологий" – (МаБИТ-08), 30 октября – 2 ноября 2008. – С. 15-20.* ***10.*** *А. Алексейчук, Л. Ковальчук., Е. Скрынник, А. Шевцов. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах. // Прикладная радиоэлектроника. – №1. – 2008. – С. 203–210.* ***11.*** *X. Wang, H. Yu. How to Break MD5 and Other Hash Functions. // Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005, P. 19-35.* ***12.*** *S. Cotini, R. L. Riverst, M. J. B. Robshaw, Y. Lisa Yin. Security of the RC6^{TM} Block Cipher, http//www.rsasecurity.com/rsalabs/rc6/.* ***13.*** *Tomas A. Berson Differential cryptanalysis mod 2^{32} with applications to MD5 // Advanced in Cryptology. – CRYPTO'98 (LNCS 372). – 1999. – P. 95-103.* ***14.*** *Ковальчук Л. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. //«Кибернетика и системный анализ» – 2010, – №6, С. 89 – 96.* ***15.*** *Ковальчук Л., Кучинская Н. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. //«Кибернетика и системный анализ» – 2012, – №5, С. 71 – 81.* ***16.*** *Кучинская Н. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига. // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації» – 2013, – №1 (23), С. 18 – 24.* ***17.*** *Кучинская Н. В., Скрыпник Л. В. Построение верхних оценок средних вероятностей целочисленных раундовых функций определённой структуры. // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації» – 2013, – №2 (24), С. 27 – 33.* ***18.*** *Ковальчук Л., Кучинська Н., Бездітний В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композиції модульного ключового суматора, блоку підстановки та лінійного оператора, що має блокову структуру. // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту* інформації в Україні» *– 2014, – №28, С.47 – 52.*

Василь Карпінець, Юрій Яремчук
Вінницький національний технічний університет

УДК: 004.056.5

ПІДВИЩЕННЯ СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНИХ ЗОБРАЖЕННЯХ ДО АТАКИ ВИЯВЛЕННЯ МІСЦЯ ЇХ РОЗТАШУВАННЯ

Анотація: **Запропоновано новий підхід до вбудовування цифрових водяних знаків (ЦВЗ) у частотну область векторних зображень на основі дискретного косинусного перетворення, що дозволяє зменшити максимальні відхилення координат точок до 20% порівняно з існуючим методом. Таке вдосконалення дозволяє зменшити вплив вбудовування ЦВЗ на візуальну якість векторних**

зображень, а також покращити статистичні характеристики зображення. Це забезпечує підвищення стійкості ЦВЗ до статистичних атак, спрямованих на виявлення місця їх розташування.
Summary: **The paper presents a new approach to embedding digital watermarks in the frequency domain vector graphics based on the discrete cosine transform, which reduces the maximum deviation of the coordinate points to 20% compared with the existing method. Such improvements can reduce the effect of embedding watermark in visual quality vector images and improve the statistical characteristics of the image. This provides increased stability watermark to statistical attacks aimed at identifying their locations.**
Ключові слова: **Стеганографія, цифровий водяний знак, захист авторського права, векторні зображення, стеганографічна стійкість.**

I Вступ

Сьогодні в інформаційних комп'ютерних системах векторні зображення широко використовуються для проектування архітектурних об'єктів, інтер'єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо, на створення яких витрачається багато часу та коштів. В зв'язку з цим виникає проблема їх захисту. При цьому найбільш перспективним є забезпечення захисту, коли не потрібно оригіналу для підтвердження авторства.

Методи вбудовування цифрових водяних знаків (ЦВЗ) у зображення, що забезпечують такий захист, у більшості базуються на частотних перетвореннях. До них відносяться методи Базіна-Барса-Маделана, Хе-Жу-Ванга, Солачідіса-Ніколаїдіса-Пітаса [2], а також метод Войта-Янга-Буша [3], який базується на зміні значень високочастотних (ВЧ) коефіцієнтів одновимірного дискретного косинусного перетворення (ДКП) векторного зображення і забезпечує зменшення впливу ЦВЗ при його вбудовуванні на якість зображення. Однак сумарна похибка відхилення координат точок відносно оригіналу в деяких випадках є досить суттєвою. Це призводить до можливого значного візуального спотворення зображення, а також до зниження стійкості до статистичних атак, спрямованих на виявлення місця розташування ЦВЗ.

