ЗМІСТ

ВСТУП

В сучасному світі широко застосовуються і бурхливо розвиваються телекомунікаційні системи в усіх сферах діяльності людини, в тому числі у військовій сфері. Досвід ООС показав, що використання телекомунікаційних систем у військовій діяльності як полегшує управління військами, так і підвищує ризик перехоплення противником інформації. У зв'язку з цим гостро постає питання підвищення рівня захищеності інформації в перспективних автоматизованих системах управління. Одним з можливих варіантів вирішення даної задачі застосування методів цифрової стеганографії.

Актуальність роботи підтверджується необхідністю підвищення захисту інформації в системах управління, широким застосуванням БПЛА під час ведення бойових дій, широким застосуванням відеоконференцзв'язку, необхідністю підвищення захисту даних в інформаційних та телекомунікаційних мережах.

В даній роботі розробляється метод непрямого стеганографічного захисту даних в контурі зображення. Проводиться аналіз його показників якості та прихованої пропускної спроможності.

1 АКТУАЛЬНІСТЬ ЗАСТОСУВАННЯ МЕТОДІВ ЦИФРОВОЇ СТЕГАНОГРАФІЇ ДЛЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

1.1 Доцільність підвищення рівня захищеності інформації в перспективних автоматизованих системах управління на командних пунктах Повітряних Сил з урахуванням досвіду проведення Операції об'єднаних сил

Розвиток транспортних засобів, авіації, ракет, робототехніки збільшує динамічність бойових дій, дозволяє здійснювати маневри в дуже короткі строки, особливо слід відмітити тактику застосування авіації, коли швидкі нальоти бомбардувальників можуть завдати значної шкоди, а враховуючи швидкість літаків у особи, приймаючої рішення є лічені хвилини для того, щоб прийняти та втілити в життя рішення щодо захисту свого повітряного простору, те ж саме стосується і ракет, і для того, щоб вчасно реагувати на дії противника, збір розвідувальної інформації та керування військами здійснюється шляхом передачі інформації через супутник, засобами радіозв'язку або через кабелі зв'язку[1].

Засоби бездротового зв'язку є більш зручними у використанні при здійсненні маневрів, великій протяжності лінії зв'язку, при координуванні дій підрозділів при виконанні операцій, але при цьому дані, що передаються по бездротовим каналам зв'язку можуть бути перехоплені противником при передачі, що несе в собі велику загрозу. Для того, щоб мінімізувати шкоду, заподіяну противником при перехоплені повідомлення, дані захищаються шляхом криптографічного шифрування повідомлення, але будь-який шифр може бути зламаним, питання постає лише у часі, який буде витрачено на розшифрування повідомлення, а інформація має властивість з часом втрачати свою цінність [2].

Необхідність підвищення рівня захищеності інформації в системах управління показана на рисунку 1.1.

Використання іноземних технологій для організації обробки і передачі даних. Відсутність вітчизняних програмних пакетів і апаратних технологій для здійснення

інформаційної підтримки функціонування системи управління (СУ) диктує необхідність використання іноземних засобів. Такий підхід негативно впливає на забезпечення безпеки інформаційних мереж. Це обумовлено можливістю зловмисника потай використовувати програми для порушення конфіденційності і цілісності спеціальної інформації. Одночасно з підвищенням загроз щодо спеціальних інформаційних ресурсів в СУ постійно підвищується значимість такої інформації. Це обумовлено тим, що порушення безпеки інформаційно-телекомунікаційної системи (ІТС) може призвести до значних втрат серед особового складу та бойової техніки.

Передача по бездротовим каналам зв'язку розпоряджень стратегічного значення. Перехоплення противником розпорядження чи наказу стратегічного значення дозволить йому прийняти заходи щодо ускладнення, або унеможливлення виконання даного розпорядження, наприклад інформація про час та місце майбутнього бомбардування нашими літаками дозволить противнику мінімізувати результативність удару, а інформація про конвой з боєприпасами, продовольством, підкріпленням, тощо, дозволить противнику завдати значної шкоди нашим військам захопивши чи знищивши цей конвой.

Обмін даними з літаками, бронетехнікою, кораблями можливий лише по бездротовим лініям зв'язку. Після призначення літака на виконання завдання за призначенням з ним весь час підтримується зв'язок, курс літака може корегуватися, його завдання може змінитися безпосередньо в повітрі, літак передає на командні пункти інформацію про стан літака, доповіді про хід виконання завдання, тощо. Перехопивши дані від літака противник отримує більше можливостей знищити його, або ж завадити виконати завдання.

Передача по бездротовим каналам зв'язку розвідувальної інформації (в т. ч. від безпілотних літальних апаратів). Перехопивши нашу розвідувальну інформацію противник знецінить її шляхом передислокації підрозділу, підвищення рівня захисту певних об'єктів, чи навпаки, зняти частину підрозділів з охорони об'єкта, якщо знає, що

в нас нема інформації про нього, окрім того противник може виявити наші засоби розвідки і знищити їх.

