УДК 004.932

В. П. Майданюк, канд. техн. наук, доцент
О. Н. Романюк, д-р техн. наук, професор
І. Р. Арсенюк, канд. техн. наук, доцент
О. О. Складанюк, аспірант
М. Л. Нечипорук, аспірант
[1,2,3,4,5]Вінницький національний технічний університет, Україна
[1]maidaniuk2000@gmail.com

Приховування рентгенівських зображень у рентгенівських зображеннях із використанням стеганографічних перетворень

Забезпечення конфіденційності біомедичних зображень є важливою задачею сучасних медичних інформаційних систем, особливо в умовах розвитку телемедицини. Рентгенівські зображення широко використовуються для діагностики та передаються через мережі, що підвищує ризик несанкціонованого доступу та витоку інформації. Традиційні криптографічні методи забезпечують високий рівень захисту даних, однак не приховують самого факту передачі, що обмежує їх ефективність у ряді практичних застосувань. У роботі досліджується стеганографічний підхід до захисту біомедичних зображень, який передбачає приховування одного рентгенівського зображення в іншому рентгенівському зображенні. Метою дослідження є забезпечення високої якості зображення-контейнера та мінімізація візуальних спотворень при вбудовуванні. Використано методи приховування у просторовій та частотній областях, зокрема із застосуванням коефіцієнтів перетворення Уолша-Адамара. Експериментальні результати показали, що відмова від нормалізації коефіцієнтів при прямому перетворенні та її виконання лише на етапі зворотного перетворення дозволяє зменшити рівень спотворень і забезпечити високу якість зображення навіть при повному заповненні контейнера. Встановлено, що використання коефіцієнтів перетворення забезпечує більшу інформаційну ємність контейнера порівняно з методами просторової області. Отримані результати підтверджують ефективність використання рентгенівських зображень як контейнерів для приховування зображень того ж типу та забезпечують високу стеганостійкість і непомітність змін.

Ключові слова: стеганографія, біомедичні зображення, рентгенівські зображення, перетворення Уолша-Адамара, приховування даних

DOI: 10.31474/1996-1588-2026-1-42-43-53

Вступ

Забезпечення конфіденційності біомедичних зображень [1,2] є важливою задачею сучасних медичних інформаційних систем, особливо в умовах активного розвитку телемедицини та цифрових технологій обробки медичних даних. Рентгенівські зображення широко використовуються [3,4] для діагностики різноманітних захворювань і є невід'ємною частиною клінічної практики. Водночас такі зображення часто передаються через відкриті або напівзахищені мережі, що підвищує ризик несанкціонованого доступу, витоку інформації та її несанкціонованої модифікації.

Порушення цілісності або конфіденційності рентгенівських знімків може призвести не лише до розкриття персональних даних пацієнтів, але й до спотворення діагностичної інформації, що, у свою чергу, може вплинути на прийняття клінічних рішень. У зв'язку з цим забезпечення надійного захисту біомедичних зображень є актуальною науково-практичною задачею.

Традиційні підходи до захисту даних базуються на використанні криптографічних методів, які забезпечують високий рівень конфіденційності шляхом шифрування інформації. Однак такі методи не приховують самого факту передачі даних, що може бути критичним у деяких застосуваннях, зокрема при передачі медичних зображень у відкритих мережах. У зв'язку з цим зростає інтерес до стеганографічних методів, які дозволяють приховувати інформацію всередині інших даних, не викликаючи підозри щодо наявності прихованого повідомлення.

Особливий інтерес становить використання рентгенівських зображень як контейнерів для приховування зображень того ж типу. Такий підхід дозволяє враховувати специфічні властивості медичних зображень, зокрема їх статистичні характеристики, обмежений динамічний діапазон та наявність областей із плавною зміною яскравості. Це створює передумови для

підвищення інформаційної ємності контейнера та забезпечення високої якості зображення після вбудовування.

У роботі розглядається задача приховування одного рентгенівського зображення в іншому рентгенівському зображенні із забезпеченням високої якості контейнера та мінімізації візуальних спотворень. Для цього досліджуються стеганографічні методи у просторовій та частотній областях, зокрема із застосуванням коефіцієнтів перетворення Уолша-Адамара, що дозволяє підвищити ємність контейнера та зберегти високу якість зображення.

Огляд методів захисту біомедичних зображень

Існуючі підходи до захисту біомедичних зображень [1-4] включають криптографічні методи [5,6], методи контролю доступу та стеганографічні методи [7,8].

Шифрування даних: шифрування біомедичних зображень перед їх зберіганням або передачею є одним з найефективніших способів захисту. Використання алгоритмів шифрування, таких як AES (Advanced Encryption Standard), забезпечує високий рівень безпеки.

Контроль доступу: впровадження систем контролю доступу, які обмежують доступ до біомедичних зображень лише авторизованим користувачам. Це може включати використання паролів, біометричної аутентифікації або багатофакторної аутентифікації.

Аудит та моніторинг: регулярний аудит та моніторинг доступу до біомедичних зображень допомагає виявляти та запобігати несанкціонованому доступу. Це включає ведення журналів доступу та аналіз підозрілої активності [1].

Використання VPN: віртуальні приватні мережі (VPN) забезпечують безпечний канал для передачі даних через Інтернет, що допомагає захистити біомедичні зображення від перехоплення під час передачі. Захист хмарних сховищ: якщо біомедичні зображення зберігаються в хмарі, важливо використовувати хмарні сервіси з вбудованими функціями шифрування та контролю доступу.

Існують специфічні методи захисту біомедичних зображень, які враховують особливості цих даних. Деякі з них такі [4]. Водяні знаки: вбудовування водяних знаків у біомедичні зображення допомагає ідентифікувати джерело зображення та виявляти несанкціоноване копіювання або модифікацію. Стиснення з шифруванням: використання методів стиснення даних разом із шифруванням дозволяє зменшити обсяг даних для зберігання та передачі, одночасно забезпечуючи їх захист.

