УДК 004.93
DOI: 10.15587/1729-4061.2021.235802

Розробка методики підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення

О. М Маковейчук, І. В Рубан, Н. М. Бологова, А. А. Коваленко, В. О Мартовицький, Т. В. Філімончук

Представлено методику підвищення стійкості методів вбудови цифрового водяного знаку в цифрові зображення. Розроблена методика підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення, яка основана на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку. Описана у роботі методика з використанням псевдоголографічного кодування цифрових водяних знаків є ефективною для всіх типів атак, що розглядалися, окрім повороту зображення. В роботі представлено статистичний показник оцінки стійкості методів нанесення цифрових водяних знаків. Показник дозволяє комплексно оцінити стійкість методу до певного ряду атак. Проведено експериментальне дослідження, щодо запропонованої методики. Найбільш ефективною ця методика є при втраті частини зображення. При попередній фільтрації цифрового водяного знаку найбільш ефективним є третій метод фільтрації, що представляє собою усереднення по клітинці з подальшою бінаризацією. Найменш ефективним є перший метод, що представляє собою бінаризацію та знаходження статистичної моди по клітинці. Для атаки афінного типу, що представляє собою поворот зображення, даний метод є ефективним тільки при компенсації повороту. Для оцінки кута повороту знаходиться матриця афінного перетворення, що отримується по узгодженому набору відповідних ORB-дескрипторів. Використання цього методу дозволяє безпомилково виділяти цифровий водяний знак для всього діапазону кутів, що досліджувалися. Проведення комплексної оцінки методики підвищення стійкості методу нанесення цифрового водяного знаку на основі Вейвлет перетворень показало, що дана методика на 20 % *краще протидіє різним типам атак.*

Ключові слова: цифрові водяні знаки, методи стеганографії, псевдоголографічне кодування, дискретне косинусне перетворення, афінне перетворення.

1. Вступ

Надійність, непомітність та здатність до вбудовування є попередніми вимогами будь-якої техніки нанесення водяних знаків. Однак дослідження дійшли висновку, що цих вимог важко досягти одночасно.

Методи стеганографії застосовуються не тільки для прихованої передачі повідомлень, але і використовують для захисту авторських або майнових прав на цифрове зображення, фотографії або інші оцифровані твори мистецтва.

Тому розробляються різні заходи захисту інформації, організаційного і технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у вбудовуванні в об'єкт, що захищається невидимих міток – цифрових водяних знаків. Цифрові водяні знаки можуть містити багато корисної інформації: коли створений файл, хто володіє авторськими правами, контактна інформація про авторів та інше. Всі внесені дані можуть розглядатися як вагомі докази при розгляді питань і судових розглядів про авторство або для доведення факту нелегального копіювання і часто мають вирішальне значення.

Атаки, що видаляють цифрові водяні знаки (фільтрація, перемодуляція, стиснення з втратами і ін.), діють проти вбудованого повідомлення, тобто, спрямовані на знищення або псування цифрового водяного знаку шляхом маніпулювання маркованим зображенням. При цьому методи впровадження цифрових водяних знаків стійких до незначної фільтрації, розробити доволі складно. Такі методи зазвичай викликають значні спотворення зображення контейнера, що є не допустимим.

Таким чином, актуальною задачею є розробка методів та підходів, які підвищують стійкість цифрових водяних знаків і не вносять значних спотворень до зображення-контейнера.

2. Аналіз літературних даних та постановка проблеми

Авторами статті [1] розроблено техніку маркування кольорових зображень цифрового водяного знаку з використанням індукції дерева рішень у області дискретного косинусного перетворення. Метод використовує області дискретного косинусного перетворення для перетворення зображення-контейнера та водяного знаку, а метод індукції дерева рішень використовується для приховування водяного знаку. Але оскільки кольорове зображення має три канали, в яких інтенсивність буде різною, то для кожного каналу потрібно буде обирати різний поріг для вибору блоків для вбудови цифрового водяного знаку. І саме використання дерева рішень робить неможливість універсального використання такого способу вбудови цифрового водяного знаку, оскільки пороги для вибору блоків вбудови необхідно буде розраховувати для кожного зображення окремо.

В роботі [2] автори представляють геометрично інваріантне зображення водяних знаків на основі афінних коваріантних областей (ACR), які забезпечують певний ступінь стійкості. Для подальшого підвищення надійності використовується нова схема водяних знаків на основі роботи [3], яка нечутлива до геометричних спотворень, а також загальних операцій обробки зображень. Данна схема складається в основному з трьох компонентів:

1) процедура вибору ознак, заснована на алгоритмі теоретичної кластеризації графів, застосовується для отримання набору стабільних ACR, що не перекриваються;

2) для кожного обраного ACR виконуються локальна нормалізація і вирівнювання орієнтації для створення геометрично інваріантної області, яка може поліпшити стійкість запропонованої схеми водяних знаків;

3) для запобігання погіршенню якості зображення, викликаного нормалізацією і зворотньою нормалізацією, застосовується непряма зворотна нормалізація для досягнення хорошого компромісу між непомітністю і надійністю.

Проте даний метод стійкий тільки до геометричних спотворень зображень.

Автори розробили алгоритм водяних знаків із використанням сингулярного представлення матриці та генетичного алгоритму [4]. Метод використовує сингулярний вектор для вставки водяного знаку в контейнер. Крім того, методика генетичного алгоритму використовується для підвищення ефективності запропонованої схеми. Але обчислювальна складність, яка виникає при використанні генетичного алгоритму унеможливлює використання такого підходу у реальних умовах.

Водяні знаки на основі вейвлетів представлені в [5]. Метод використовує масштабний коефіцієнт для модифікації окремого вектора зображення-контейнера. Крім того, для оптимізації балансу між суперечливими факторами водяних знаків використовується багатоцільова оптимізація рою частинок. Але залишилися невирішеними питання, пов'язані з спотвореннями зображення в яких втрачається значна частина інформації (наприклад великий відсоток шуму або втрата частини зображення)

В роботі [6] запропоновано методику вбудови водяних знаків, що базується на сприйнятті людиною кольору. Вона забезпечує нову візуальну модель, яка може точно оцінити ступінь до помітних спотворень зорової системи людини. Проте в роботі не висвітлено, яким чином обирати потрібну область для вбудови. Це не дає можливість оцінити стійкість цієї методики.

У цій роботі [7, 8] пропонується стійку методику нанесення водяних знаків, яка поєднує в собі особливості дискретного перетворення вейвлетів (DWT), дискретного косинусного перетворення та розкладання особливих значень. У цій техніці DWT використовується для розкладання кольорових зображень на різні частотні та часові шкали. Відповідно до результатів поєднання особливостей DWT-DCT з технологією SVD забезпечує надійність проти обробки зображень та геометричних атак у кольоровій моделі YIQ. Проте дана методика виявилась нестійкою до інших типів атак.

Стійкий гібридний метод подвійного нанесення водяних знаків обговорює в роботі [9]. Але при підвищенні коофіцієнту вбудови цифрового водяного знаку для досягнення більш високого рівня стійкості спостерігаються незначні артефакти на зображенні-контейнері.

Основними проблемами при реалізації методів для забезпечення захисту авторського права в зображеннях, що представляють відкриті стеганосистеми, є суттєве руйнування чи знищення цифрових водяних знаків при високих коефіцієнтах ущільнення зображення, афінних перетвореннях та інших типів атак, а також пов’язане з цим помітне погіршення якості зображення.

Тому актуальними є дослідження, спрямовані на розробку методів та підходів, які підвищують стійкість цифрових водяних знаків і не вносять значних спотворень до зображення-контейнера.

3. Мета та задачі дослідження

Метою даної роботи є розробка методики підвищення стійкості методів нанесення цифрових водяних знаків на цифрові зображення. Це дасть можливість подальшого використання методів вбудови цифрових водяних знаків у комерційних проектах, з забезпеченням допустимого рівня стійкості.

Для досягнення мети були поставлені наступні завдання:

– розробити функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків в зображення;

– запропонувати показник оцінки стійкості;

– провести експериментальне дослідження, щодо запропонованої методики.

4. Матеріали та методи дослідження

Сучасні дослідження для створення ефективної системи водяних знаків використовують різні методи для вдосконалення та збалансування таких характеристик як: стійкість, непомітність, надійність.

Зауважимо, що в роботі не накладається ніяких обмежень на вид атак, тому вимагається, щоб пропонований метод стеганографії був стійким по відношенню до втрати частини зображення, в яке додано водяний знак.

Напрямок вирішення цієї проблеми дає так звана голографічна метафора – розподілена форма представлення цифрових зображень, яка є стійкою по відношенню до завад [10–14].

Ідея запропонованого перетворення досить прозора: цифрове зображення розгортається в одновимірну послідовність так, щоб «далекі» точки зображення мали «близькі» номера в одновимірній послідовності.

При цьому кожній точці з координатами (m, n) на зображенні ставиться у відповідність деяке число k, яке і визначає номер даної точки у псевдоголографічній послідовності. При порядковому скануванні та запису отриманої послідовності формується «псевдоголограма».