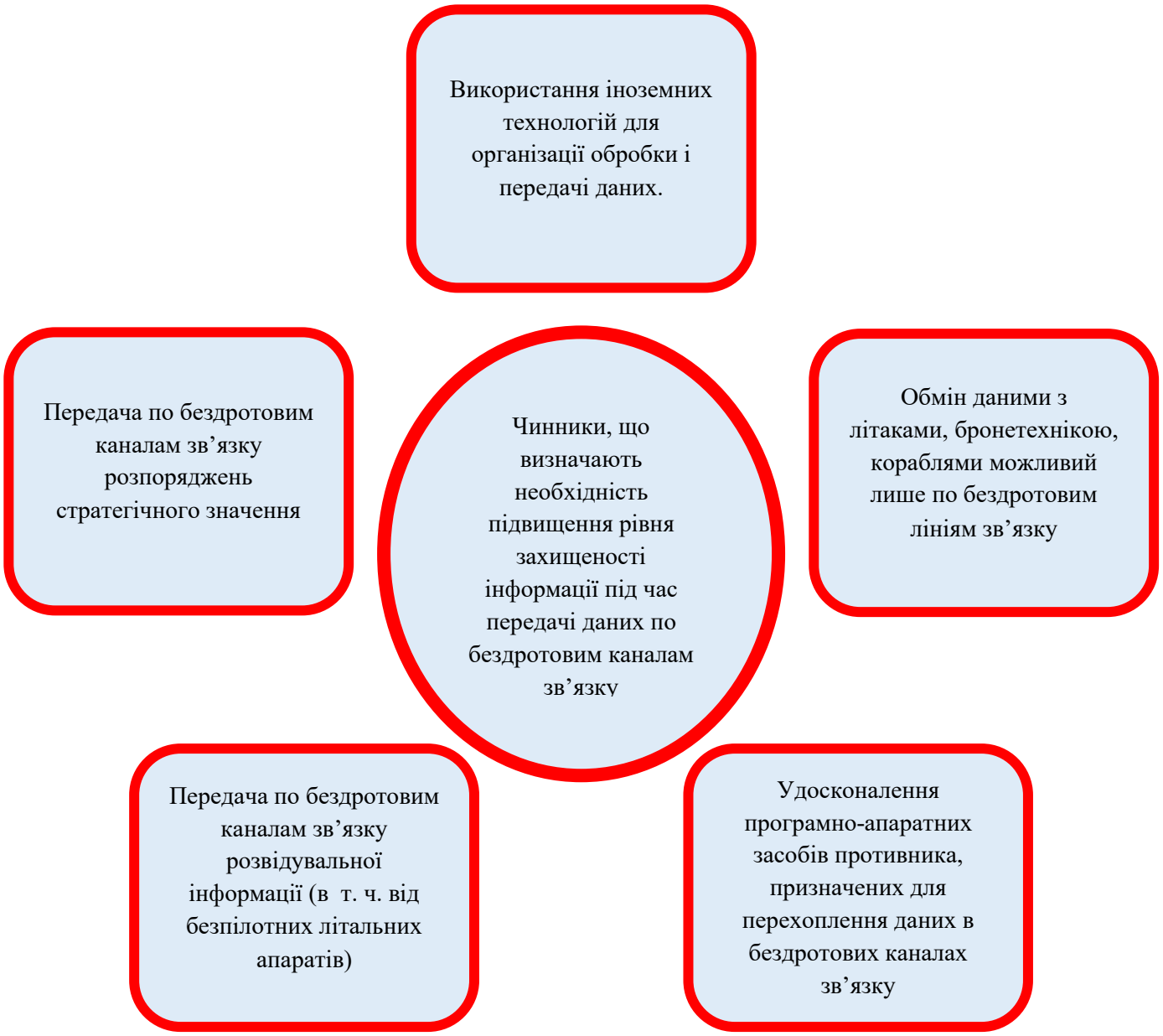

Рисунок 1.1 – Чинники, що визначають необхідність підвищення рівня захищеності інформації під час передачі даних по бездротовим каналам зв'язку

Удосконалення програмно-апаратних засобів противника, призначених для перехоплення даних в бездротових каналах зв'язку. З удосконаленням програмно-

апаратних засобів противник все частіше буде перехоплювати наші повідомлення, все швидше їх розшифровувати, що вимагає від нас підвищення рівня захищенності повідомлень.

1.2 Доцільність застосування методів цифрової стеганографії для підвищення рівня захищеності інформації в перспективних автоматизованих системах обробки розвідувальної інформації на командних пунктах Повітряних Сил

При обґрунтуванні застосування методів цифрової стеганографії (ЦС) розглянемо фактори, які впливають на ін формаційну безпеку в системах управління.

Підвищення можливостей противника для успішного криптоаналізу. Розвиток існуючих і розробка нових апаратних і програмних засобів для здійснення криптоаналізу противником супроводжується необхідністю підвищення безпеки спеціальних інформаційних ресурсів.

Відсутність можливості використання криптографічних методів з гарантованим захистом. Цей фактор пояснюється необхідністю використання значних апаратних та програмних ресурсів для забезпечення гарантованого захисту ІТС, що не завжди можливо забезпечити в умовах функціонування СУ.

Жорсткі вимоги щодо оперативності доставки спеціальної інформації. Для інформаційного забезпечення систем управління в Повітряних Силах (ПС) досить гостро стоїть питання оперативності та своєчасності доставки спеціальної інформації. Така умова ускладнює використання складних систем захисту для забезпечення необхідного рівня безпеки спеціальних інформаційних ресурсів (СІР).

Підвищена важливість переданої оперативної інформації для прийняття рішень. Важливість результатів успішного функціонування систем управління супроводжується підвищенням значення інформаційного забезпечення. Цей факт у свою чергу, диктує необхідність забезпечення гарантованого рівня безпеки ІТС. Це тягне за собою значні втрати людських і матеріальних ресурсів.

Тому поряд зі складними методами захисту інформації від несанкціонованого доступу потрібно використовувати методи комп'ютерної стеганографії. На відміну від криптографії, стеганографія дозволяє приховати факт наявності секретного повідомлення.

Цифрова стеганографія - напрям комп'ютерної стеганографії, що базується на приховуванні інформації в цифрових об’єктах, які спочатку мали аналогове походження. Вбудовування інформації може відбуватися в графічні, звукові та текстові документи [3, 5-8].

Для приховування даних в тексті використовують надмірність письмової мови та формати представлення тексту. Дані методи поділяються на 3 групи:

- методи довільного інтервалу;
- синтаксичні методи;
- семантичні методи.

В методах довільного інтервалу використовують маніпулювання вільним місцем між реченнями, в кінці текстових рядків, між словами, які вирівняні по ширині тексту.

Метод заміни інтервалу між реченнями дозволяє вбудовувати в текст повідомлення, яке має двійковий формат, шляхом розміщення одного або двух пробілів після кожного символу завершення речення. В якості символів завершення можуть бути точки, точки з комою. При цьому одиночним пробілом можна кодувати біт «1», подвійним – біт «0».

Вбудовування інформації в аудіо сигнали є досить перспективними, оскільки будуються на особливостях слухової системи людини (ССЛ). ССЛ не може відрізнити тихі звуки на фоні гучних, не може відрізнити абсолютну фазу, а також більшість спотворень вноситься навколишнім середовищем, що ССЛ просто ігнорує. Існують такі методи вбудовування інформації:

а) Кодування найменш значущих біт. Використовуючи звуковий сигнал, заміни найменш значущого біта (НЗБ) кожної точки, можна вбудувати великий об'єм інформації. Теоретично, пропускна спроможність стеганоканала складає 1Кб/сек на

1кГц, тому бітова швидкість передачі складе 8 Кб/сек послідовності яка оцифрована з частотою 8 кГц. Через високу пропускну спроможність каналу з'являється відчутний низькочастотний слух. Головним недоліком кодування НЗБ є його слаба стійкість до сторонніх впливів. Вбудована інформація може бути знищена шумами в каналі. Даний метод корисний тільки в замкнутих, повністю цифрових каналах.

б) Метод фазового кодування замінює вихідний звуковий сегмент на опорну фазу, характер зміни якої відображає дані, які необхідно вбудувати. Перед початком вбудовування фази на відправляючій та прийомній стороні узгоджуються. Даний метод є одним із ефективних методів по критеріям оцінок відносно шуму. Недоліком методу є низька пропускна спроможність.

в) Метод розширення спектру розширює сигнал прямої послідовності перемножуючи його на елементарну посилку – псевдовипадкової послідовності (ПВП) максимальної довжини, модульовану відомою частотою. При передачі повідомлення враховується наступне:

- псевдовипадкову послідовність максимальної довжини;
- адресату відомо потік ключів для вилучення інформації;
- адресату відомі частота елементарних посилок, швидкість передачі даних, частота несучої.