Анонімізація даних: видалення або маскування особистої інформації з біомедичних зображень перед їх обробкою або передачею допомагає захистити конфіденційність пацієнтів.

Блокчейн: використання блокчейн-технологій для зберігання та передачі біомедичних зображень забезпечує високий рівень безпеки та прозорості, оскільки кожна транзакція записується у незмінний реєстр [1]. Машинне навчання для виявлення аномалій: Використання алгоритмів машинного навчання для аналізу доступу до біомедичних зображень та виявлення підозрілої активності може допомогти запобігти несанкціонованому доступу.

Разом з тим, недостатня увага приділяється стеганографічним методам захисту біомедичних зображень. Криптографічні методи забезпечують високий рівень захисту, проте не приховують самого факту передачі інформації. Стеганографічні методи, навпаки, дозволяють приховувати інформацію всередині інших даних, зокрема цифрових зображень. Важливим аспектом при цьому є вибір контейнера. Найбільшу місткість забезпечують графічні файли, у яких можна модифікувати молодші біти пікселів без помітного погіршення якості зображення.

Існують два методи приховування [7,8] інформації в зображеннях:

- у просторовій області (безпосередньо в пікселях);
- у частотній області (у коефіцієнтах перетворень, таких як Фур'є, Уолша-Адамара або дискретне косинусне перетворення).

Методи частотної області потребують більших обчислювальних витрат, проте дозволяють підвищити ємність контейнера та стеганостійкість [9-11]. Особливий інтерес становить підхід, при якому одне рентгенівське зображення приховується в іншому рентгенівському зображенні [9-10]. Рентгенівські знімки характеризуються вузьким динамічним діапазоном та наявністю ділянок із плавною зміною яскравості, що створює передумови для збільшення кількості прихованих бітів у кожному пікселі без помітної деградації якості. Таким чином, стеганографічні методи, орієнтовані на використання рентгенівських зображень як контейнерів для приховування зображень того ж типу, є перспективним напрямом досліджень.

Метою роботи є забезпечення високої якості зображення-контейнера при приховуванні одного рентгенівського зображення в іншому та зменшення обчислювальних витрат.

Розробка стеганографічних методів захисту зображень

Основна ідея роботи полягає у використанні одного рентгенівського зображення як контейнера

для приховування іншого рентгенівського зображення. На відміну від традиційних підходів, де контейнер і повідомлення мають різну природу, використання однорідних даних забезпечує:

- підвищену непомітність;
- кращу адаптацію алгоритмів;
- ефективніше використання інформаційної ємності.

Рентгенівські зображення характеризуються:

- вузьким динамічним діапазоном;
- плавними переходами яскравості;
- низькою чутливістю до незначних змін молодших біт.

Це дозволяє приховувати значну кількість інформації без помітних спотворень.

Нехай задано:

- контейнерне зображення $C(x,y)$ – рентгенівський знімок;
- зображення, що приховується $S(x,y)$ – рентгенівський знімок.

Необхідно отримати зображення $C'(x,y)$, яке:

- візуально не відрізняється від $C(x,y)$;
- містить вбудовану інформацію $S(x,y)$;
- дозволяє відновлення $S(x,y)$ за наявності ключа.

Процес вбудовування описується як:

$$C'(x,y) = F(C(x,y), S(x,y), K) \quad (1)$$

де K – ключ, що визначає псевдовипадкове розсіювання.

Для оцінки якості використовується метод експертних оцінок та середньоквадратичне відхилення (СКВ):

$$MSE = \frac{1}{M*N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y) - C'(x,y))^2, \quad (2)$$

де M, N – розміри сторін зображення.

Недоліки методів приховування в частотній області можна значно зменшити, якщо використовувати, наприклад, перетворення Уолша-Адамара для обчислення якого використовуються лише операції додавання та віднімання.

Пряме і зворотне перетворення, як правило, визначається з однаковою константою нормування так [11,12]:

$$[F(\mathrm{u,v})] = \frac{1}{N}[H(\mathrm{u,v})][f(\mathrm{x,y})][H(\mathrm{u,v})], \quad (3)$$

$$f(\mathrm{x,y}) = \frac{1}{N}[H(\mathrm{u,v})][F(\mathrm{u,v})][H(\mathrm{u,v})],$$

де $H(u,v)$ – матриця Адамара, упорядкована за Уолшом;

$f(x,y)$ – значення пікселя початкового зображення;

$F(u,v)$ – коефіцієнти (трансформанти) перетворення Уолша-Адамара.

Швидке обчислення перетворення Уолша-Адамара у двовимірному випадку зручно виконувати у два етапи.

Перший етап: виконується одномірне перетворення кожного рядка (або стовпця) фрагмента розміром 8×8 елементів. Отримані коефіцієнти зберігаються в пам'яті.

Другий етап: після обробки всіх рядків фрагмента виконується одномірне перетворення кожного стовпця (або рядка) масиву коефіцієнтів, отриманих на першому етапі.

Загальна кількість операцій для перетворення масиву розміром $N \times N$ при цьому становить:

$$m_0 = 2N2\,(N-1).$$

Без застосування швидкого алгоритму обчислення перетворення Уолша-Адамара двовимірне перетворення виконується шляхом прямого перемноження вихідного масиву на матрицю базисних функцій. Це передбачає виконання великої кількості операцій через повне матричне множення. Для масиву розміру $N \times N$:

$$m = N^2\,(N^2-1).$$

При $N = 8, m/m_0 = 4{,}5$.