Таке перетворення дозволяє за довільним зв'язним фрагментом отриманої послідовності реконструювати зменшену копію вихідного зображення (або, застосовуючи інтерполяційні методи, реконструювати повномасштабну апроксимацію вихідного зображення). Тобто фрагмент одновимірної послідовності подібно аналоговій голограмі містить достатньо інформації про все зображенні в цілому.

Подібне «голографічне» представлення зображень є стійким по відношенню до пошкоджень даних, оскільки навіть при втраті частини інформації зображення можна відновити з певною точністю, яка залежить від розміру втрат.

Таким чином, пропонується для зображення водяного знаку проводити процедуру псевдоголографічного кодування, яка полягає у перемішуванні пікселів зображення за допомогою відомої псевдовипадкової перестановки [15]:

$$w_{perm} = w[p], \tag{1}$$

де w_{perm} – результат перемішуванні пікселів, p – відома псевдовипадкова перестановка. Для отримання такої перестановки зручно скористатися алгоритмом, який полягає у генерації псевдовипадкової рівномірно розподіленої послідовності x, яка потім сортується за зростанням і приймається, як перестановка p (індекси у відсортованій послідовності). Зауважимо, що доцільно розглядати лише глобальні перестановки, використання блочних перестановок вимагає виконання умови на розмір блоку, який повинен бути більшим за кореляційний радіус зображення (що у даному випадку є співмірним з розміром QR коду) [16].

При додаванні цифрових знаків (watermark) до зображень пропонується використовувати вейвлет-перетворення (Digital Wavelet Transform, DWT) [17–19]. При цьому зображення-контейнер перетворюється за допомогою DWT на чотири піддіапазони: низький-високий (LH), високий-низький (HL), високий-високий (HH) та низький-низький (LL) [20]. Формально можемо це записати у вигляді

$$[LL,\ HL,\ LH,\ HH] = DWT(f), \tag{2}$$

де f – зображення-контейнер, $DWT()$ – функція, яка здійснює DWT, [*LL, HL ,LH, HH*] – відповідні піддіапазони вейвлет-перетворення.

При цьому можна використовувати більшість відомих типів DWT, у роботі використовувалися вевлети Добеши [21].

Водяний знак мультиплікативно модифікує піддіапазон *LL*, в якому зосереджена основна інформація про зображення:

$$LL_w = LL \bullet (1 + \alpha w), \tag{3}$$

де w – зображення-водяний знак, LL_w – модифікований піддіапазон *LL*, α – параметр, оператор (•), який означає по-елементне множення матриць. Зауважимо, що зображення-водяний знак повинно мати вдвічі менший розмір, ніж зображення-контейнер. Вихідне зображення (із доданим водяним знаком) створюється за допомогою оберненого вейвлет-перетворення:

$$f_w = DWT^{-1}([LL_w,\ HL,\ LH,\ HH]), \tag{4}$$

де f_w – зображення-контейнер із доданим водяним знаком, $DWT^{-1}()$ – функція, оберненого перетворення DWT.

Для виділення цифрових водяних знаків описана вище процедура виконується у зворотному порядку:

1) аналогічно до (1) проводиться вейвлет-перетворення:

$$\left[LL',\ HL',\ LH',\ HH'\right] = DWT\left(f_w\right), \tag{5}$$

де [*LL', HL', LH', HH'*] – відповідні піддіапазони вейвлет-перетворення;

2) знаходиться оцінка цифрового водяного знаку *w'* як різниця *LL* – піддіапазонів зображення з водяним знаком та зображення-контейнера:

$$w' = LL' - LL; \tag{6}$$

3) оскільки оцінка цифрового водяного знаку *w'* буде модульована *LL* (вирази (3) та (5)), то враховуючи наявність шуму пропонується проводити фільтрацію зображення *w'*. У важливому частинному випадку, коли цифровий водяний знак представляє собою бінарний матричний код (наприклад, QR код) для фільтрації можна використати такі процедури, які будуть виконуватися для кожної клітинки матричного коду w_q^1:

– бінаризація та знаходження статистичної моди по клітинці:

$$w_q^1 = \mathrm{mode}\left(w_q' > \tau_1\right), \tag{7}$$

де w_q^1 – результат фільтрації для першого методу; *mode*() – функція, що повертає значення статистичної моди; τ_1 – поріг бінаризації;

– усереднення по бінаризованих значень по клітинці та подальша бінаризація:

$$w_q^2 = \mathrm{mean}\left(w_q' > \tau_1\right) > \tau_2, \tag{8}$$

де w_q^2 – результат фільтрації для другого методу; mean() – функція усереднення; τ_2 – поріг бінаризації;

– усереднення по клітинці та подальша бінаризація:

$$w_q^3 = \mathrm{mean}\left(w_q'\right) > \tau_3, \tag{9}$$

де w_q^3 – результат фільтрації для другого методу; τ_3 – поріг бінаризації.

Пороги бінаризації $\tau_{1,2,3}$ знаходяться по алгоритму Отсу [22] або використовуючи адаптивну бінаризацію [23].

Дане дослідження враховує основні фактори та нові методики, що використовуються потенційними дослідниками для створення надійної системи нанесення ЦВЗ на цифрові зображення.

5. Результати дослідження методики підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення

5. 1. Функціональна модель процесу забезпечення підвищення стійкості

Функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення показано на рис. 1.

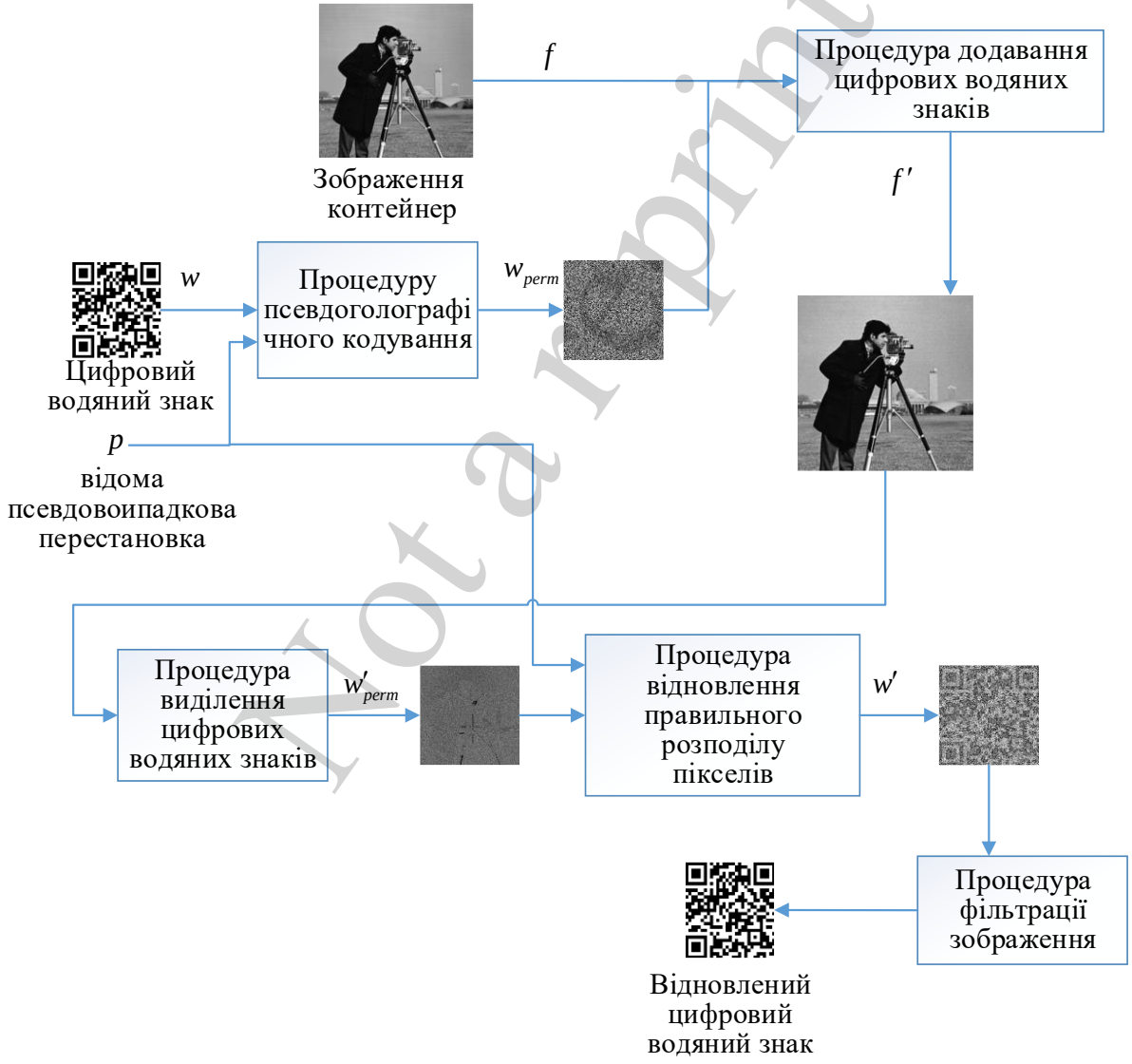


Рис. 1. Функціональна модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків на цифрові зображення

На рис. 1 використано наступні позначення: f – зображення контейнер, w – цифровий водяний знак, p – відома псевдовипадкова перестановка, w_{perm} – перемішаний цифровий водяний знак, f' – зображення-контейнер із доданим водяним знаком, w'_{perm} – виділений перемішаний цифровий водяний знак, w' – відновлений цифровий водяний знак зі спотвореннями.