Вбудовування інформації в зображення є найбільш опрацьованим та розповсюдженим. Це обумовлено рядом причин: розповсюдження цифрових зображень, великий об’єм пропускної спроможності стеганографічного каналу, низька чутливість людського ока до незначних спотворень кольору, яскравості, контрасту. Існує два методи вбудовування даних в зображення: метод безпосереднього вбудовування даних і метод непрямого вбудовування даних.

В безпосередніх методах інформаційна послідовність секретного повідомлення вбудовується шляхом заміни даних контейнера на дані повідомлення.

Методи безпосереднього вбудовування даних мають такі переваги:

- простота реалізації алгоритму;

- великі обсяги вбудованих даних;

- невеликі значення часових витрат на реалізацію вбудовування і вилучення, при яких час вбудовування і час вилучення є найменшими;

- відсутністю необхідної попередньої обробки зображення-контейнера (ЗК) та прихованого повідомлення.

Серед методів безпосереднього вбудовування найбільш широко використовуваними на практиці є методи вбудовування в найменш значущий біт і методи на основі розширення спектра.

У непрямих методах вбудовування одного біта повідомлення здійснюється створенням залежності між певними параметрами ЗК, при якій стеганографічний декодер, відповідно до зворотніх стеганографічних перетворень, виділяє 0 або 1 біта вбудованої інформації. Існують наступні методи непрямого вбудовування даних:

- метод відносної заміни величин дискретно-косинусного перетворення (ДКП) (метод Коха та Жао). Один з найбільш поширених на сьогодні методів. В алгоритмі методу реалізовано розбиття зображення на блоки 8 * 8 пікселів для застосування до кожного з них ДКП. В результаті даного перетворення виходить матриця 8 * 8 коефіцієнтів ДКП. Кожен блок використовується для приховування одного біта даних. Для обох сторін при організації секретного каналу, вибираються два конкретних коефіцієнта ДКП, з певними координатами в масиві коефіцієнтів. Безпосередньо приховані починається з випадкового вибору блоку зображення, призначеного для кодування біта даних. Вбудовування відбувається такою модифікацією коефіцієнтів, щоб при передачі «0» їх різниця перевищувала деяку позитивну величину, а для «1» ця різниця робиться меншою в порівнянні з деякою негативною величиною. Таким чином, первинне зображення модифікується за рахунок внесення зміни в коефіцієнти ДКП. Після відповідної корекції коефіцієнтів проводиться зворотне дискретне-косинусне перетворення.

- метод модифікації яскравості (метод Куттера-Джордана-Боссена). Вбудовування повідомлення відбувається в спектр синього кольору, так як зорова

система людини найменш чутлива до змін кольору. Вбудовування секретного біта відбувається на основі зміни яскравості. Стійкість повідомлення прямо залежить від енергії вбудованого сигналу. Добування інформації відбувається «наосліп». Приймальна сторона зіставляє значення сусідніх пікселів. Для підвищення стійкості один біт повідомлення може повторюватися кілька разів. Даний метод стійкий до багатьох відомих атак.

- метод Бенгана-Мемона-Ео-Юнг. Вбудовування здійснюється в спектральні коефіцієнти зображення-контейнера шляхом їх модифікації. Для цього в спектральної області вибираються три коефіцієнта ДКП, що дозволяє зменшити візуальні спотворення. Для вбудовування «0», ці коефіцієнти змінюються таким чином, що б третій коефіцієнт став менше будь-якого з двох перших. Якщо необхідно приховати «1», він стає більше, ніж перший і другий коефіцієнти. Використання трьох коефіцієнтів ДКП замість двох зменшує спотворення, що вносяться в результаті вбудовування приховуваного повідомленням.

В розділі наведені чинники, що вимагають підвищення рівня захищеності інформації в в перспективних автоматизованих системах обробки розвідувальної інформації. Обумовлене використання цифрової стеганографії для підвищення рівня захищеності інформації, наведено існуючі методи цифрової стеганографії.

2 РОЗРОБКА МЕТОДУ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ДАНИХ В КОНТУРІ ЗОБРАЖЕННЯ

2.1 Вибір ділянок контуру для вбудовування інформації

Розробляємий метод повинен забезпечувати надійність приховування інформації в зображеннях, вбудовування відносно великого обсягу інформації та стійкість до спотворень. Тому, пропонується вбудовувати дані в контури зображення. Зображення має велику кількість контурів, що забезпечить можливість для забезпечення відносно великого обсягу для вбудовування інформації. Вбудовування інформації буде виконуватися непрямим методом, шляхом модифікації елементів. При цій модифікації необхідно враховувати належність модифікуємих елементів до інтервалів. Це необхідно для вилучення інформації на приймальній стороні [10-12].

Необхідно вибрати контури зображення для вбудовування даних та ділянки в цих контурах, в які буде вбудовуватись інформація. При виборі контурів було виявлено, що в більшості випадків контур не широкий (рис 2.1):

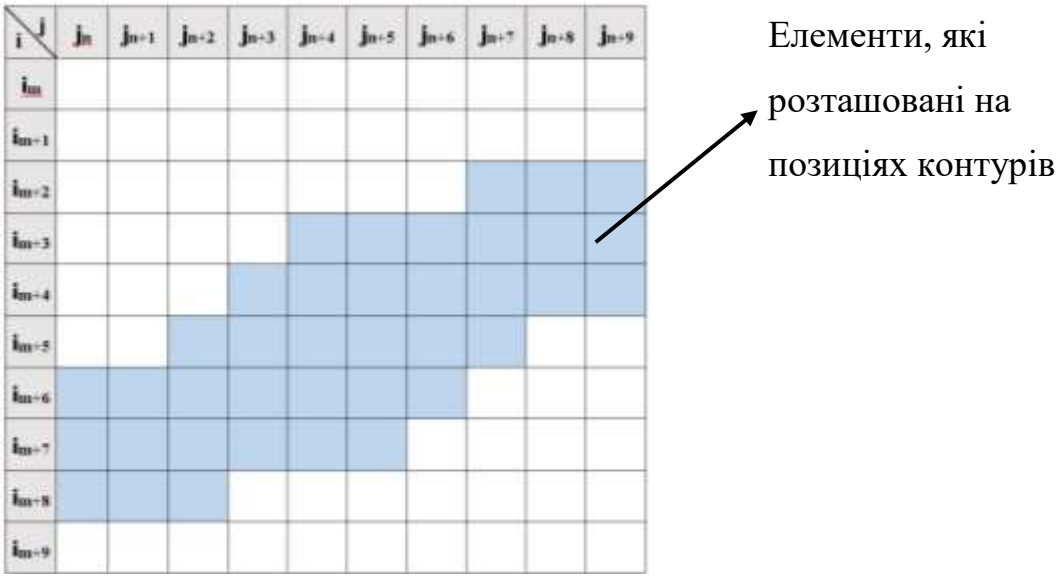

Рисунок 2.1 – Ширина контуру в зображенні

Алгоритм визначення ділянок для вбудовування наступний:

1. Перебираючи всі елементи маски зображення знаходимо елемент контуру bi,j для якого виконується умова що елементи bi-1,j-1 – bi+1,j+1 також належать контуру, такий елемент є першою реперною точкою (R1), необхідною для подальшого вбудовування даних (рис 2.2):

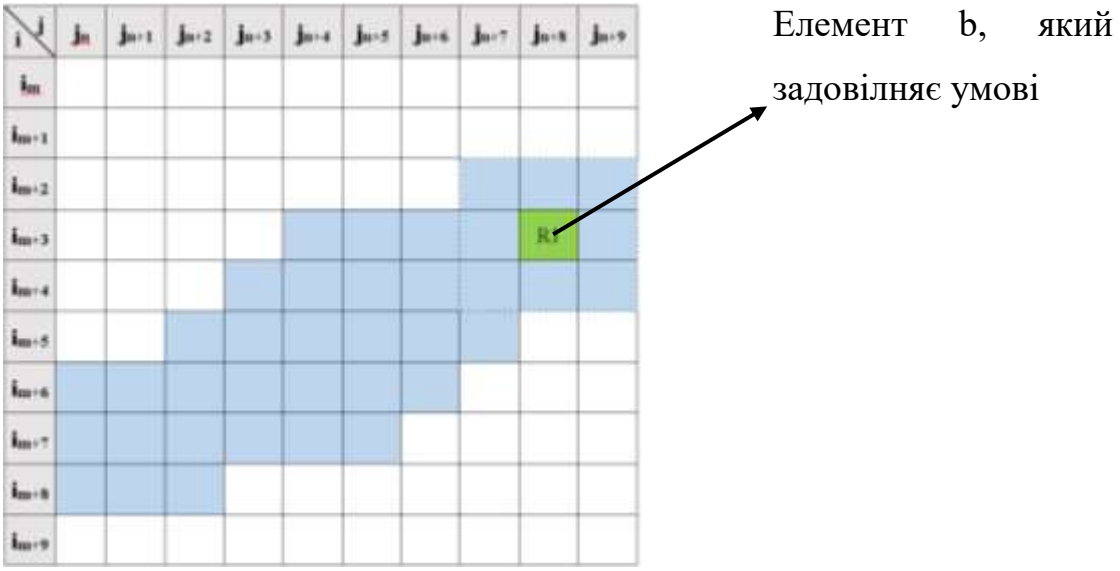

Рисунок 2.2 – Елемент b, який задовільняє умові

2. Шукаємо контурні елементи зображення, які знаходяться на відстані n (значення задається ключем) від знайденого елемента контура R1 та задовільняють умові, висунутій до елемента R1 (рис 2.3):

3. Перевіряємо чи всі елементи зображення, що лежать на відрізку (лінії порівняння P) обмеженому знайденими точками є елементами контуру і не лежать на границі контуру. (рис 2.4):

4. Виділяємо смуги порівняння V_1 та V_0 (рис 2.5). Смуга порівняння – це область контуру, що починається від лінії порівняння та відходить в сторону на ширину M, яка задається ключем.

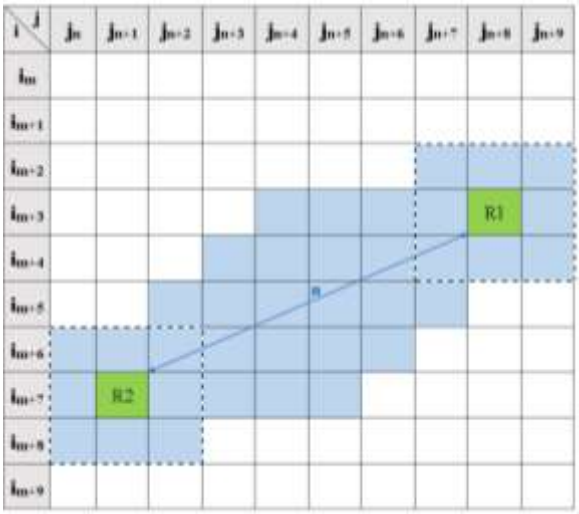

Рисунок 2.3 – Елемент R2 на відстані n від елемента R1

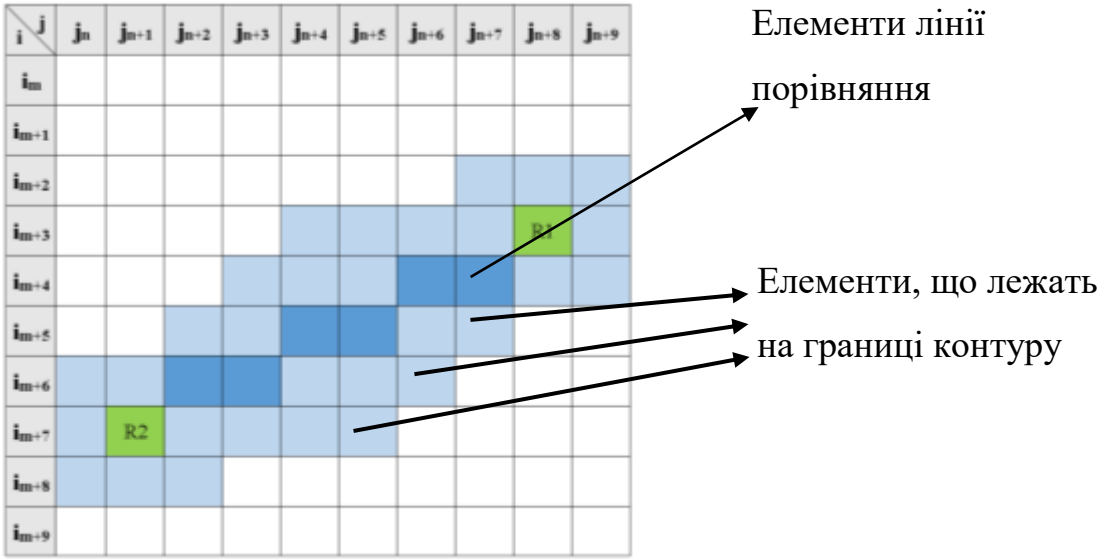

Рисунок 2.4 – Розміщення в контурі лінії порівняння

Елементи смуги V_1 для M = 1 визначаються за формулами:

$$i_{v_1} = \begin{cases} i_p, \text{ якщо } j_{v_1} = j_p - 1 \\ i_p - 1, \text{ якщо } j_{v_1} = j_p \end{cases}, \quad (2.1)$$

у випадку коли $j_{R1} > j_{R2}$, або

$$j_{v_1} = \begin{cases} j_p, \text{ якщо } i_{v_1} = i_p - 1 \\ j_p + 1, \text{ якщо } i_{v_1} = i_p \end{cases}, \quad (2.2)$$

у випадку коли $j_{R1} \leq j_{R2}$.