Тобто, виконання двовимірного перетворення через два послідовних одномірних дозволяє суттєво зменшити кількість арифметичних операцій. Матриця Адамара розмірності 8×8 елементів для одновимірного перетворення упорядкована за Уолшом має такий вигляд:

$$\mathrm{H} = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{vmatrix}$$

Саме ця матриця буде використана для виконання перетворення Уолша-Адамара фрагментів розміром 8×8. Процедура передбачає застосування одномірного перетворення до кожного рядка даних, а потім застосування одномірного перетворення до кожного стовпця даних, отриманих після першого етапу. Пряме і зворотне перетворення симетричні. Різниця тільки в тому, що пряме перетворення передбачає квантування трансформант, тобто цілочисельне ділення кожного значення на відповідний коефіцієнт квантування, зворотне перетворення включає деквантування, коли кожне значення трансформанти множиться на відповідний коефіцієнт квантування. Ця симетрія та чітка структура алгоритму забезпечують його ефективність у багатьох задачах, зокрема в обробці

зображень, стисканні даних і спектральному аналізі. Незалежно від типу даних (просторові або частотні) контейнера алгоритм приховування однаковий в обох випадках. Алгоритм приховування включає такі кроки.

Крок 1. Розсіювання бітів зображення, що захищається в площині зображення контейнера (або площині коефіцієнтів перетворення) з використанням конгруентного генератора псевдовипадкових чисел (ПВЧ) та їх гамування. Для кожної складової кольору (RGB) використовується свій генератор ПВЧ. Він формує послідовності псевдовипадкових чисел $T(i)$ у відповідності з співвідношенням [5]:

$$T(i+1) = (A \times T(i) + C) \bmod M \qquad (4)$$

де $T(0)$ – початкова величина, обрана як твірне число; A і C – константи.

Такий датчик ПВЧ генерує псевдовипадкові числа з визначеним періодом повторення, що залежить від обраних значень A і C. Лінійний конгруентний генератор має максимальну довжину $M = 2^n$ тільки тоді, коли $C -$ непарне; $A \bmod 4 = 1$. Значення $T(0), A, C$ можуть бути ключем шифру. А в якості значення M вибирається найближче число кратне «2» більше кількості пікселів в зображенні-контейнері, що підвищує криптостійкість шифрування.

Крок 2. В кожному пікселі (або коефіцієнтах перетворення Уолша Адамара для складових кольору) контейнера приховується 12 біт зображення що захищається Для приховування використовуються 4 молодших біти в кожній складовій кольору. Причому дані, що приховуються в поточному пікселі контейнера належать різним пікселям зображення, що захищається. Блок-схема алгоритму приховування для однієї складової кольору просторовій області приведена на рис. 1, а в частотній на рис. 2.

Оцінка складності стеганографічного методу захисту зображень

У програмуванні, обчислювальну складність алгоритмів зазвичай оцінюють за кількістю дій, які виконує алгоритм та за обсягом задіяної пам'яті. У переважній більшості випадків, для позначення оцінки складності алгоритмів використовують так звану O-нотацію, в математиці таке позначення застосовують для порівняння асимптотичної поведінки функцій. O-нотація визначає функцію (назвемо її $g(n)$), яка показує, як буде змінюватися обчислювальна складність алгоритму зі зміною кількості вхідних даних у найгіршому для алгоритму випадку [13].

Знайдемо оцінку складності для стандарту шифрування DES. В цьому стандарті до блоку, що підлягає шифруванню, застосовується початкова перестановка (IP), потім складна обчислювальна процедура в залежності від ключа, а в кінці обернена перестановка (IP^{-1}). Обчислювальна процедура виконується з використанням мережі Фейстеля, що містить 16 каскадів.

На кожному етапі виконується зчитування блоку з пам'яті, операція додавання за модулем «2» і запис в пам'ять. У сучасних процесорах найбільш повільною є операції читання-запису оперативного запам'ятовуючого пристрою (ОЗП), оскільки внутрішні операції в процесорі виконуються на частотах 2 ГГц або більших на декількох конвеєрах, а запис-читання пам'яті на частотах лише 200-300 МГц, тому оцінимо кількість звертань до ОЗП. Будемо вважати, що процесор може читати і писати пам'ять блоками по n біт за один машинний цикл читання, а також не будемо враховувати складність генерації ключів шифрування для кожного етапу. Тобі в алгоритмі DES початкова перестановка вимагає як мінімум 2 операції – читати і писати. Якщо кількість каскадів мережі Фейстеля k, то на кожному каскаді також потрібно виконати 2 операції – читати і писати. І нарешті обернена перестановка також 2 операції. Таким чином: $g1(k) = 2k + 4$. Тобто, будемо вважати, що складність алгоритму DES $O(2k + 4)$ лінійно залежить лише від кількості каскадів мережі Фейстеля.

Оцінимо складність стеганографічних методів при тих же початкових умовах. Читання n біт зображення, що приховується вимагає 1 операції читання. Якщо в кожному пікселі приховується m біт, де $m < r$, де r – кількість біт на піксель, то потрібно $2 * (n/(m * r))$ операцій читання-запису. Тоді: $g2(m) = 1 + 2 * (n/(m * r))$. Наприклад, якщо $k = 16$, то $g1(k) = 36$. А для $g2(m)$ при $n = 64$, $r = 8, m = 1$ (найгірший випадок) маємо: $g2(m) = 1 + 2 * (64/(1 * 8)) = 17$. Тобто запропонований метод забезпечує меншу складність алгоритму і відповідно вищу швидкість роботи. Залежність $g2(m)$ наведена на рис. 3.

Результати досліджень

Для виконання досліджень мовою програмування C++ розроблено додаток Windows для дослідження методів захисту біомедичних зображень від несанкціонованого доступу шляхом виконання криптографічних та стеганографічних перетворень. Тестування роботи програми в режимі стеганографічного захисту в просторовій області. При приховуванні зображення в зображенні-контейнері головною вимогою є забезпечення таємності самого факту приховування. Тобто візуально зображення-контейнер не повинно відрізнятись після приховування від початкового.