Методика, описана на рис. 1, включає в себе наступні етапи:

1. Перемішування пікселів цифрового водяного знаку. Суть даного етапу полягає в тому, що за допомогою генератора псевдовипадкових чисел формується послідовність індексів $l=\{l_1, l_2, \ldots, l_{n\times m}\}$, де n, m – розмір водяного знаку w в пікселях. Після чого k-піксель водяного знаку переміщується на місце пікселя з індексом l_k. Таким чином отримуємо перемішаний відомою послідовністю цифровий водяний знак (w_{perm}).

2. Вбудова перемішаного цифрового водяного знаку (w_{perm}) в зображення-контейнер з цифровим (f). На даному етапі за допомогою будь-якого методу вбудови цифрового водяного знаку відбуваються нанесення (w_{perm}). В даній роботі для нанесення цифрового знаку використовувався метод з використанням вейвлет перетворень. В роботі використовувалися вевлети Добеши [21], для представлення зображення-контейнера (f) та перемішаного цифрового водяного знаку (w_{perm}). Після чого використовуючи коефіцієнт LL та деякий коефіцієнт α за допомогою формул (3), (4) здійснюється додавання частотний спектру перемішаного цифрового водяного знаку (w_{perm}) в частотний спектр зображення-контейнера (f).

3. Вилучення перемішаного цифрового водяного знаку (w_{perm}) з зображення-контейнера з цифровим водяним знаком (f'). На даному етапі за допомогою формули (3) здійснюється вейвлет перетворення та представлення зображення в частотному спектрі. За допомогою формули (6) знаходиться оцінка цифрового водяного знаку w' як різниця LL – піддіапазонів зображення з водяним знаком та зображення-контейнера.

4. Відновлення нормальної послідовності пікселів цифрового водяного знаку. Цей етап є зворотною процедурою представленою на першому етапі, після чого отримуємо нормальну послідовність пікселів цифрового водяного знаку.

5. Використання фільтрації цифрового водяного знаку. На цьому етапі для покращення цифрового водяного знаку використовуються різні методи фільтрації зображення. В роботі використовувалися три методи фільтрації зображення, описані формулами (7)–(9).

В даній методиці за рахунок псевдоголографічного кодування відбувається перетворення ЦВЗ, яке є стійкою по відношенню до різного типу спотворень. Це в свою чергу в комбінації з методами фільтрації зображень після виділення ЦВЗ і відновлення нормального розподілу пікселів ЦВЗ дозволяє досягти високого рівня стійкості методів нанесення ЦВЗ при різних атаках.

5. 2. Показник оцінки стійкості методів вбудови цифрових водяних

Стійкість методу вбудови цифрового водяного знаку можна оцінити в статистичному сенсі, прийняв наступні припущення.

Метод нанесення цифрового водяного знаку *W* може бути визначений як набір деяких функцій *F* та *G*, які описують процес вбудови і вилучення цифрового водяного знаку на множині всіх даних:

$$E = \left(E_i, i = 1,2,...,N\right). \tag{11}$$

E представляє собою набір даних, необхідних для роботи методу вбудови і вилучення цифрового водяного знаку.

Для спрощення будемо вважати, що набір вхідних даних *E* включає значення контейнер для вбудови *Im* та цифровий водяний знак *Wm*:

$$E_i = \left\{\mathrm{Im}_i, Wm_i\right\}. \tag{12}$$

Робота методу складеться з двох етапів: вбудова $F\left(E_i\right) = Im_i^*$ та вилучення $G\left(Im_i^*\right) = Wm_i$. Оскільки стійкість – це здатність алгоритму протистояти атакам, то введемо функцію атаки $At_j \in At$, де *At* – це множина допустимих атак на цифровий водяний знак.

Використавши функцію $At_j\left(Im_i^*\right)$ отримаємо спотворений контейнер $\left(Im_i^{*\prime}\right)$ з цифровим водяним знаком. Тоді для деяких значень E_i отримане значення від $G\left(Im_i^{*\prime}\right)$ може знаходитися в допустимих межах Δi:

$$\left|G\left(Im_i^{*\prime}\right) - G\left(Im_i^*\right)\right| \le \Delta i. \tag{13}$$

Для всіх інших E_i, що утворюють підмножину $E_l \in E$, виконання $G\left(Im_i^{*\prime}\right)$ не забезпечує прийнятного результату, тобто:

$$\left|G\left(Im_i^{*\prime}\right) - G\left(Im_i^*\right)\right| > \Delta i. \tag{14}$$

Всі такі випадки називаються хибними. В якості критерію порівняння відповідності формула (13) та (14) можуть виступати і інші критерії оцінки відповідності двох зображень, наприклад оцінки, представлені в роботах [24, 25].

Перетворення виду

$$F \to \forall At_j, At_j \in At \to G, \tag{15}$$

має результатом коректне зчитування ЦВЗ з контейнеру або хибне спрацювання, що представлено формулами (13), (14). Таким чином, ймовірність P того, що після використання атаки на контейнер з цифрового водяного знаку $At_j\left(Im_i^*\right) = \left(Im_i^{*\prime}\right)$ вилучення ЦВЗ з контейнера призведе до хибного результату (14), дорівнює ймовірності, що набір вхідних даних E_i, що використаний при j-й атаці, належить множені E_l. Нехай $n_{l,j}$ – число різних наборів вхідних даних, що містяться в E_l, для j-ї атаки, тоді $Q_j=n_{l,j}/N$ є ймовірність того, що виконання послідовності функцій (15) на наборі даних E_i, випадково вибраним з E серед однаково ймовірних, закінчиться хибним вилученням цифрового водяного знаку.

При цьому $P_j=1–Q=1–n_{l,j}/N$ є ймовірність того, що при j-й атаці на елемент E_i, випадково обраний з множини E, буде отримане значення цифрового водяного знаку, яке знаходитися в допустимих межах, – вираз (13).

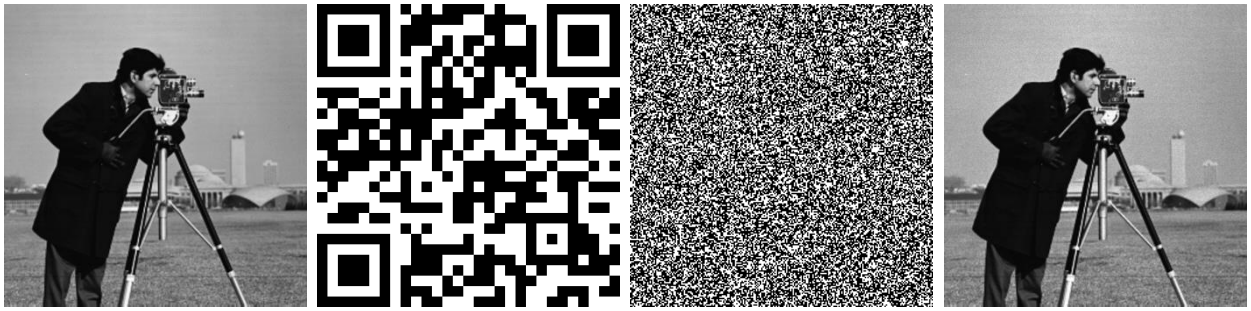
Оскільки проведення різних атак є незалежними подіями, то ймовірність того, що ці атаки не забезпечує прийнятного результату – вираз (14), – дорівнюватиме добутку ймовірностей допустимих значень цифрового водяного знаку після кожної атаки:

$$R = \prod_1^j P_j. \tag{16}$$

Цей добуток ймовірностей і буде оцінювати надійність методу ЦВЗ.

5. 3. Експериментальне дослідження методики вбудови цифрових водяних знаків

Для експериментів в якості зображення-контейнера було використано тестове зображення у градаціях сірого Cameraman (рис. 2, *а*). Для зображення цифрового водяного знаку – бінарне зображення QR-code, що представляє собою матрицю 29×29 елементів, де закодовано повідомлення ‘KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS’ (рис. 2, *б*). При цьому розмір зображення QR-code є 464×464 пікселів (тобто, розмір одної клітинки 16×16), Cameraman було перемасштабовано до розміру 928×928. Для отримання цифрового водяного знаку пікселі зображення QR-code були перемішані за допомогою описаної вище процедури (рис. 2, *в*). Результат додавання цифрового водяного знаку (значення параметру α=0.1) наведено на рис. 2, *г*.