Представлений в роботі [4] метод забезпечує зменшення сумарної похибки відхилення координат точок від оригіналу [5]. Для цього в методі використовується двовимірне ДКП і зміна коефіцієнтів ДКП проводиться таким чином, щоб його вплив на якість зображення був мінімальним при забезпеченні чіткого розпізнавання бітів ЦВЗ. Однак, в деяких випадках максимальне відхилення точок досягає великих значень, яке може призвести до помітних спотворень окремих точок, що може бути неприпустимим для деяких зображень та додатків, що їх використовують.

У роботі [6] представлено метод, в якому для усунення проблеми виникнення значних відхилень точок під час вбудовування біти ЦВЗ вбудовуються лише у ті матриці коефіцієнтів ДКП, зміна яких не призводить до таких відхилень. Для визначення придатних для вбудовування матриць запропоновано умови відбору з використанням граничного значення величини зміни коефіцієнтів внаслідок вбудовування ЦВЗ. Однак проведений в роботі [7] детальний аналіз запропонованого методу з відбором придатних матриць показав, що все таки можливі окремі випадки, коли відхилення координат точок внаслідок вбудовування ЦВЗ можуть бути значними. Це пов'язано з особливостями алгоритму зміни коефіцієнтів при вбудовуванні ЦВЗ.

Тому актуальним є вдосконалення запропонованого методу щодо усунення таких відхилень координат точок внаслідок вбудовування ЦВЗ і, відповідно, підвищення стійкості до атаки виявлення місця розташування ЦВЗ.

II Вдосконалення методу вбудовування ЦВЗ у векторні зображення

Згідно з запропонованим методом [4] та методом відбору придатних для вбудовування ЦВЗ матриць ДКП [6] для вбудовування одного біту ЦВЗ змінюється значення одного високочастотного (ВЧ) коефіцієнта $F_i(u_1, v_1)$ матриці ДКП залежно від значень двох ВЧ-коефіцієнтів $F_i(u_2, v_2)$ та $F_i(u_3, v_3)$.

Після вибору позицій трьох коефіцієнтів $F_i(u_1, v_1)$, $F_i(u_2, v_2)$ та $F_i(u_3, v_3)$ проводиться перевірка придатності відповідної їм i-ої матриці $F_i(u, v)$ для вбудовування біту ЦВЗ:

$$\left|F_i(u_1, v_1) - F_i(u_2, v_2)\right| \le P_h, \quad (1)$$

$$\left|F_i(u_1, v_1) - F_i(u_3, v_3)\right| \le P_h. \quad (2)$$

Якщо матриця не відповідає умовам (1) та/або (2), вона пропускається і аналізується наступна. Якщо ж матриця відповідає цим умовам, проводиться вбудовування біту ЦВЗ.

Вбудовування бітів ЦВЗ m_j в придатні матриці здійснюється таким чином. Якщо біт $m_j = 0$, то перевіряється умова:

$$F_i(u_1,v_1) < \frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{2}. \quad (3)$$

Якщо умова (3) виконується, значення коефіцієнта $F_i(u_1,v_1)$ залишається без змін, інакше значення коефіцієнта $F_i'(u_1,v_1)$ у матриці $F_i'(u,v)$ з вбудованим бітом ЦВЗ отримується таким чином:

$$F_i'(u_1,v_1) = \frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{2} - P. \quad (4)$$

Величина P використовується для забезпечення чіткої ідентифікації бітів ЦВЗ при витягуванні.