При проведенні досліджень в якості контейнера виберемо зображення типу рентгенівське зображення та довільне зображення.

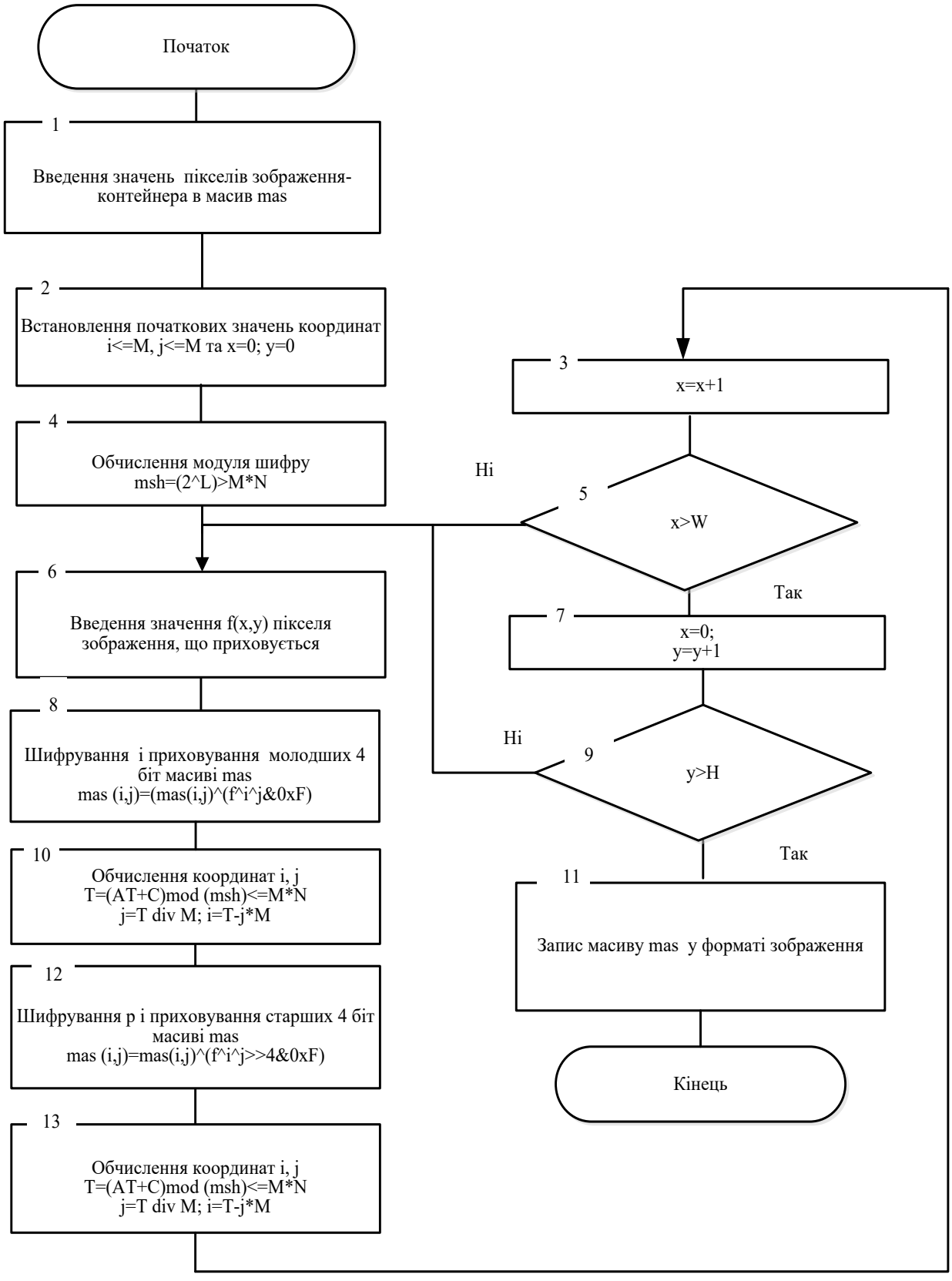

Рисунок 1 – Блок-схема алгоритму приховування в просторовій області

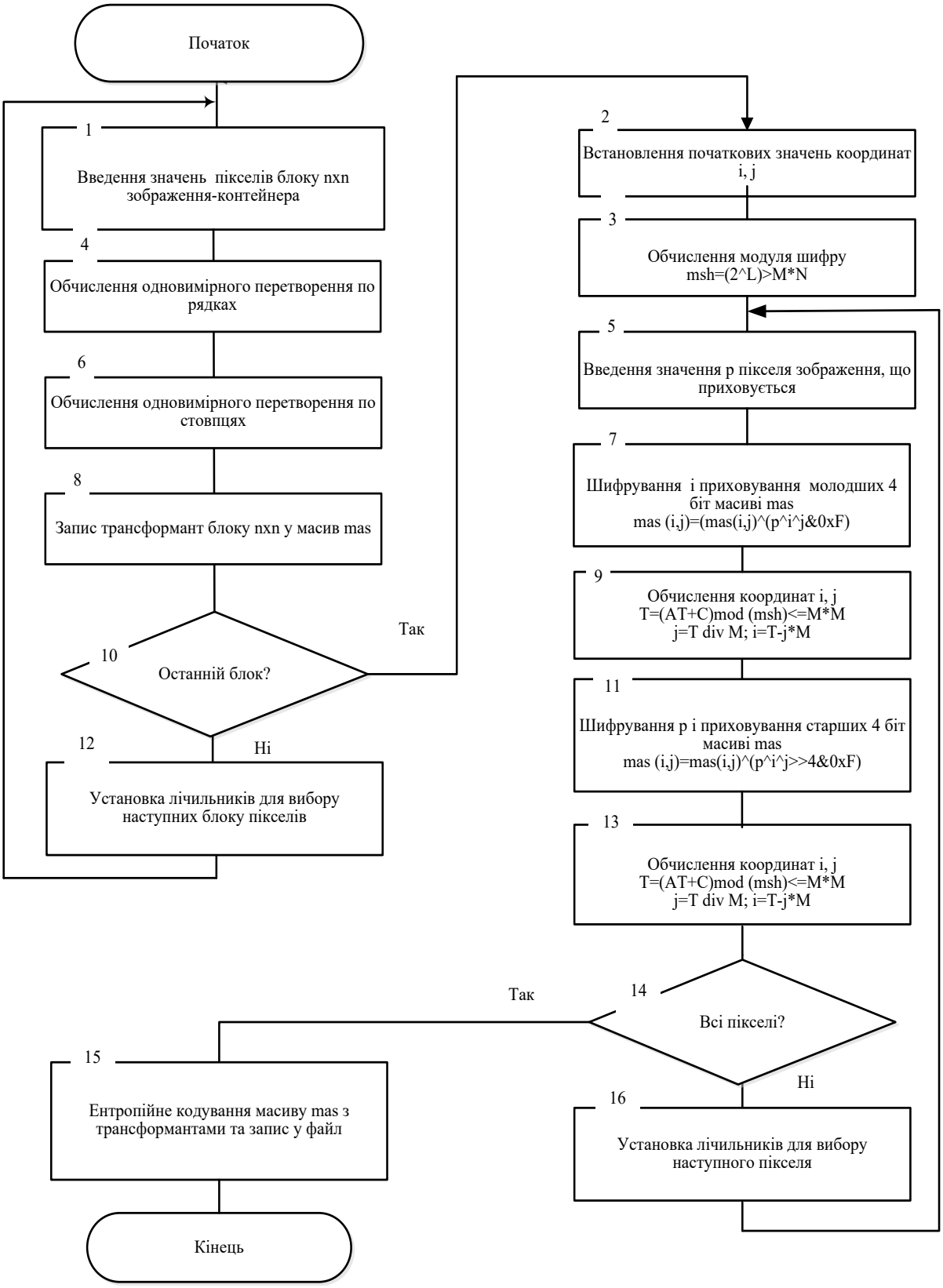

Рисунок 2 – Загальна блок-схема приховування в коефіцієнтах перетворення Уолша-Адамара

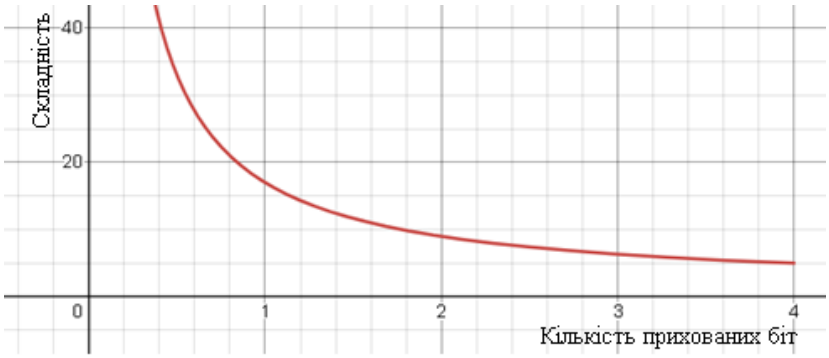