а *б* *в* *г*

Рис. 2. Вхідні зображення: *а* – зображення-контейнер *Cameraman*; *б* – *QR-code*.; *в* – цифровий водяний знак (перемішаний *Cameraman*); *г* – результат додавання цифрового водяного знаку

При проведенні експерименту були досліджені вплив атаки таких типів:

– додавання нормально розподіленого шуму із заданим середнім і дисперсією;

– додавання шуму типу «сіль-і-перець» із заданою густиною;

– поворот на заданий кут;

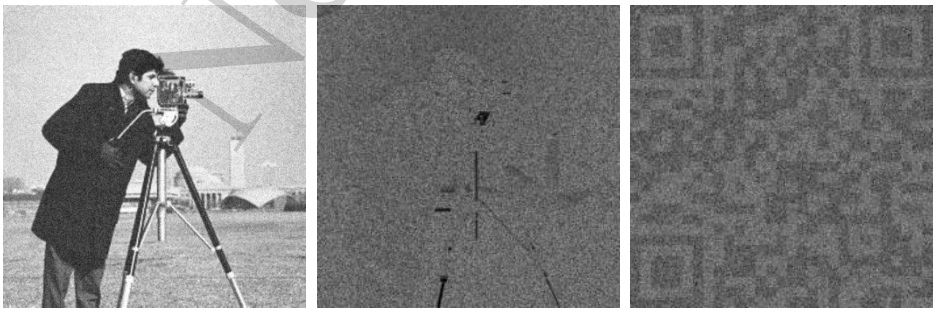
– видалення частини зображення заданого розміру;

– jpeg-компресія із заданим параметром якості.

Для кожного типу атак визначалась загальна кількість помилок у матриці QR коду, яка отримується з виділеного цифрового водяного знаку.

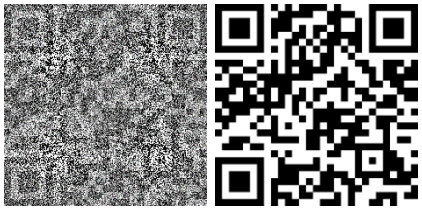
Досліджувався вплив нормально розподіленого адитивного шуму з середніми μ=0:0,001:0,05 і дисперсіями σ^2=0:0,001:0,05. Результати наведено на рис. 3–7.

При дослідженні впливу нормально розподіленого адитивного шуму (рис. 3) можна побудувати графіки залежності кількості помилок від параметрів шуму, наведені на рис. 7–9.



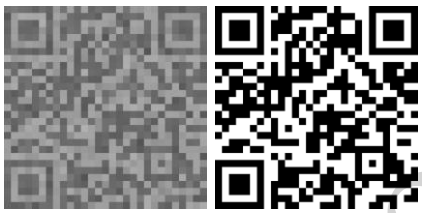
а *б* *в*

Рис. 3. Вплив нормально розподіленого адитивного шуму: *а* – додавання шуму, μ=0.2, σ^2=0.25; *б* – виділення цифрового водяного знаку; *в* – відновлення правильного розташування пікселів у цифровому водяному знаку



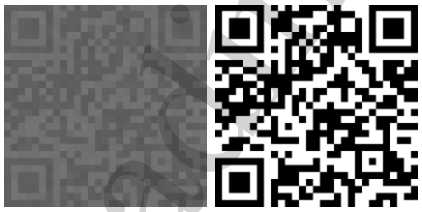
а *б*

Рис. 4. Перший метод фільтрації: *а* – бінаризація зображення; *б* – застосування операції статистичної моди до кожної клітинки;



а *б*

Рис. 5. Другий метод фільтрації: *а* – усереднення бінаризованого зображення по кожній клітинці; *б* – бінаризація зображення;



а *б*

Рис. 6. Третій метод фільтрації: *а* – усереднення зображення по кожній клітинці; *б* – бінаризація зображення

Далі досліджувався вплив шуму типу «сіль-і-перець» з густиною ρ=0:0,01:0,5. Результати наведено на рис. 10–13.

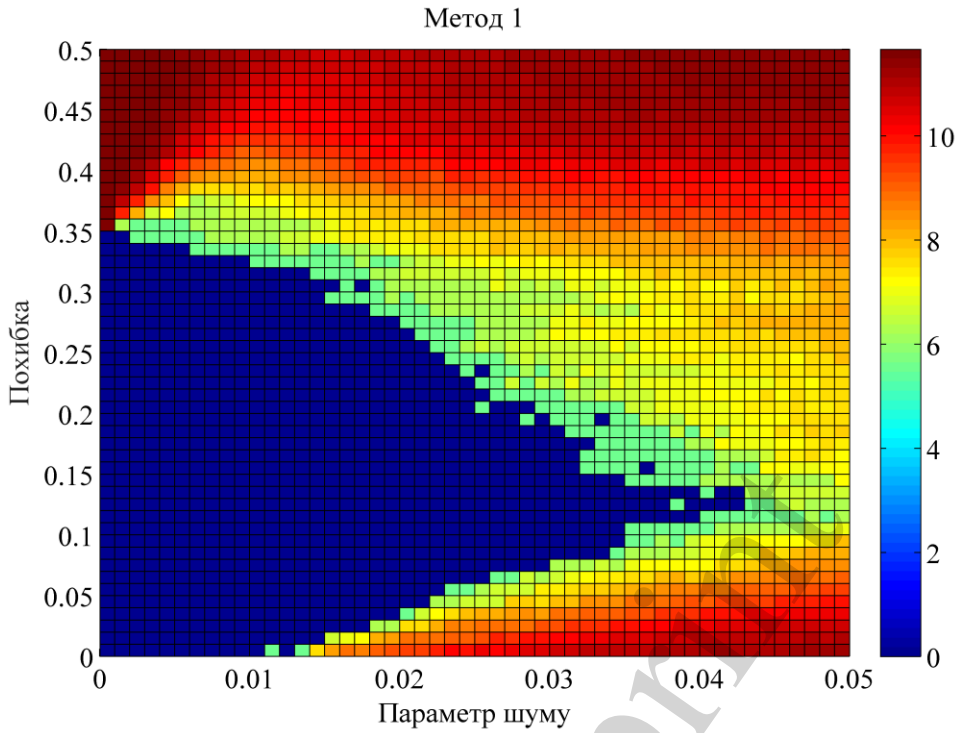


Рис. 7. Графіки залежності кількості помилок від параметрів шуму для першого методу фільтрації

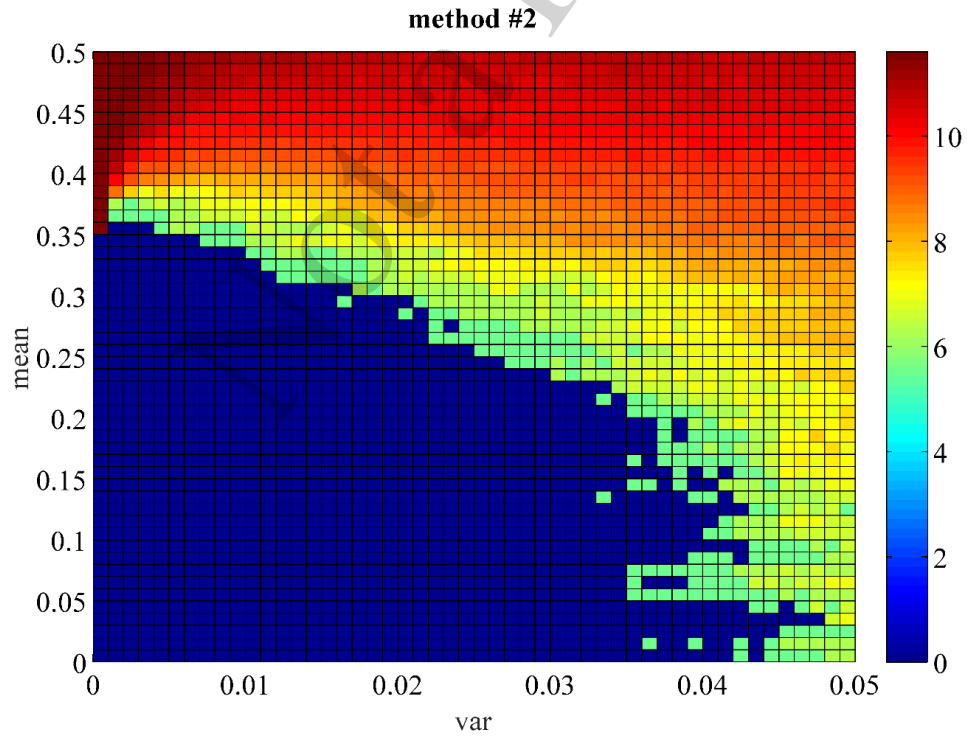


Рис. 8. Графіки залежності кількості помилок від параметрів шуму для другого методу фільтрації