Якщо при вбудовуванні біт у ЦВЗ $m_j = 1$, то перевіряється виконання такої умови:

$$F_i(u_1,v_1) > \frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{2}. \quad (5)$$

Якщо умова (5) виконується, то коефіцієнт $F_i'(u_1,v_1)$ буде дорівнювати значенню коефіцієнта $F_i(u_1,v_1)$, інакше:

$$F_i'(u_1,v_1) = \frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{2} + P. \quad (6)$$

Таким чином, згідно з запропонованим підходом для відбору придатних матриць окремі випадки значних відхилент можуть виникати, коли значення модулів різниці коефіцієнтів для вбудовування $F_i(u_1,v_1)$ та $F_i(u_2,v_2)$, а також різниці $F_i(u_1,v_1)$ та $F_i(u_3,v_3)$ сягають граничного значення P_h. Тоді зміна коефіцієнта $F_i(u_1,v_1)$ буде найбільшою, оскільки згідно з формулою для вбудовування бітів ЦВЗ (4) та (6) його значення замінюється на середнє арифметичне значення двох інших коефіцієнтів, збільшене або зменшене на величину P, що може призвести до значних спотворень.

Крім того, залежно від характеристик зображення, діапазон значень ВЧ-коефіцієнтів може бути досить широким. Враховуючи ще те, що коефіцієнти ДКП представляються додатними та від'ємними числами, величина P_h часто може бути більшою або меншою від значення коефіцієнта $F_i(u_1,v_1)$ у декілька разів. В такому випадку істотна зміна коефіцієнта $F_i(u_1,v_1)$ відносно початкового значення суттєво вплине на координати точок. Тому, саме такі випадки можуть бути причиною значних відхилень в деяких точках.

Для прикладу, спочатку розглянемо випадок з гранично допустимими значеннями коефіцієнтів для вбудовування, наприклад $F_i(u_2,v_2) = F_i(u_1,v_1) + P_h$ та $F_i(u_3,v_3) = F_i(u_1,v_1) + P_h$. Тоді після вбудовування значення коефіцієнта $F_i(u_1,v_1)$ згідно з формулами (3) та (5) зміниться на $F_i'(u_1,v_1)$ наступним чином:

$$F_i'(u_1,v_1) = \frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{2} \pm P = F_i(u_1,v_1) + P_h \pm P. \quad (7)$$

З виразу (7) видно, що для даного прикладу значення нового коефіцієнта $F_i'(u_1,v_1)$ буде залежати від величини P_h, на яку воно буде збільшене.

Тепер визначимо граничне значення придатності для вбудовування, яке буде дорівнювати $P_h = 2 \cdot F_i(u_1,v_1)$. Тоді значення коефіцієнта $F_i'(u_1,v_1)$ після вбудовування біту ЦВЗ буде дорівнювати:

$$F_i'(u_1,v_1) = F_i(u_1,v_1) + 2 \cdot F_i(u_1,v_1) \pm P = 3 \cdot F_i(u_1,v_1) \pm P,$$

що змінить значення коефіцієнта майже в 3 рази.

В зв'язку з цим, для зменшення величини зміни коефіцієнтів і, відповідно координат точок, пропонується змінювати значення коефіцієнта $F_i(u_1,v_1)$ на величину, що дорівнює сумі двох інших коефіцієнтів, поділену на число, яке залежить від значень трьох коефіцієнтів $F_i(u_1,v_1)$, $F_i(u_2,v_2)$, $F_i(u_3,v_3)$ для кожної матриці $F_i(u,v)$.

Для прикладу, розглянемо попередній випадок, проте суму двох коефіцієнтів $F_i(u_2,v_2)$ та $F_i(u_3,v_3)$ поділимо не на 2, а на 4. Тоді отримаємо таке значення зміненого коефіцієнта:

$$F_i'(u_1,v_1)=\frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{4}\pm P=\frac{F_i(u_1,v_1)+P_h}{2}\pm P=\frac{3}{2}F_i(u_1,v_1)\pm P,$$

яке у 2 рази, відповідно, менше ніж у попередньому випадку.