Рисунок 3 – Залежність складності алгоритму від кількості біт, що приховуються в одному пікселі

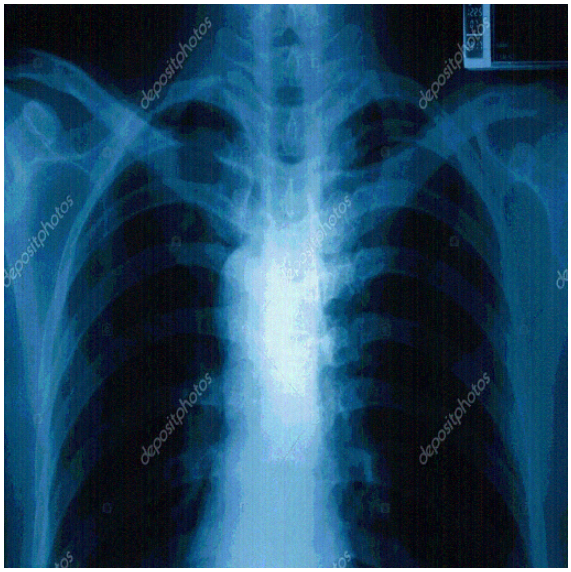

Рисунок 4 – Зображення-контейнер з вбудованим зображенням (5біт)
СКВ=9-10

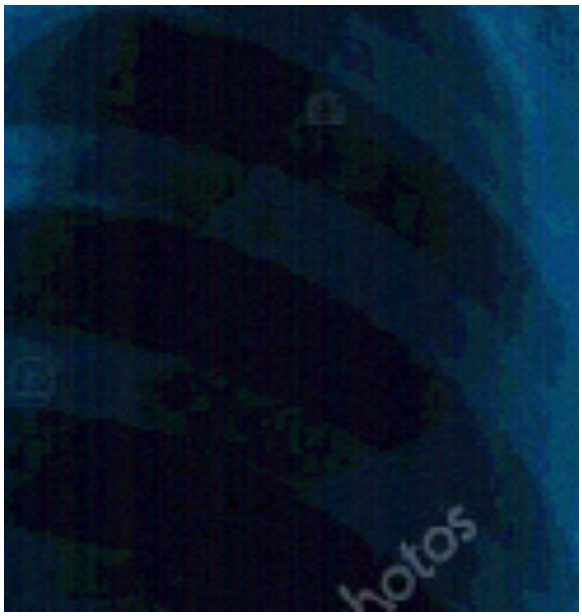

Рисунок 5 – Фрагмент зображення-контейнер з вбудованим зображенням (4біт). Повне заповнення контейнера, СКВ=6