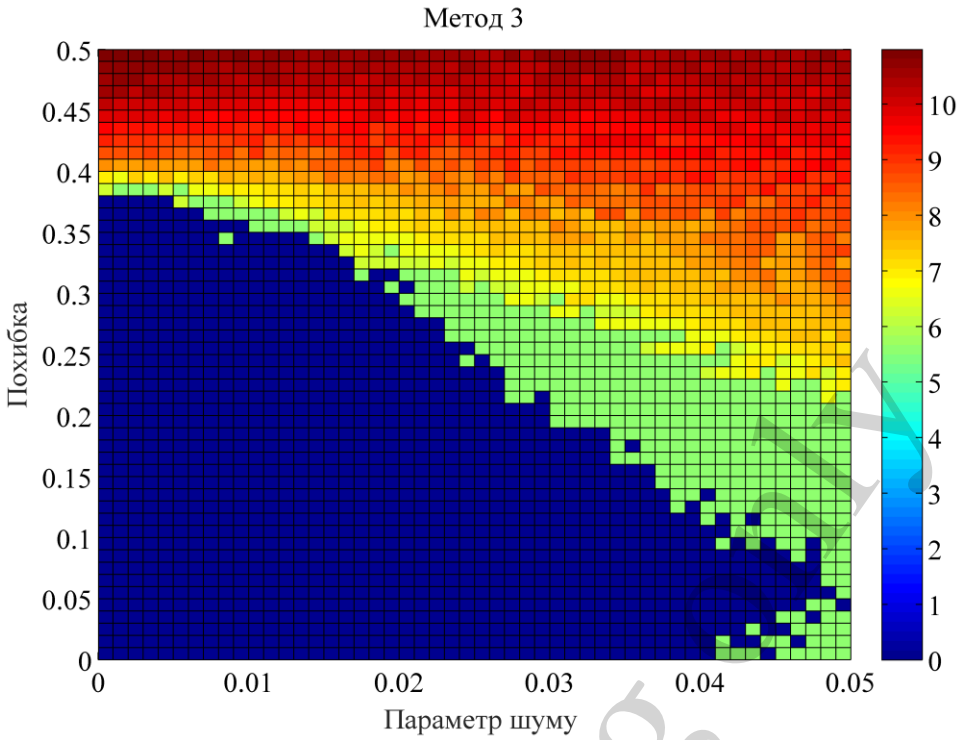
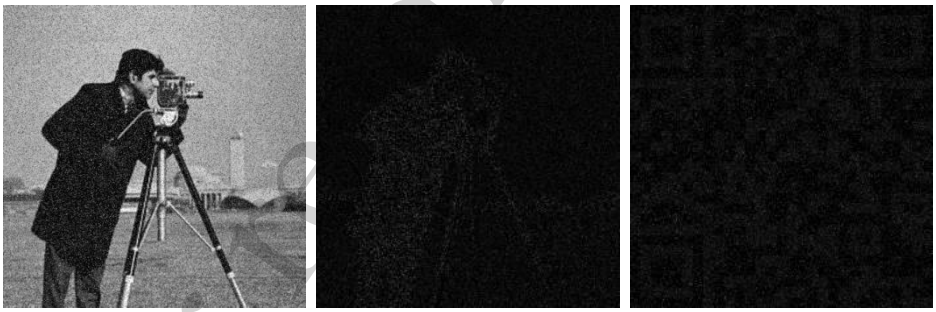


Рис. 9. Графіки залежності кількості помилок від параметрів шуму для третього методу фільтрації



а *б* *в*

Рис. 10. Вплив нормально розподіленого адитивного шуму: *а* – додавання шуму, ρ=0,15; *б* – виділення цифрового водяного знаку; *в* – відновлення правильного розташування пікселів у цифровому водяному знаку

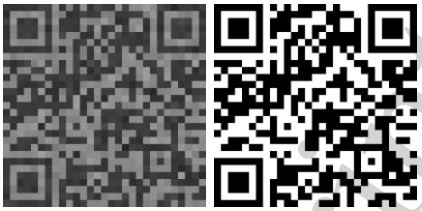
При дослідженні впливу шуму типу «сіль-і-перець» (рис. 10–13) можна побудувати графіки залежності кількості помилок від параметрів шуму (рис. 14).

Дослідження впливу повороту зображення на цифровий водяний знак проводилося в два етапи.

На першому етапі досліджувався вплив повороту зображення на кути φ=-2°:0,1°: 2°. Результати наведено на рис. 15–18.

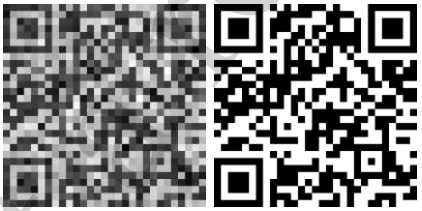
а *б* *в*

Рис. 11. Перший метод фільтрації: *а* – бінаризація зображення; *б* – застосування операції статистичної моди до кожної клітинки; *в* – різниця між фільтрованим зображенням і оригінальним QR кодом



а *б*

Рис. 12. Другий метод фільтрації: *а* – усереднення бінаризованого зображення по кожній клітинці; *б* – бінаризація зображення



а *б*

Рис. 13. Третій метод фільтрації: *а* – усереднення зображення по кожній клітинці; *б* – бінаризація зображення

Для кожного методу фільтрації наведено графіки залежності кількості помилок від кута повороту (рис. 19).

Всі методи фільтрації для даного типу атаки є однаково неефективними.

Другий етап включає в себе дослідження використання компенсації повороту перед вилученням цифрового водяного знаку з зображення-контейнера.

Щоб оцінити кут повороту, знайдемо матрицю афінного перетворення між оригінальним і повернутим зображеннями-контейнерами. Для цього на кожному із цих зображень визначимо розташування точок особливостей (в якості яких будемо використовувати дескриптори ORB [24]). Зауважимо, що для детектування достатньої кількості дескрипторів, ці зображення необхідно згладити за допомогою гауссівського фільтра з σ=3 (рис. 20).

Знаходження відповідних точок дискрипторів ORB проводиться за допомогою алгоритму RANSAC [25]. RANSAC (абр. RANdom SAmple Consensus) це ітеративний метод, що використовується для оцінки параметрів математичної моделі для набору спостережуваних даних, які містять викиди (рис. 21).

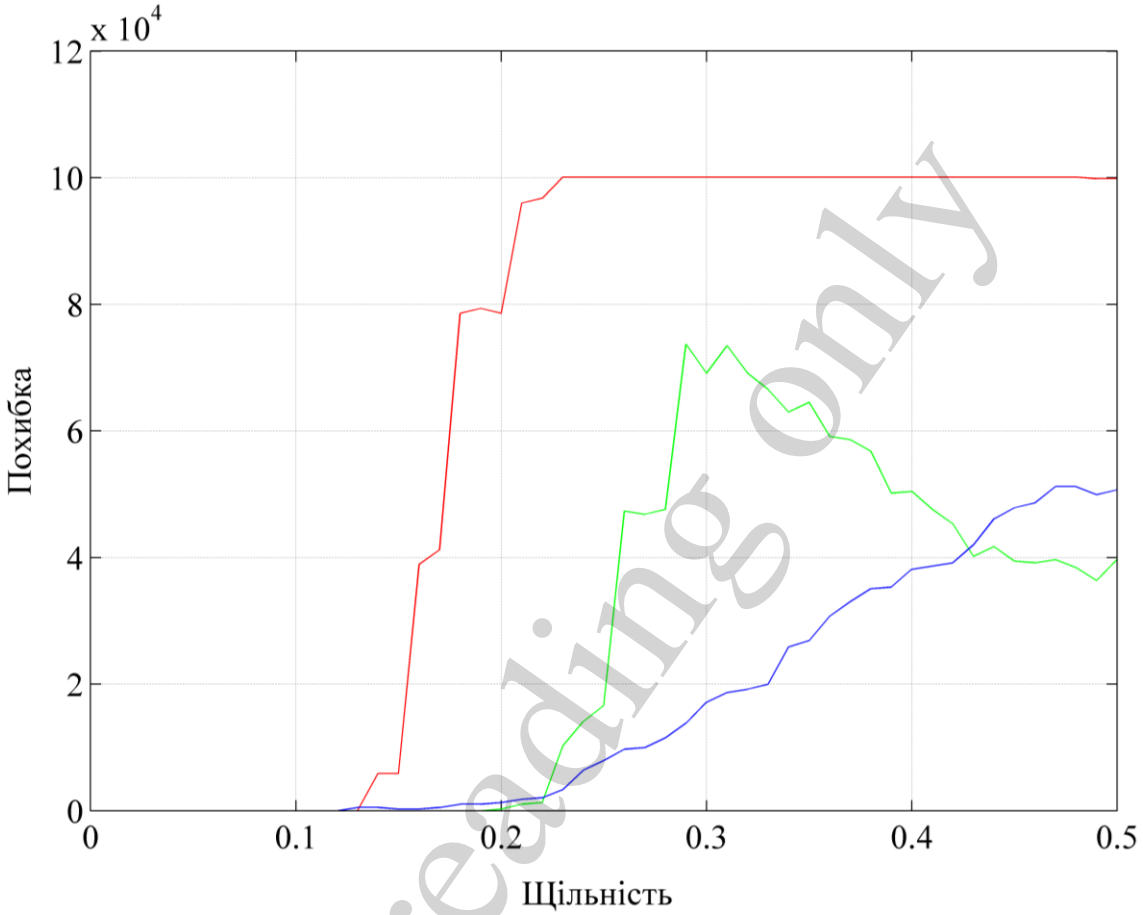
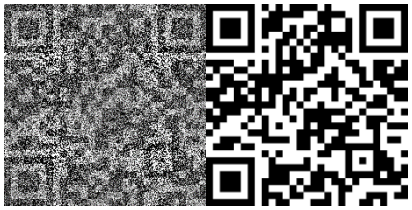