Таким чином, для даного випадку, збільшивши дільник у формулах (4) та (6) можна забезпечити меншу зміну коефіцієнта $F_i(u_1,v_1)$.

Позначимо як d параметр, який буде дільником для суми коефіцієнтів $F_i(u_2,v_2)$ та $F_i(u_3,v_3)$. Величину параметра d пропонується визначати залежно від значень коефіцієнтів $F_i(u_1,v_1)$, $F_i(u_2,v_2)$, $F_i(u_3,v_3)$.

Співвідношення значень коефіцієнтів для вбудовування ЦВЗ може суттєво відрізнятися як між різними зображеннями, так і між матрицями $F_i(u,v)$ в межах одного зображення. Тому для досягнення найкращого результату значення параметра d потрібно визначати конкретно у кожному випадку з урахуванням особливостей зображення та вимог до збереження його якості, стійкості та розміру ЦВЗ. Для цього попередньо перед вбудовуванням ЦВЗ після визначення придатних матриць за значеннями коефіцієнтів $F_i(u_1,v_1)$, $F_i(u_2,v_2)$ та $F_i(u_3,v_3)$ потрібно визначити співвідношення їх значень для кожної відповідної матриці $F_i(u,v)$:

$$d_i=\left|\frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{F_i(u_1,v_1)}\right|. \tag{8}$$

Після чого отримаємо набір значень d для кожної матриці коефіцієнтів, при яких зміна коефіцієнтів після вбудовування ЦВЗ буде найменшою.

Проте використання окремого параметра d для кожної матриці $F_i(u,v)$ зменшить стійкість методу до спотворень, а також значно ускладнить обчислення. Тому, як і в методі [4], пропонується використовувати одне значення для всіх матриць коефіцієнтів.

Одним з варіантів визначення найоптимальнішого значення параметра d пропонується обчислювати його як середнє значення серед усіх значень d:

$$d=\frac{1}{w}\sum_{z=0}^{w-1}\left|\frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{F_i(u_1,v_1)}\right|, \tag{9}$$

де z - номер матриці $F_i(u,v)$ з придатними для вбудовування коефіцієнтами, w - кількість таких матриць.

Таким чином вбудовування бітів ЦВЗ m_j буде здійснюватися так: якщо біт $m_j=0$, то перевіряється умова:

$$F_i(u_1,v_1)<\frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{d}. \tag{10}$$

Якщо умова (10) виконується, значення коефіцієнта $F_i(u_1,v_1)$ залишається без змін, тобто у матриці $F_i'(u,v)$ з вбудованим бітом ЦВЗ коефіцієнт $F_i'(u_1,v_1)$ буде дорівнювати значенню коефіцієнта $F_i(u_1,v_1)$, інакше значення $F_i'(u_1,v_1)$ отримується як сума значень коефіцієнтів $F_i(u_2,v_2)$ та $F_i(u_3,v_3)$, поділена на число d, зменшена на значення P, тобто:

$$F_i'(u_1,v_1)=\frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{d}-P. \tag{11}$$

Якщо при вбудовуванні біт ЦВЗ $m_j=1$, то перевіряється виконання такої умови:

$$F_i(u_1,v_1)>\frac{F_i(u_2,v_2)+F_i(u_3,v_3)}{d}. \tag{12}$$

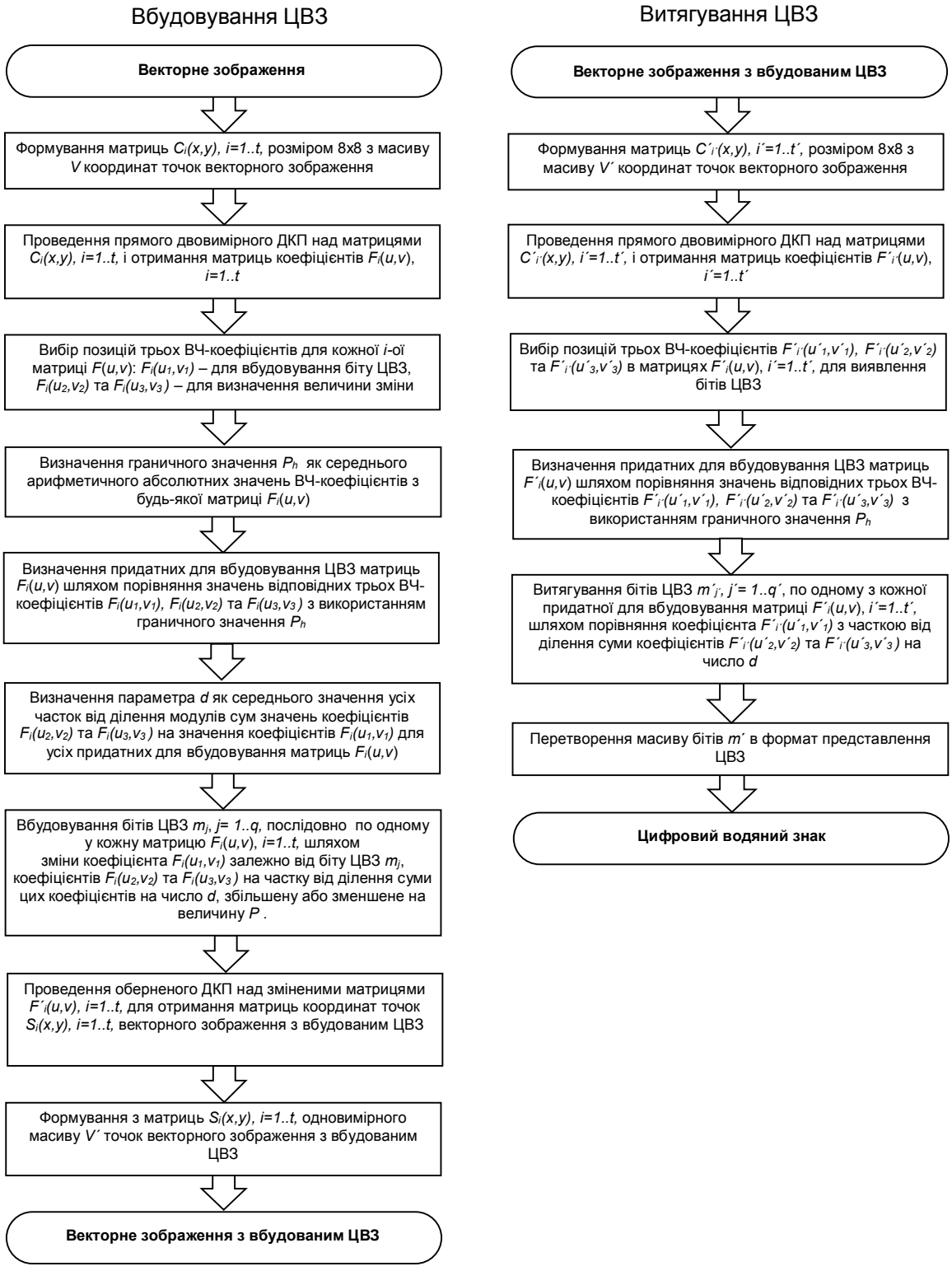

Рисунок 1 – Схема запропонованого методу вбудовування ЦВЗ у векторні зображення

Якщо умова (12) виконується, то коефіцієнт $F_i'(u_1, v_1)$ буде дорівнювати значенню коефіцієнта $F_i(u_1, v_1)$, інакше:

$$F_i'(u_1, v_1) = \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{d} + P\,. \tag{13}$$

При витягуванні бітів ЦВЗ умови для розпізнавання бітів ЦВЗ мають такий вигляд:

$$\begin{cases} m'_{j'} = 0, \ якщо \ \ F'_{i'}(u'_1, v'_1) < \dfrac{F'_{i'}(u'_2, v'_2) + F'_{i'}(u'_3, v'_3)}{d} \\ m'_{j'} = 1, \ якщо \ \ F'_{i'}(u'_1, v'_1) > \dfrac{F'_{i'}(u'_2, v'_2) + F'_{i'}(u'_3, v'_3)}{d} \end{cases} \tag{14}$$

При витягуванні ЦВЗ буде використовуватись таке ж значення числа d, як і при вбудовуванні.