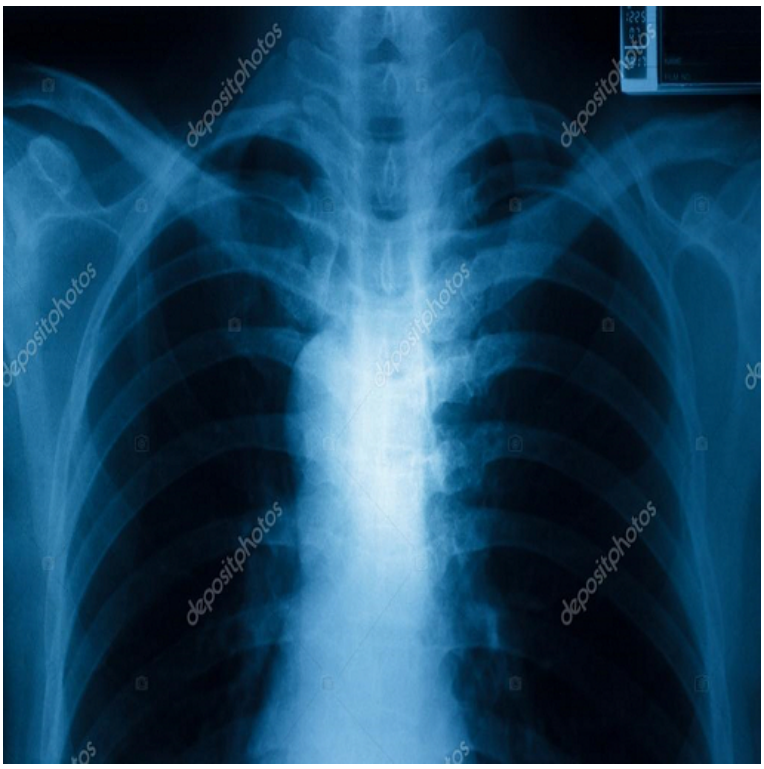

Рисунок 6 – Відновлене зображення-контейнер з вбудованим в ненормалізовані коефіцієнти Уолша-Адамара зображенням. Повне заповнення контейнера, СКВ =1

Таблиця 1 – Стеганографічний захист в частотній області при повному заповненню контейнера (4 біти на кожний коефіцієнт перетворення Уолша-Адамара)

Розмір початкового зображення, байт		Розмір зображення після приховування та ущільнення без втрат, байт	Середньо-квадратичне відхилення (СКВ)	Візуальна оцінка якості
786486 (color)	Нормалізація коефіцієнтів при прямому і зворотному перетворенні	532541	7	Погана, помітні зміни
	Нормалізація коефіцієнтів тільки при зворотному перетворенні	717101	1	Відмінна

Будемо досліджувати залежність візуальної якості зображення після вбудовування зображення, що захищається від кількості біт вбудованих у кожний піксель.

Вбудуємо по 5 біт в кожну складову кольору в зображення контейнер image1GK.bmp (рентгенівський знімок) та lena512.bmp (зображення в градаціях сірого). Вибір довільного зображення в градаціях сірого пояснюється тим, що на такому зображенні спотворення більш помітні у порівнянні з кольоровим. Вбудовується зображення image2Chr256.bmp (рентгенівське зображення) розміром 256x256. Результати наведено на рис. 4.

Спотворення помітні (рис. 4), тому необхідно зменшити кількість біт, що приховуються до 4. Для дослідження використаємо ті ж самі зображення в якості контейнера і зображення що приховується. Аналіз результатів дослідження показує, що спотворення

візуально непомітні при приховуванні по 4 біти в кожній складовій кольору пікселя, тобто 12 біт на піксель, СКВ=4. Але при розмірах зображення, що приховується, 256x256, контейнер розміром 512x512 заповнюється лише наполовину. Тому сформуємо зображення розміром 362x362, яке забезпечує повне заповнення контейнера розміром 512x512. Дійсно, 512x512=262144 пікселя.

Оскільки на 1 піксель приховуваного зображення потрібно 2 пікселя контейнера, то це значення поділити на 2: 262144:2=131072. Тоді сторона квадратного зображення не повинна перевищувати квадратний корінь з цього числа, тобто бути рівною 362. Результати досліджень для такого зображення наведено на рис. 5. Спотворення візуально помітні, про що свідчить і зростання СКВ до 6.

Тому можна зробити такі висновки: при приховуванні 4 біт в кожному пікселі кожної складової кольору кількість пікселів в контейнері повинна перевищувати кількість пікселів зображення, що приховуються, у 4 рази. Тоді заповнюваність контейнера не перевищуватиме половини можливої місткості і спотворення будуть непомітні.

Тестування роботи програми в режимі стеганографічного захисту в частотній області. Досліджується залежність якості відновленого зображення від кількості біт вбудованих в коефіцієнти перетворення Уолша-Адамара при розмірах фрагментів, які вибираються з зображення, 8x8. Всі коефіцієнти квантування встановлюються в значення «1», тобто використовуються режим «майже без втрат».

Розглянуто два варіанти приховування зображення у коефіцієнтах перетворення Уолша-Адамара:

- класичний варіант – нормалізація коефіцієнтів (ділення на 8) при прямому та зворотному перетворенні як у виразі (3);
- варіант без нормалізації при прямому перетворенні – ділення виконується лише при зворотному перетворенні (на 64).