Рис. 14. Графіки залежності кількості помилок від параметрів шуму

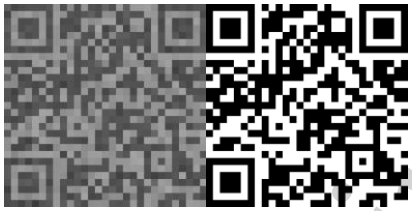
а *б* *в*

Рис. 15. Вплив нормально розподіленого адитивного шуму: *а* – додавання шуму, φ=0,2°; *б* – виділення цифрового водяного знаку; *в* – відновлення правильного розташування пікселів у цифровому водяному знаку



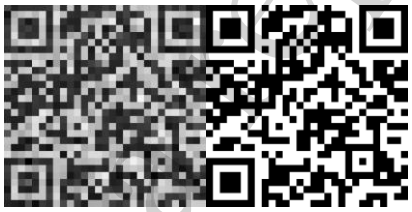
а *б*

Рис. 16. Перший метод фільтрації: *а* – бінаризація зображення; *б* – застосування операції статистичної моди до кожної клітинки



а *б*

Риск. 17. Другий метод фільтрації: *а* – усереднення бінаризованого зображення по кожній клітинці; *б* – бінаризація зображення



а *б*

Рис. 18. Третій метод фільтрації: *а* – усереднення зображення по кожній клітинці; *б* – бінаризація зображення

Знайшовши таким чином відповідні набори дочок будуємо матрицю афінного перетворення T [24]. Тоді кут повороту знаходяться із співвідношення [25]:

$$\varphi = \operatorname{atan}\frac{T_{21}}{T_{11}}. \tag{10}$$

Описаний метод компенсації легко узагальнюється на інші координатні перетворення, що є перспективним напрямком подальших досліджень.

Знаючи кут повороту, довернемо зображення у протилежному напрямку (рис. 22).

Результати роботи представлено на рис. 23–25.

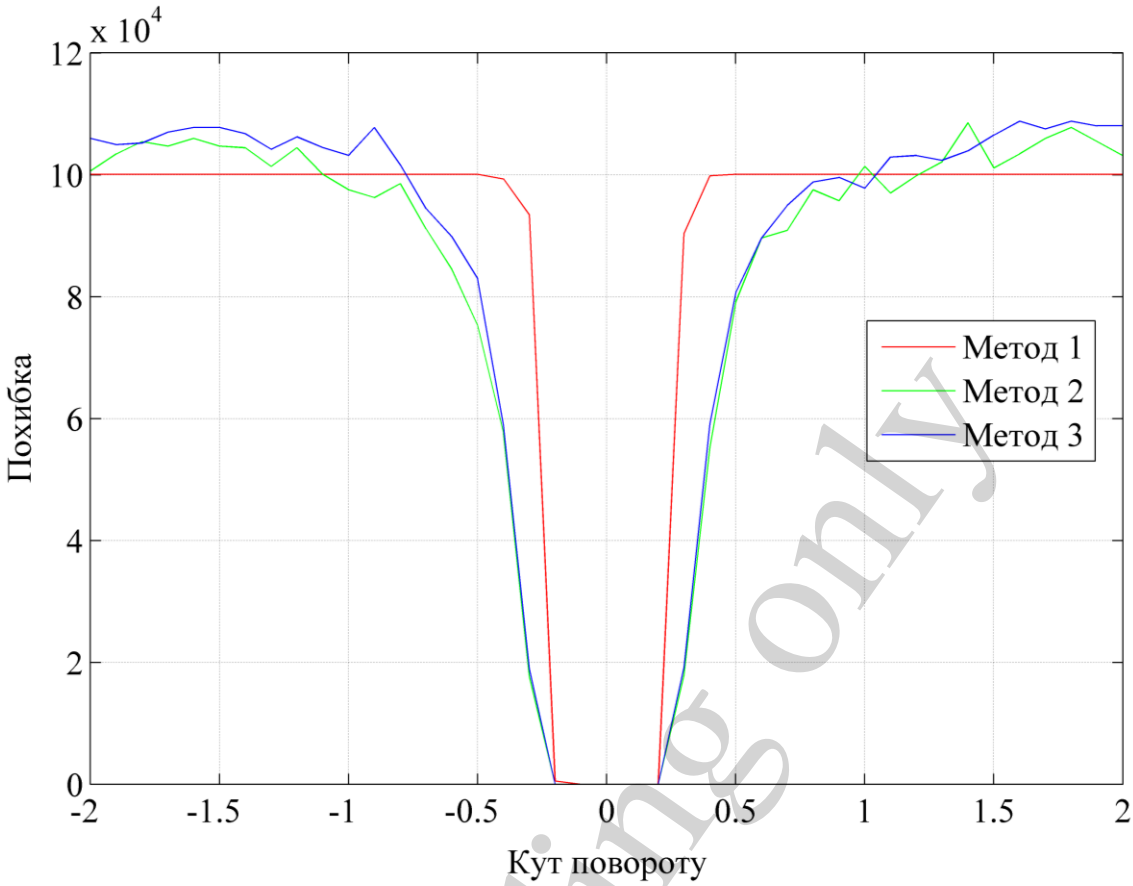


Рис. 19. Графіки залежності кількості помилок від параметрів шуму

а *б*

Рис. 20. Згладжені зображення-контейнери: *а* – оригінальне зображення; *б* – повернуте зображення, кут повороту 10°

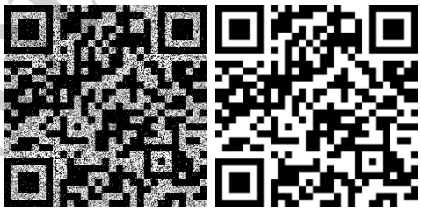
Наступним етапом було дослідження впливу видалення частини зображення – центрального квадрата зі стороною *a*=0:50:900. Результати наведено на рис. 24–29.

Для кожного методу фільтрації наведено графіки залежності кількості помилок від розмірів видаленого квадрата (рис. 30).

Рис. 21. Знаходження відповідних точок дискрипторів Oriented FAST and Rotated BRIEF

а *б* *в*

Рис. 22. Компенсація повороту: *а* - зображення-контейнер; *б* - виділення цифрового водяного знаку; *в* - відновлення правильного розташування пікселів у цифровому водяному знаку



а *б*

Рис. 23. Перший метод фільтрації: *а* - бінаризація зображення; *б* - застосування операції статистичної моди до кожної клітинки

При досліджені впливу компресії зображення за допомогою алгоритму Jpeg у залежності від значення параметра якості рис. 31–34 можна побудувати наступні графіки (рис. 35).

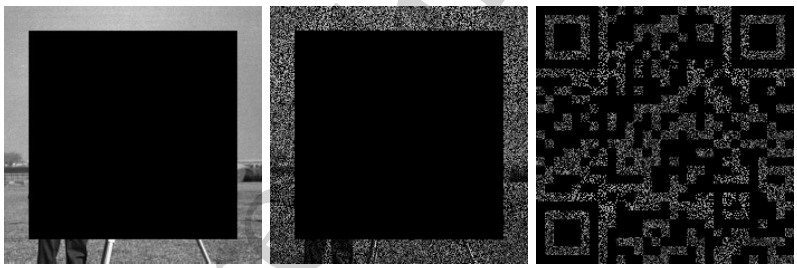
Далі досліджувався вплив компресії зображення за допомогою алгоритму Jpeg у залежності від значення параметра якості q=1:100. Результати наведено на рис. 31–34.

а *б* *в*

Рис. 24. Другий метод фільтрації: *а* - усереднення бінаризованого зображення по кожній клітинці; *б* - бінаризація зображення

а *б*

Рис. 25. Третій метод фільтрації: *а* - усереднення зображення по кожній клітинці; *б* - бінаризація зображення; *в* - різниця між фільтрованим зображенням і оригінальним QR кодом

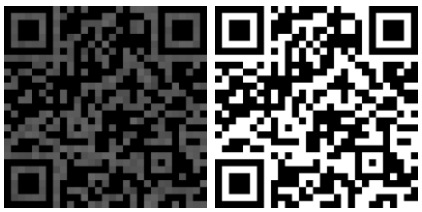


а *б* *в*

Рис. 26. Вплив видалення частини зображення: а - видалення центрального квадрата зі стороною *а*=750; *б* - виділення цифрового водяного знаку; *в* - відновлення правильного розташування пікселів у цифровому водяному знаку

а *б* *в*

Рис. 27. Перший метод фільтрації: *а* - бінаризація зображення; *б* - застосування операції статистичної моди до кожної клітинки – всі результуючі значення рівні 0; *в* - різниця між фільтрованим зображенням і оригинальним QR кодом



а *б*

Рис. 28. Другий метод фільтрації: *а* – усереднення бінаризованого зображення по кожній клітинці; *б* – бінаризація зображення

а *б*

Рис. 29. Третій метод фільтрації: *а* – усереднення зображення по кожній клітинці; *б* – бінаризація зображення