Елементи смуги V_0 для M = 1 визначаються за формулами:

$$i_{v_0} = \begin{cases} i_p, \text{ якщо } j_{v_0} = j_p + 1 \\ i_p + 1, \text{ якщо } j_{v_0} = j_p \end{cases} \quad (2.3)$$

у випадку коли $j_{R1} > j_{R2}$, або

$$j_{v_0} = \begin{cases} j_p, \text{ якщо } i_{v_0} = i_p + 1 \\ j_p - 1, \text{ якщо } i_{v_0} = i_p \end{cases}, \text{ якщо } j_{R1} \leq j_{R2} \quad (2.4)$$

у випадку коли $j_{R1} \leq j_{R2}$.

В формулах 2.1 – 2.4:

v – елемент смуги V, який є сусіднім до *p*;

p – елемент лінії порівняння P.

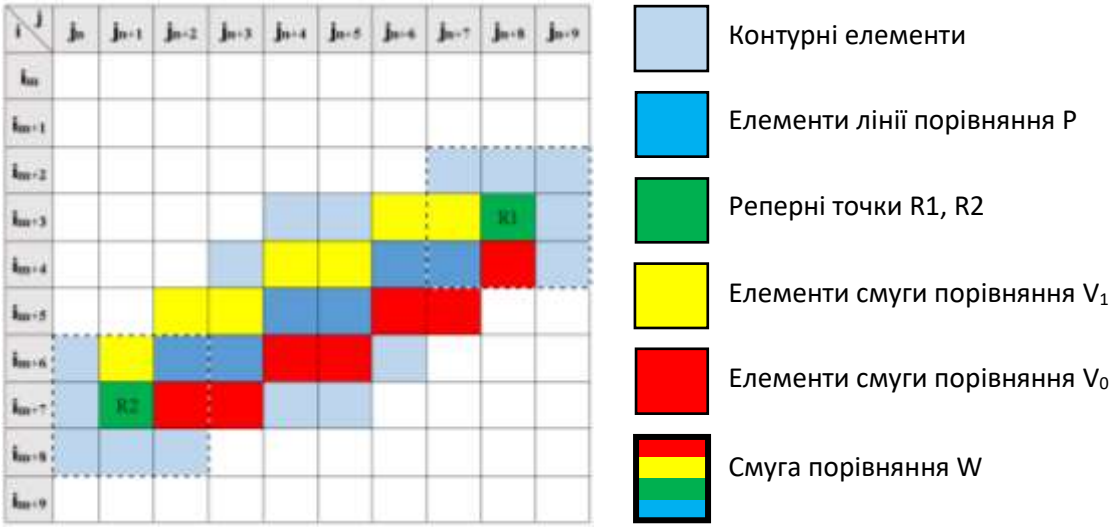

Рисунок 2.5 – Виділена ділянка вбудовування даних на масці зображення

5. Переносимо ділянку вбудовування даних з маски зображення на саме зображення (рис 2.6):

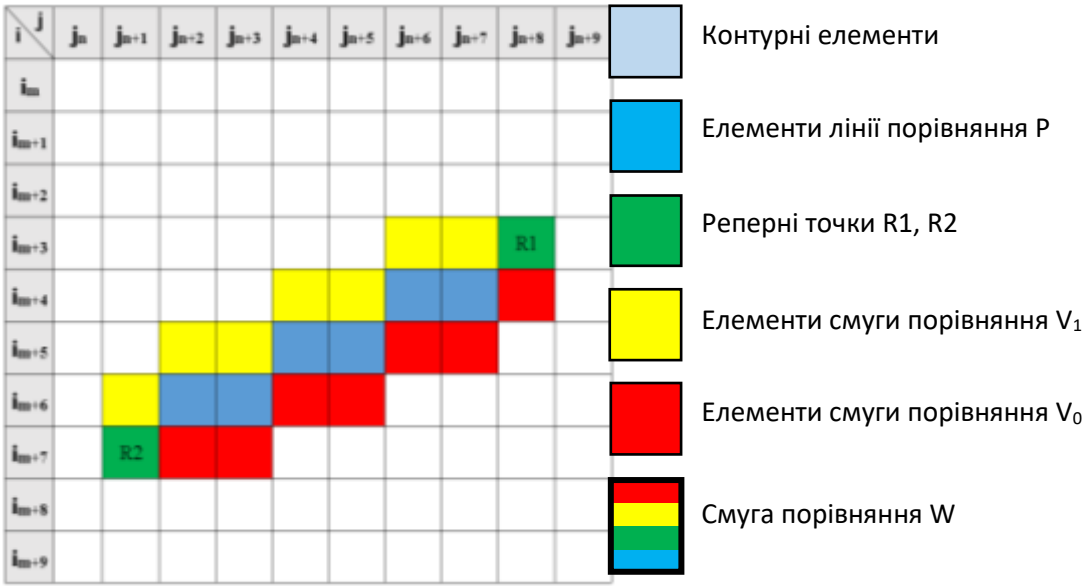

Рисунок 2.6 – Виділена ділянка вбудовування даних на вихідному зображенні

2.2 Вбудовування інформації

Після виявлення ділянки переходимо безпосередньо до вбудовування інформації. Алгоритм вбудовування наступний:

1. Виділяємо елементи які ми будемо змінювати та не змінювані елементи в процесі вбудовування. Для цього ми:

a. Розставляємо елементи смуг порівняння V в порядку зростання (рис. 2.7).

b. Визначаємо довжину інтервалів *d* за формулою

$$d_y = \frac{a_{max_y} - a_{min_y}}{3}, \qquad (2.5)$$

де:

- змінна *a* це елемент зображення;
- змінна *y* вказує на приналежність елементу до відповідної смуги порівняння і приймає значення

$$y = (0,1).$$

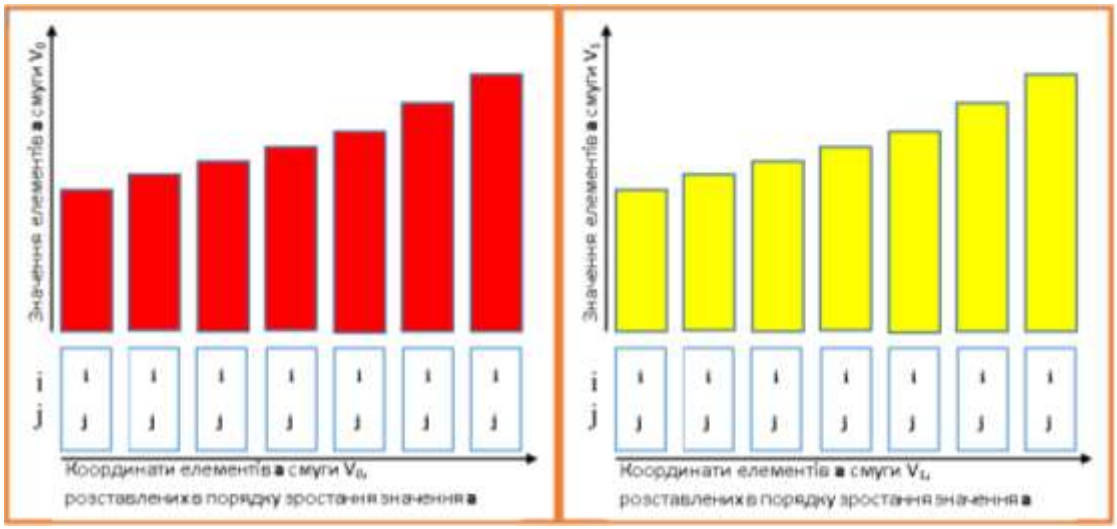

Рисунок 2.7 – Розставлені в порядку зростання елементи

c. Визначаємо границі інтервалів *z* за формулою

$$z_{q_y} = a_{min_y} + d_y * (q - 1), \quad (2.6)$$

де змінна q є номером границі інтервалів та приймає значення

$$q = (1,4).$$

Елементи, які потрапляють у інтервал $z_2 – z_3$ незмінювані (рис. 2.8).

2. Перевіяємо що вбудовано в даній ділянці зараз. Для цього ми виконуємо наступні дії:

a. Обраховуємо середні значення S_j (рис. 2.3) за формулою

$$S_{t_y} = \frac{\sum_{m=1}^{n} a_m}{n}, \quad (2.7)$$

де:

- змінна *t* є номером інтервалу і приймає значення

$$t = (1,3);$$

- змінна *n* це кількість елементів *a* на інтервалі;
- змінна *m* є номером елементу *a* на інтервалі і приймає значення

$$m = (1,n).$$

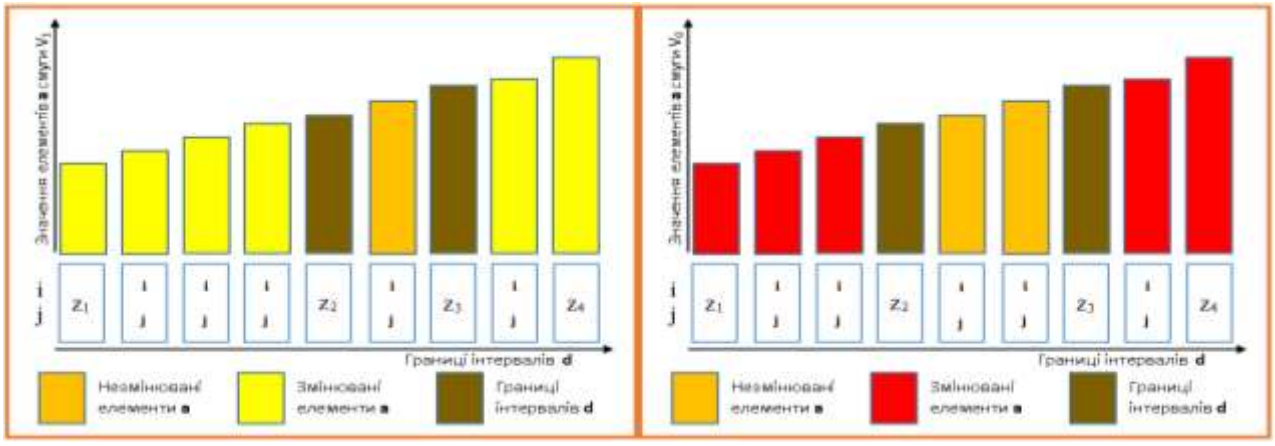

Рисунок 2.8 – Незмінювані елементи

b. Обчислюємо коефіцієнт порівняння H, який дорівнює:

$$H = \frac{S_3}{S_1+S_2}. \tag{2.8}$$

c. Порівнюємо значення коефіцієнта H смуги «1» з значенням коефіцієнта H смуги «0». Якщо ми вбудовуємо «1», значення коефіцієнта H смуги «1» має бути більшим ніж значення коефіцієнта H смуги «0» і навпаки, для цього використовуємо наступну формулу:

$$bit = \begin{cases} 1, & H_1 > H_0 + 0{,}06 \\ 0, & H_1 < H_0 - 0{,}06 \end{cases}. \tag{2.9}$$

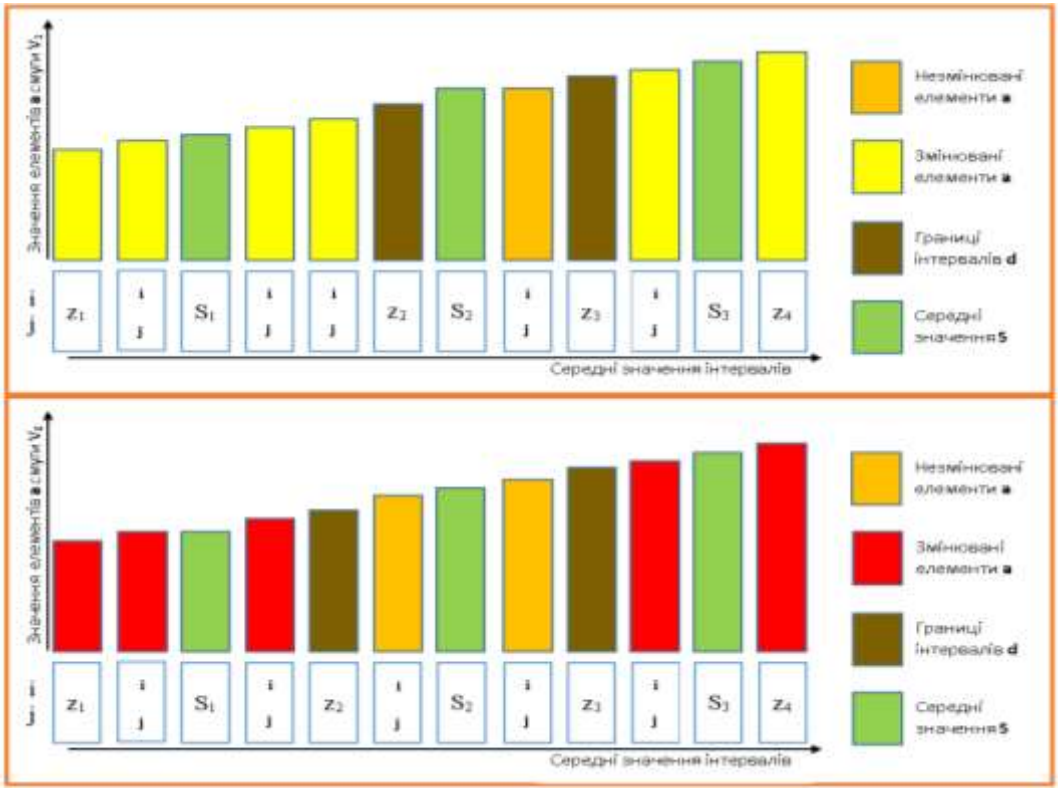

Рисунок 2.9 – середні значення інтервалів

Якщо значення *bit* відповідає значенню, яке ми збираємося приховати залишаємо значення *a* незмінними, якщо ж ні переходимо до пункту 3.