Вбудовування здійснюється по 4 біти в кожен коефіцієнт для кожної складової кольору зображення-контейнера image1GK.bmp (рентгенівський знімок) розміром 512×512. Приховується зображення image2Chr256.bmp (рентгенівське зображення) розміром 256×256.

У випадку використання нормалізованих коефіцієнтів спотворення візуально непомітні, однак середньоквадратичне відхилення (СКВ) зростає на 1 у порівнянні з приховуванням у просторовій області. Це пояснюється тим, що похибка, яка виникає при зворотному перетворенні, розповсюджується на весь блок зображення.

При повному заповненні контейнера спостерігаються помітні регулярні спотворення. Тому було змінено умови експерименту: нормалізація коефіцієнтів виконується лише при зворотному перетворенні. Отримані результати (рис. 6, табл. 1) показали, що у цьому випадку спотворення є візуально непомітними, а значення СКВ становить 1, що є прийнятним з точки зору стеганостійкості.

Збільшення розміру файлу з коефіцієнтами після ущільнення без втрат пояснюється відсутністю нормалізації при прямому перетворенні. При цьому вплив на якість відновленого зображення зменшується, оскільки нормалізація виконується після зворотного перетворення шляхом цілочислового ділення на 64, що фактично усуває спотворення молодших бітів

Висновки

У роботі досліджено методи приховування одного рентгенівського зображення в іншому рентгенівському зображенні із використанням стеганографічних перетворень у просторовій та частотній областях.

Проведені дослідження показали, що найбільш ефективним є приховування у коефіцієнтах перетворення Уолша-Адамара, яке забезпечує найбільший об'єм контейнера та найвищу якість зображення-контейнера з вбудованим зображенням.

Встановлено, що відмова від нормалізації коефіцієнтів при прямому перетворенні та виконання нормалізації лише на етапі зворотного перетворення дозволяє зменшити візуальні спотворення та досягти високої якості контейнера навіть при повному його заповненні.

Таким чином, використання ненормалізованих коефіцієнтів перетворення Уолша-Адамара є доцільним для забезпечення високої якості зображення-контейнера та підвищення інформаційної ємності.

Разом з тим, результати дослідження визначають перспективні напрями подальших досліджень:

1) підвищення ємності контейнера за рахунок врахування частотних характеристик коефіцієнтів перетворення;
2) дослідження застосування інших ортогональних перетворень, зокрема дискретного косинусного, перетворення Фур'є та вейвлет-перетворень;
3) вивчення впливу квантування коефіцієнтів перетворень на ефективність стеганографічного захисту та ступінь ущільнення даних;
4) застосування методів штучного інтелекту, зокрема deep learning, для підвищення ефективності приховування біомедичних зображень.

Отримані результати підтверджують доцільність використання рентгенівських зображень як контейнерів для приховування зображень того ж типу, що забезпечує високу якість, стеганостійкість та непомітність внесених змін.

Література

1. Безпека та конфіденційність у віддаленій радіології. URL: https://radiolance.ua/bezpeka-ta-konfidentsijnist-u-viddalenij-radiologiyi/ (дата звернення: 21.02.2026).
2. Як захистити дані від несанкціонованого доступу? URL: https://cybercalm.org/novyny/yak-zahystyty-dani-vid-nesanktsionovanogo-dostupu-porady/ (дата звернення: 21.02.2026).
3. Коваль Л. Г. Обробка біомедичних зображень та реконструкція об'єктів : конспект лекцій. Вінниця : ВНТУ, 2020.
4. A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations / B. Zhang, B. Rahmatullah, S. L. Wang et al. *Multimedia Tools and Applications*. 2020. DOI:10.1007/s11042-020-09629-4.
5. Майданюк В. П., Романюк О. Н., Тужанський С. Є. Основи теорії інформації та кодування. Вінниця : ВНТУ, 2022.
6. Шифрування медичних зображень / О. О. Романюк, В. П. Майданюк, С. Є. Павлов та ін. *Медико-технічна співпраця заради перемоги: актуальні завдання медичної, біологічної фізики та інформатики* : матеріали III Всеукр. наук.-практ. конф. з міжнар. участю (м. Вінниця, 5–6 квіт. 2024 р.). Вінниця : Едельвейс, 2024. С. 86–89.
7. Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. Комп'ютерна стеганографія. Вінниця : ВНТУ, 2017.
8. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія : навч. посіб. Харків : ХНЕУ, 2011.
9. Майданюк В. П., Грицишин В. О. Захист біомедичних зображень від несанкціонованого доступу. *Інформаційні технології і автоматизація – 2024* : матеріали XVII міжнар. наук.-практ. конф. (м. Одеса, 31 жовт. – 1 листоп. 2024 р.). Одеса : ОНТУ, 2024. С. 200–201.
10. Грицишин В. О., Майданюк В. П. Використання стеганографії для захисту рентгенівських знімків. *Електронні інформаційні ресурси: створення, використання, доступ та управління* : зб. матеріалів Міжнар. наук.-практ. інтернет-конф. (м. Суми/Вінниця, 20–21 листоп. 2024 р.). Суми ; Вінниця : НІКО ; КЗВО «Вінницька академія безперервної освіти», 2024. С. 41.
11. Майданюк В. П., Грицишин В. О. Ущільнення зображень з використанням перетворення Уолша-Адамара. *Матеріали LII наук.-техн. конф. підрозділів ВНТУ* (м. Вінниця, 21–23 черв. 2023 р.). 2023.
12. Ущільнення медичних зображень / О. О. Романюк, В. П. Майданюк, С. Є. Павлов та ін. *Медико-технічна співпраця заради перемоги: актуальні завдання медичної, біологічної фізики та інформатики* : матеріали III Всеукр. наук.-практ. конф. з міжнар. участю (м. Вінниця, 5–6 квіт. 2024 р.). Вінниця : Едельвейс, 2024. С. 89–93.
13. Hopcroft J. E., Motwani R., Ullman J. D. Introduction to Automata Theory, Languages, and Computation. 2nd ed. Boston : Addison–Wesley, 2001. 521 p. URL: https://archive.org/details/introductiontoau00hopc (Last accessed: 13.04.2026).