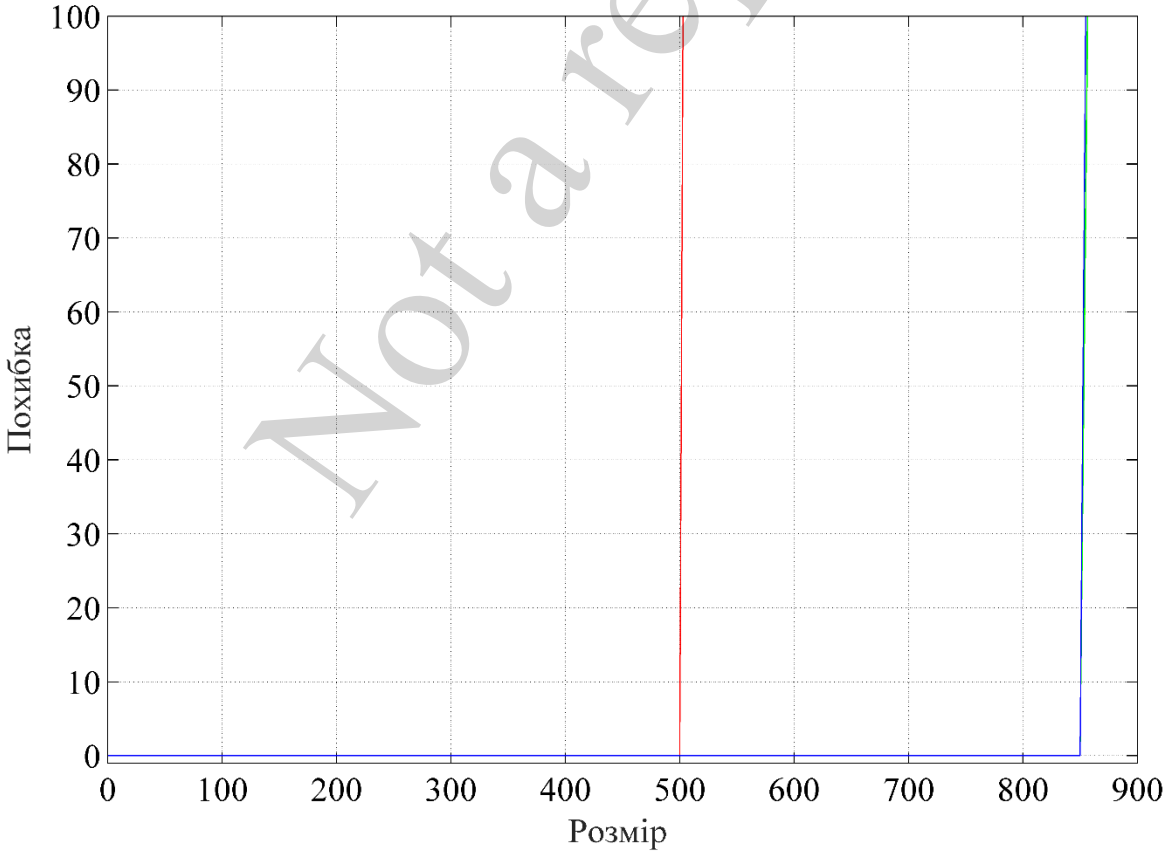


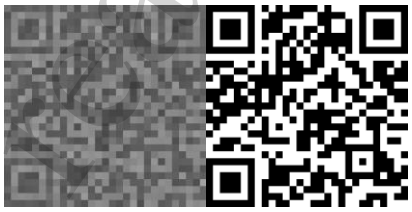
Рис. 30. Графіки залежності кількості помилок від розмірів видаленого квадрата

а *б* *в*

Рис. 31. Вплив Jpeg-компресії зображення: *а* – Jpeg-компресія, *q*=9; *б* – виділення цифрового водяного знаку; *в* - відновлення правильного розташування пікселів у цифровому водяному знаку

а *б* *в*

Рис. 32. Перший метод фільтрації: *а* – бінаризація зображення; *б* – застосування операції статистичної моди до кожної клітинки; *в* – різниця між фільтрованим зображенням і оригинальним QR кодом



а *б*

Рис. 33. Другий метод фільтрації: *а* – усереднення бінаризованого зображення по кожній клітинці; *б* – бінаризація зображення

Далі була проведена оцінка стійкості запропонованої методики.

При оцінці надійності запропонованої методики використовувалось п’ять типів атак:

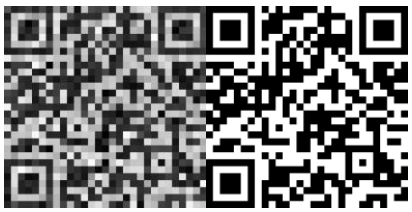
– додавання нормально розподіленого шуму із заданим середнім і дисперсією;

– додавання шуму типу «сіль-і-перець» із заданою густиною;

– поворот на заданий кут;

– видалення частини зображення заданого розміру;

– jpeg-компресія із заданим параметром якості.



а *б*

Рис. 34. Третій метод фільтрації: *а* – усереднення зображення по кожній клітинці; *б* – бінаризація зображення

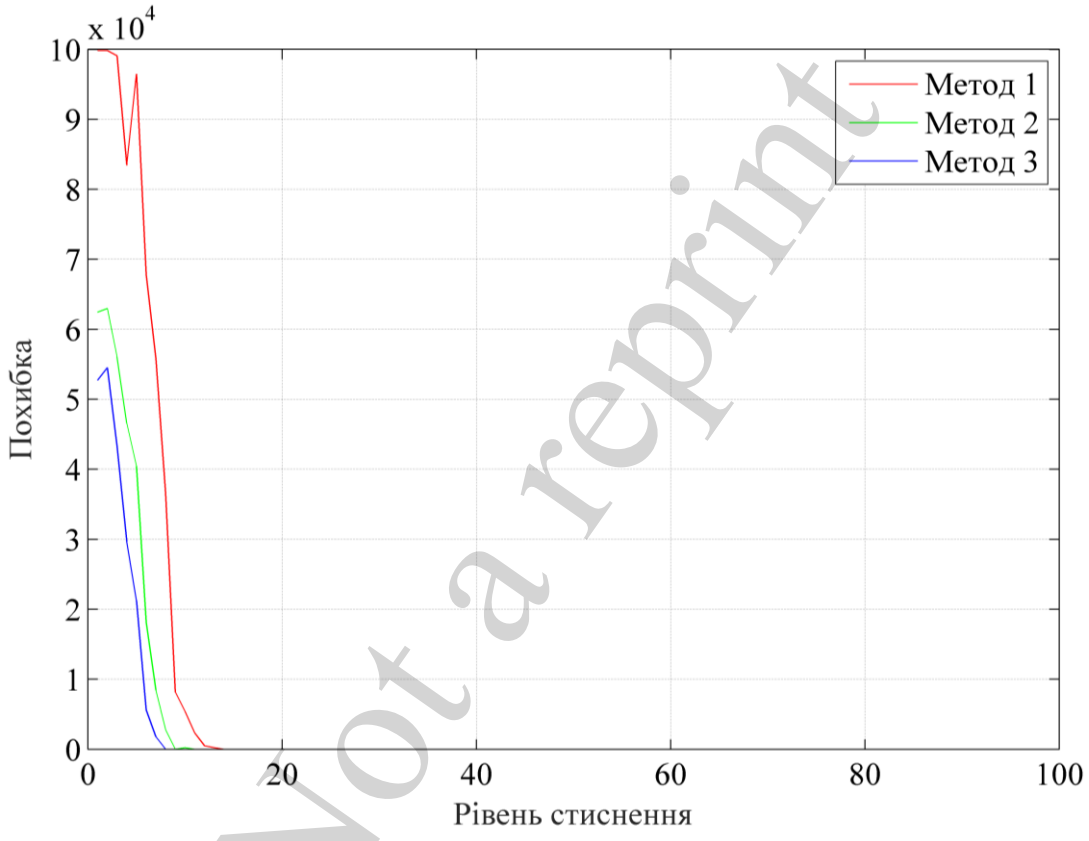


Рис. 35. Графіки залежності кількості помилок від параметра якості

Кожен тип атак включав по 500 різних варіацій цих атак. Результати тестування представлені в табл. 1.

Таблиця 1

Результати оцінки надійності

Методи вбудови цифрових водяних знаків	оцінювати надійність методу нанесення цифрового водяного знаку
Класичний метод нанесення цифрового водяного знаку з використанням вейвлет перетворень	0,6348
Нанесення цифрового водяного знаку на основі вейвлет перетворень з використанням запропонованої методики	0,8344

6. Обговорення результатів дослідження методики підвищення стійкості вбудови цифрових водяних знаків.

Описаний у роботі метод псевдоголографічного кодування цифрових водяних знаків є ефективним для всіх типів атак, що розглядалися, окрім повороту зображення. Найбільш ефективним цей метод є при втраті частини зображення.

Проаналізувавши графіки на рис. 7–9, можна зробити висновок, що найбільш ефективним є третій метод фільтрації.

Як видно з графіку рис. 14, другий і третій методи фільтрації є ефективними і дають співмірні результати.

Дослідження атаки типу «поворот» проводилося в два етапи. На першому етапі досліджувався вплив повороту зображення на кути φ=-2°:0,1°:2°. Для кожного методу фільтрації наведено графіки залежності кількості помилок від кута повороту (рис. 19).