3. Вбудовуємо потрібний *bit*. Ми змінюємо значення елементів, які входять в інтервали $z_1 - z_2$ і $z_3 - z_4$.

При встраюванні «*bit = 1*» використовуємо такі формули:

для *y = 1* a_{k_y} обчислюємо за цією формулою:

$$a_{k_y} = \begin{cases} a_{k_y} - 1, \rightarrow z_1 \leq a_{k_y} < z_2 \\ a_{k_y} + 1, \rightarrow z_3 < a_{k_y} \leq z_4 \end{cases}; \quad (2.10)$$

для *y = 0* – користуємось наступною формулою:

$$a_{k_y} = \begin{cases} a_{k_y} + 1, \rightarrow z_1 \leq a_{k_y} < z_2 \\ a_{k_y} - 1, \rightarrow z_3 < a_{k_y} \leq z_4 \end{cases}. \quad (2.11)$$

При встраюванні «*bit = 0*» використовуємо такі формули:

для *y = 1* a_{k_y} обчислюємо за цією формулою:

$$a_{k_y} = \begin{cases} a_{k_y} + 1, \rightarrow z_1 \leq a_{k_y} < z_2 \\ a_{k_y} - 1, \rightarrow z_3 < a_{k_y} \leq z_4 \end{cases}; \quad (2.12)$$

для *y = 0* – користуємось наступною формулою:

$$a_{k_y} = \begin{cases} a_{k_y} - 1, \rightarrow z_1 \leq a_{k_y} < z_2 \\ a_{k_y} + 1, \rightarrow z_3 < a_{k_y} \leq z_4 \end{cases}. \quad (2.13)$$

Після виконання цього пункту переходимо до пункту **1.b** і виконуємо алгоритм доти, доки нас не буде задовільняти умова пункту **2.c**. Коли умова виконана повертаємо змінені значення *a* на вихідні позиції та переходимо до пошуку наступної зони вбудовування, якщо ця зона виявилася останньою, зображення-контейнер готовий до передачі. Структурні схеми приховування та вилучення даних представлені на додатку А та додатку В відповідно.

В даному розділі розроблено метод стеганографічного приховування даних в контурі зображення непрямим способом шляхом модифікації елементів контуру. Описано алгоритм виявлення ділянок для вбудовування даних а також наведеній механізм модифікації елементів що містять контурну інформацію.

3 ОЦІНКА РОЗРОБЛЕНОГО МЕТОДУ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ДАНИХ В КОНТУРІ ЗОБРАЖЕННЯ

До усіх існуючих та розроблюваних методів цифрової стеганографії однією з головних вимог є пропускна здатність. Канал прихованої передачі даних організовується в каналах відкритого зв'язку. Тому, можна зробити висновок що пропускна здатність прихованого каналу не може перевищити пропускну здатність відкритого каналу.

Прихована пропускна здатність – максимальна кількість інформації, що може бути вбудована до одного елемента контейнера. Обов'язковою умовою при цьому є безпомилковість передавання прихованих даних одержувачеві, а також їх захищеність від таких атак порушника, як спроби виявлення факту наявності каналу прихованого зв'язку, одержання змісту прихованих повідомлень, навмисне введення сфальсифікованих даних або ж руйнування вбудованої до контейнера інформації.

Оскільки основною задачею розроблюваних стеганографічних методів є організація прихованого каналу зв'язку в каналі загального користування, то використане стеганографічне перетворення повинно гарантовано забезпечувати надійність сприйняття формуючого стеганоповідомлення [4].

Необхідно враховувати, що виконання даної вимоги буде вище, якщо стеганографічний метод і реалізуючий його алгоритм будуть вносити найменші спотворення при вбудовуванні елементів повідомлення в елементи зображення-контейнера.

- стеганографічне перетворення повинно буду стійким до атак проти вбудованого повідомлення. Для забезпечення нечутливості стеганоповідомлення до атакуючих впливів поріг спотворення елементів не повинен перевищувати заданого значення.
- при вбудовуванні даних в зображення-контейнер необхідно враховувати особливості машинних похибок при виконанні алгоритмів обчислення.

Організація прихованого каналу зв’язку в розроблюваних методах стеганографії повинна проходити разом з перевіркою цілісності передаваємої конфіденційної інформації. Для цього необхідно:

- забезпечити можливість перевірки цілісності передаваємої інформації шляхом перевірки особливостей параметрів матриці зображення-контейнера; порушення яких можливе лише при атакуючому впливу противника на повідомлення(контейнер);
- при розробці методу необхідно забезпечити незмінність при вбудовуванні додаткової інформації характерних особливостей матриці зображення-контейнера, використовуємих для організації перевірки цілісності передаваємої інформації.

Для порівняння і оцінки існуючих стеганографічних систем розглянемо показники ефективності їх функціонування. Така оцінка повинна дати повну картину успішного використання оцінюваних стеганографічних методів для прихованої передачі СІР. Розглянемо основні показники ефективності стеганографічних перетворень [2].

Відносна стеганографічна ємність $w_{відн}$ стеганографічної системи. Значення відносної стеганографічної ємності показує процентне відношення об’єму $w_{вбуд}$ вбудовуваної інформації відносно об’єму $w_{поч}$ зображення-контейнера. Дана величина використовується для оцінки ефективності стеганографічної системи по питомому об'єму вбудовуваної інефомації відносно об'єму зображення-контейнера. Величина $w_{відн}$ відносної стеганографічної ємності системи обчислюється за наступною формулою:

$$w_{відн} = \frac{w_{вбуд}}{w_{поч}}, \tag{3.1}$$

де

$$w_{вбуд} = \frac{3 \cdot z_{рядк} z_{стовп}}{\omega}, \tag{3.2}$$

де $3 \cdot z_{рядк} z_{стовп}$ – розмір зображення оригіналу;

ω – кількість елементів необхідних для вбудовування 1 біта.