References

1. "Security and privacy in remote radiology" ["Bezpeka ta konfidentsijnist u viddalenij radiologiyi"] , available at: https://radiolance.ua/bezpeka-ta-konfidentsijnist-u-viddalenij-radiologiyi/.
2. "How to protect data from unauthorized access?" ["Yak zahystyty dani vid nesanktsionovanogo dostupu?"] , available at: https://cybercalm.org/novyny/yak-zahystyty-dani-vid-nesanktsionovanogo-dostupu-porady/.
3. Koval, L. G. (2020), *Biomedical image processing and object reconstruction: lecture notes* [*Obrobka biomedychnykh zobrazhen ta rekonstruktsiia obiektiv: konspekt lektsii*] , VNTU, Vinnytsia.
4. Zhang, B., Rahmatullah, B., Wang, S. L. et al. (2020), "A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations" , *Multimedia Tools and Applications*. DOI: 10.1007/s11042-020-09629-4.
5. Maidaniuk, V. P., Romanyuk, O. N., Tuzhanskyi, S. Ye. (2022), *Fundamentals of information theory and coding* [*Osnovy teorii informatsii ta koduvania*] , VNTU, Vinnytsia.
6. Romanyuk, O. O., Maidaniuk, V. P., Pavlov, S. Ye. et al. (2024), "Encryption of medical images" ["Shyfruvannia medychnykh zobrazhen"] , *Medyko-tekhnichna spivpratsia zarady peremohy: materialy III Vseukr. nauk.-prakt. konf.* , Edelveis, Vinnytsia, pp. 86–89.
7. Khoroshko, V. O., Yaremchuk, Yu. Ye., Karpinets, V. V. (2017), *Computer steganography* [*Kompiuterna stehanohrafiia*] , VNTU, Vinnytsia.

8. Kuznietsov, O. O., Yevseiev, S. P., Korol, O. H. (2011), *Steganography: study guide* [*Stehanohrafiia: navch. posib.*] , KhNEU, Kharkiv.
9. Maidaniuk, V. P., Hrytsyshyn, V. O. (2024), "Protection of biomedical images from unauthorized access" ["Zakhyst biomedychnykh zobrazhen vid nesanktsionovanoho dostupu"] , *Informatsiini tekhnolohii i avtomatyzatsiia – 2024: materialy XVII mizhnar. nauk.-prakt. konf.* , ONTU, Odesa, pp. 200–201.
10. Hrytsyshyn, V. O., Maidaniuk, V. P. (2024), "Using steganography to protect X-ray images" ["Vykorystannia stehanohrafii dlia zakhystu renthenivskykh znimkiv"] , *Elektronni informatsiini resursy: zbirnyk materialiv Mizhnar. nauk.-prakt. internet-konf.*, NIKO, Sumy; Vinnytsia, p. 41.
11. Maidaniuk, V. P., Hrytsyshyn, V. O. (2023), "Image compression using the Walsh-Hadamard transform" ["Ushchilnennia zobrazhen z vykorystanniam peretvorennia Uolsha-Adamara"] , *Materialy LII nauk.-tekhn. konf. pidrozdiliv VNTU* , Vinnytsia.
12. Romanyuk, O. O., Maidaniuk, V. P., Pavlov, S. Ye. et al. (2024), "Medical image compression" ["Ushchilnennia medychnykh zobrazhen"], *Medyko-tekhnichna spivpratsia zarady peremohy: materialy III Vseukr. nauk.-prakt. konf.*, Edelveis, Vinnytsia, pp. 89–93.
13. Hopcroft, J. E., Motwani, R., Ullman, J. D. (2001), *Introduction to Automata Theory, Languages, and Computation*, 2nd ed., Addison–Wesley, Boston, 521 p., available at: https://archive.org/details/introductiontoau00hopc.

Надійшла до редакції 21.02.2026

V. P. MAIDANIUK, O. N. ROMANYUK, I. R. ARSENIUK, O. O. SKLADANIUK, M. L. NECHYPORUK
[1,2,3,4,5]Vinnytsia National Technical University, Vinnytsia, Ukraine
[1]maidaniuk2000@gmail.com

HIDING X-RAY IMAGES IN X-RAY IMAGES USING STEGANOGRAPHIC TRANSFORMATIONS

Ensuring the confidentiality of biomedical images is an important task in modern medical information systems, especially in the context of telemedicine development. X-ray images are widely used for diagnostics and are transmitted over communication n networks, which increases the risk of unauthorized access and data leakage. Traditional cryptographic methods provide a high level of data protection but do not conceal the fact of data transmission, which limits their effectiveness in certain applications. This paper investigates a steganographic approach to biomedical image protection based on embedding one X-ray image into another X-ray image. The purpose of the study is to ensure high quality of the container image and to minimize visual distortions during embedding. Methods in both spatial and frequency domains are used, in particular embedding based on Walsh–Hadamard transform coefficients. Experimental results show that avoiding coefficient normalization during the forward transform and applying normalization only at the inverse stage reduces distortions and preserves high visual quality even at full container capacity. It is established that embedding in transform coefficients provides higher container capacity compared to spatial-domain methods. The obtained results confirm the effectiveness of using X-ray images as containers for hiding images of the same type, ensuring high imperceptibility and steganographic robustness.

Keywords: steganography, biomedical images, X-ray images, Walsh-Hadamard transform, data hiding