На відміну від методу [4], де для виявлення бітів ЦВЗ необхідне знання тільки позицій коефіцієнтів $F_i(u_1, v_1)$, $F_i(u_2, v_2)$ та $F_i(u_3, v_3)$, даний підхід передбачає також необхідність знання параметра d, яке буде різним для кожного зображення. Це вимагає знання та передачу додаткових даних, проте це забезпечує додаткову стійкість методу до зловмисних атак, адже зловмисник не зможе відновити значення d, яке потрібне для розпізнавання бітів вбудованого ЦВЗ, навіть якщо він знає позиції коефіцієнтів.

Схему вбудовування та витягування ЦВЗ з запропонованим методом представлено на рис. 1.

На етапі вибору параметра *d* слід зазначити, що його значення залежить від значень ВЧ-коефіцієнтів, які, в свою чергу, визначаються зі значень координат точок зображення. Деякі зображення, наприклад векторні карти, можуть мати дуже різні пропорції сторін по вертикалі та горизонталі. Тому в таких зображеннях часто матриці ДКП-коефіцієнтів для *y* координати точок значно відрізняються від матриць для *x* координати. Відповідно для меншого спотворення зображення слід визначати число *d* для обох масивів координат точок окремо.

Проведений аналіз показав, що запропонований підхід забезпечує зменшення значення максимального відхилення координат точок до 20% порівняно з результатами у випадку з використанням критерію відбору придатних матриць коефіцієнтів ДКП. Зменшення відхилень дозволить підвищити стійкість ЦВЗ до статистичних атак, спрямованих на виявлення місця їх розташування.

III Висновки

В роботі було запропоновано новий підхід до вбудовування ЦВЗ у частотну область векторних зображень на основі ДКП, що дозволяє зменшити максимальні відхилення координат точок до 20% порівняно з існуючим методом. Таке вдосконалення дозволяє зменшити вплив вбудовування ЦВЗ на візуальну якість векторних зображень, а також покращити статистичні характеристики зображення. Це забезпечує підвищення стійкості ЦВЗ до статистичних атак, спрямованих на виявлення місця їх розташування.

Список використаної літератури: ***1.*** *В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук. Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ. – 2003. – 143 с.* ***2.*** *Liangbin Zheng, Yulu Jia, Qun Wang. Research on Vector Map Digital Watermarking Technology // First International Workshop on Education Technology and Computer Science – 2009. – P. 303-307.* ***3.*** *M. Voigt, B. Yang and C. Busch. Reversible watermarking of 2D vector data // ACM Mutimedia and Security Workshop. – 2004, – P. 160-165.* ***4.*** *Карпінець В. В., Яремчук Ю. Є. Вирішення проблеми погіршення якості векторних зображень при вбудовуванні цифрових водяних знаків // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні – 2010. – № 1(20). – С.73-83.* ***5.*** *Карпінець В. В., Яремчук Ю. Є. Аналіз впливу цифрових водяних знаків на якість векторних зображень // Сучасний захист інформації. – 2011. – №1. – С.72-82.* ***6.*** *Карпінець В. В., Яремчук Ю. Є. Зменшення відхилень координат точок внаслідок вбудовування цифрових водяних знаків у векторні зображення // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні – 2010. – № 2(21). – С.101-109.* ***7.*** *Яремчук Ю. Є., Карпінець В. В. Аналіз стійкості стеганографічного перетворення до вбудовування цифрових водяних знаків у зображення // Інформаційні технології та комп'ютерна інженерія.- 2007. - №1(8).- С. 212-217.*