У відсотках значення відносної стеганографічної ємності системи оцінюється на основі наступного виразу:

$$w_{відн} = \frac{w_{вбуд}}{w_{поч}} \cdot 100\% . \tag{3.3}$$

Ймовірність $P_{вил}$ безпомилково вилучених даних авторизованим користувачем. Дана величина використовується для оцінки безпомилково вилученої інформації при авторизованому доступі. Дана ймовірність обчислюється за наступною формулою:

$$P_{вил} = \frac{w_{вил}}{w_{вбуд}}, \tag{3.4}$$

де $w_{вбуд}$ – об'єм вбудовуваної інформації, біт;

$w_{вил}$ – об'єм безпомилково вилучених даних, біт.

У випадку, коли $P_{вил}$ приймає значення одиниці, кількість безпомилково вилучених вбудованих даних авторизованим користувачем дорівнює 100%.

Пікове відношення сигнал шум (ПВСШ) h зображення з вбудованими даними при неавторизованому доступі вимірюється в дБ. Дана величина характеризує візуальні спотворення, які вносяться в зображення-контейнер в процесі вбудовування та обчислюється за наступною формулою:

$$h = 20\lg(255 / СКВ), \tag{3.5}$$

де *СКВ* – середнє квадратичне відхилення зображення з вбудованими даними відносно зображення-контейнера і обчислюється на основі наступної формули:

$$СКВ = \sqrt{\frac{\sum_{i=1}^{z_{рядк}} \sum_{j=1}^{z_{стовп}} (a_{ij} - a'_{ij})}{z_{рядк} z_{стовп}}}, \quad (3.6)$$

де a_{ij},, a_{ij} – елементи відповідно початкового і стеганографічно перетвореного зображень;

$z_{рядк}$ $z_{стовп}$ – розмір зображення-контейнера.

Чим більше значення пікового відношення сигнал шум, тим менше візуальних спотворень вноситься до зображення в процесі вбудовування.

За формулами 3.1-3.4 проведемо обчислення показників якості для наступних методів:

- найменш значущого біта;
- розширення спектру;
- методу Тао ;
- розробленого методу.

Дані розрахунків наведені в таблиці 3.1.

Таблиця 3.1 – Значення показників якості

Показник якості		Метод стеганографічного вбудовування			
		НЗБ	РС	Тао	Розроблений метод
Відносна ємність, %	ω=2	12,25	0,78	3,1	3.6
	ω=4	6,25			
Ймовірність вилучення даних		0,5	0,5	0,7	0.99
Пікове відношення сигнал шум, дБ		12,53	13,29	18,54	22,12

Висновки до розділу 3

Проведено аналіз розробленого методу, порівняно його показники якості з показниками найбільш розповсюджених методів. Виявлено, що розроблений метод по показнику відносної ємності уступає лише методу заміни НЗБ при цьому на порядок перевершує його по показнику ймовірності правильного вилучення даних та по піковому відношенню сигнал-шум. Інші ж методи він перевершує по всіх показниках.

ВИСНОВКИ

В даній роботі наведені чинники, що вимагають підвищення рівня захищеності інформації в перспективних автоматизованих системах обробки розвідувальної інформації. Обумовлене використання цифрової стеганографії для підвищення рівня захищеності інформації, наведено існуючі методи цифрової стеганографії.

Розроблено метод непрямого стеганографічного вбудовування даних в найбільш стійкі блоки контуру до атакуючих впливів. Даний метод вбудовує біти шляхом модифікації елементів, що містять контурну інформацію. Описано алгоритм виявлення ділянок для вбудовування даних а також наведеній механізм модифікації елементів що містять контурну інформацію.

Вперше запропоновано використання стійких областей зображення для стеганографічного приховування інформації. На відміну від інших методів, визначення областей для вбудовування здійснюється на основі використання маскування для виявлення меж однорідних областей зображення.

Проведено аналіз розробленого методу, порівняно його показники якості з показниками найбільш розповсюджених методів. Виявлено, що розроблений метод по показнику відносної ємності уступає лише методу заміни НЗБ при цьому на порядок перевершує його по показнику ймовірності правильного вилучення даних та по піковому відношенню сигнал-шум. Інші ж методи він перевершує по всіх показниках.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Алімпієв А. М. Застосування досвіду АТО для підготовки фахівців зв'язку, РТЗ, А та ІС. / А. М. Алімпієв, О. І. Кушнір, К. С. Васюта. – Х. : ХНУПС, 2016. – 328 с.
2. Мельник А.С Інформаційні системи та мережі. Вісник / А. С. Мельник, М.М. Голобородько НУ "Львівська політехніка". – № 673.– Львів, 2010. – С. 365-374.
3. Аграновський А.В. Стеганографія, цифрові водяні знаки та стегоаналіз / А. В. Аграновський, А. В. Балакін, В. Г. Грибунин. – К.: Вузовская книга, 2015. – 220 с.
4. Бараннік В.В. Метод непрямого стеганографічного вбудовування даних в зображення-контейнер з урахуванням інформації контуру. / В. В. Бараннік, О. М. Шатун, Д. В. Бараннік – К.: Наукоємні технології. Том 39, № 2. 2018. С. 232-239.
5. Гонсалес Р. Цифрова обробка зображень. 3-е видання. / Р. Гонсалес, Р. Вудс. – К. : Техносфера, 2012. – 1104 с.
6. Грибунін В. Г. Цифрова стеганографія — К.: СОЛОН-Пресс, 2012. – 272 с.
7. Конахович Г.Ф. Компьютерна стеганографія. Теорія та практика / Г.Ф. Конахович, А.Ю.Пузиренко — Київ: К-Пресс, 2016. — 288 с.
8. Міано Дж. Формати та алгоритми стиснення зображень в дії — К.: Триумф, 2013. — 336 с.
9. Barannik V. A. Steganographic Method Based On The Modification Of Regions Of The Image With Different Saturation/ V. Barannik, A. Lekakh, A. Bekirov, D. Barannik / Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (S5). – 2018. – p. 81-85.
10. Barannik V. V. The method of video streams processing for information technologies of aero monitoring. / V. Barannik, A. Musienko, Yu. Ryabukha, O. Suprun, A. Slobodyanyuk / 14th International Conference [IEEE Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)], 2018. – P.233 – 236.
11. Barannik V.V. The method of video streams processing for information technologies of aero monitoring / V. Barannik, A. Musienko, Y. Ryabukha, O. Suprun, A. Slobodyanyuk // 14th International Conference on Advanced Trends in Radioelecrtronics,

Telecommunications and Computer Engineering (TCSET) / Lviv, Slavske, Ukraine 20-24 Feb. 2018.– P. 233-236.

12 Бараннік В. В. Технологія підвищення безпеки передачі даних з використанням стеганографічного підходу в автоматизованих системах управління спеціального призначення. / В.В.Бараннік, І.М.Тупиця, М.М.Кодацький – Х.:Радіоелектроніка та інформатика №4(87), 2019.