Проаналізувавши отримані результати підчас поворотів зображення можна зробити такі висновки. По-перше, без компенсації повороту всі методи фільтрації для даного типу атаки є однаково неефективними – якщо зображення повернуте на кут, що більший ніж 0.2°, то коректне виділення цифрового водяного знаку є неможливим. По-друге, використовуючи запропонований метод компенсації, всі три методи фільтрації працюють абсолютно безпомилково в усьому діапазоні досліджуваних кутів φ=–10°:10°.

При атаці видаленні частини зображення з графіку рис. 30 видно, що найбільш ефективним є третій метод фільтрації.

При досліджені впливу компресії зображення за допомогою алгоритму Jpeg, у залежності від значення параметра якості (рис. 31–34), видно (рис. 35), що всі три методи дають співмірні результати, найбільш ефективним є третій метод фільтрації.

Як можна побачити з результатів тестування, за рахунок використання псевдоголографічного кодування забезпечується неоднорідність вбудови цифрового водяного знаку в зображення контейнер. Це дозволяє підвищити стійкість методу до втрати частини пікселей цифрового водяного знаку. А методи фільтрації цифрового водяного знаку дозволяють по статистичним ознакам відновити втрачену інформацію.

Таким чином, виходячи з результатів, наведених в табл. 1, можна сказати, що використання запропонованої методики підвищило надійність методу на 20 %.

Вище зазначене дозволяє визначити, що запропонована методика має переваги в тому, що в незалежності від методу вбудови цифрового водяного знаку буде забезпечуватися приріст стійкості.

Для розвитку запропонованої методики планується в подальшому провести дослідження методів псевдоголографічного кодування з застосуванням теорії хаосу.

6. Висновки

1. Розроблена функціональна модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення, основана

на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку. Описаний у роботі метод псевдоголографічного кодування цифрових водяних знаків є ефективним для протидії усім типам атак, що розглядалися, окрім повороту зображення. Проведення комплексної оцінки методики підвищення стійкості методу вбудови цифрового водяного знаку на основі Вейвлет перетворень показало, що її використання на 20 % покращує стійкість до різних типів атак.

2. В роботі представлено показник оцінки стійкості методів нанесення цифрових водяних знаків, який враховує всі типи атак і дозволяє провести комплексну оцінку стійкості методу вбудови цифрових водяних знаків.

3. Проведено експериментальне дослідження щодо запропонованої методики. Найбільш ефективною ця методика є при втраті частини зображення. При попередній фільтрації цифрового водяного знаку найбільш ефективним є третій метод фільтрації. Цей метод і представляє собою усереднення по клітинці і подальшу бінаризацію. Найменш ефективним є перший метод бінаризації і знаходження статистичної моди по клітинці. Бінаризацію доцільно проводити за алгоритмом Отсу. Для атаки афінного типу, що представляє собою поворот зображення, даний метод є ефективним тільки при компенсації повороту. Для оцінки кута повороту знаходиться матриця афінного перетворення, що отримується по узгодженому набору відповідних ORB-дескрипторів. Використання цього методу дозволяє безпомилково виділяти цифровий водяний знак для всього діапазону кутів, що досліджувалися.

Література

1. Patel, S. B., Mehta, T. B., Pradhan, S. N. (2011). A unified technique for robust digital watermarking of colour images using data mining and DCT. International Journal of Internet Technology and Secured Transactions, 3 (1), 81. doi: https://doi.org/10.1504/ijitst.2011.039680
2. Gao, X., Deng, C., Li, X., Tao, D. (2010). Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40 (3), 278–286. doi: https://doi.org/10.1109/tsmcc.2009.2037512
3. Seo, J. S., Yoo, C. D. (2006). Image watermarking based on invariant regions of scale-space representation. IEEE Transactions on Signal Processing, 54 (4), 1537–1549. doi: https://doi.org/10.1109/tsp.2006.870581
4. Aslantas, V. (2008). A singular-value decomposition-based image watermarking using genetic algorithm. AEU - International Journal of Electronics and Communications, 62 (5), 386–394. doi: https://doi.org/10.1016/j.aeue.2007.02.010
5. Loukhaoukha, K., Nabti, M., Zebbiche, K. (2014). A robust SVD-based image watermarking using a multi-objective particle swarm optimization. Opto-Electronics Review, 22 (1). doi: https://doi.org/10.2478/s11772-014-0177-z
6. Wei, Z. H., Qin, P., Fu, Y. Q. (1998). Perceptual digital watermark of images using wavelet transform. IEEE Transactions on Consumer Electronics, 44 (4), 1267–1272. doi: https://doi.org/10.1109/30.735826

7. Santhi, V., Rekha, N., Tharini, S. (2008). A hybrid block based watermarking algorithm using DWT-DCT-SVD techniques for color images. 2008 International Conference on Computing, Communication and Networking. doi: https://doi.org/10.1109/icccnet.2008.4907259

8. Divecha, N. H., Jani, N. (2012). Image Watermarking Algorithm using DCT, DWT and SVD. IJCA Proceedings on National Conference on Innovative Paradigms in Engineering and Technology (NCIPET 2012), 13–16.

9. Singh, A. K. (2016). Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimedia Tools and Applications, 76 (6), 8881–8900. doi: https://doi.org/10.1007/s11042-016-3514-z

10. Bruckstein, A. M., Holt, R. J., Netravali, A. N. (1997). Holographic image representations: the subsampling method. Proceedings of International Conference on Image Processing. doi: https://doi.org/10.1109/icip.1997.647439

11. Bruckstein, A. M., Holt, R. J., Netravali, A. N. (1998). Holographic representations of images. IEEE Transactions on Image Processing, 7 (11), 1583–1597. doi: https://doi.org/10.1109/83.725365

12. Markovskii, A. V. (2001). On Quasiholographic Coding of Digital Images. Automation and Remote Control 62, 1688–1697. doi: https://doi.org/10.1023/A:1012470618018

13. Кузнецов, О. П., Марковский, А. В. (2002). Квазиголографический подход к кодированию графической информации. Искусственный интеллект, 2, 474–482.

14. Dovgard, R. (2004). Holographic Image Representation With Reduced Aliasing and Noise Effects. IEEE Transactions on Image Processing, 13 (7), 867–872. doi: https://doi.org/10.1109/tip.2004.827228

15. Маковейчук, О. М. (2019). Новий тип маркерів доповненої реальності. Сучасні інформаційні системи, 3 (3), 43–48. doi: https://doi.org/10.20998/2522-9052.2019.3.06

16. Маковейчук, О. М., Рубан, І. В., Худов, Г. В. (2019). Використання генетичних алгоритмів для знаходження інверсних псевдовипадкових блочних перестановок. Системи управління, навігації та зв'язку, 4, 72–81. doi: https://doi.org/10.26906/sunz.2019.4.072

17. Xia, X. G., Boncelet, C., Arce, G. (1998). Wavelet transform based watermark for digital images. Optics Express, 3 (12), 497. doi: https://doi.org/10.1364/oe.3.000497

18. Lai, C.-C., Tsai, C.-C. (2010). Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. IEEE Transactions on Instrumentation and Measurement, 59 (11), 3060–3063. doi: https://doi.org/10.1109/tim.2010.2066770

19. Yusof, Y., Khalifa, O. O. (2007). Digital watermarking for digital images using wavelet transform. 2007 IEEE International Conference on Telecommunications

and Malaysia International Conference on Communications. doi: https://doi.org/10.1109/ictmicc.2007.4448569

20. Mallat, S. G. (1989). A theory for multiresolution signal decomposition: the wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 11 (7), 674–693. doi: https://doi.org/10.1109/34.192463

21. Daubechies, I. (1992). Ten Lectures on Wavelets. CBMS-NSF Regional Conference Series in Applied Mathematics. doi: https://doi.org/10.1137/1.9781611970104

22. Otsu, N. (1979). A Threshold Selection Method from Gray-Level Histograms. IEEE Transactions on Systems, Man, and Cybernetics, 9 (1), 62–66. doi: https://doi.org/10.1109/tsmc.1979.4310076

23. Bradley, D., Roth, G. (2007). Adaptive Thresholding using the Integral Image. Journal of Graphics Tools, 12 (2), 13–21. doi: https://doi.org/10.1080/2151237x.2007.10129236

24. Yeromina, N., Petrov, S., Antonenko, N., Vlasov, I., Kostrytsia, V., Korshenko, V. (2020). The Synthesis of the Optimal Reference Image Using Nominal and Hyperordinal Scales. (2020). International Journal of Emerging Trends in Engineering Research, 8 (5), 2080–2084. doi: https://doi.org/10.30534/ijeter/2020/98852020

25. Liashko O., Klindukhova, V., Yeromina, N., Karadobrii, T., Bairamova, O., Dorosheva, A. (2020). The Criterion and Evaluation of Effectiveness of Image Comparison in Correlation-Extreme Navigation Systems of Mobile Robots. International Journal of Emerging Trends in Engineering Research, 8 (6), 2841–2847, doi: https://doi.org/10.30534/ijeter/2020/97862020