МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Методи стеганографічної обробки мультимедійних даних в стільникових мережах п'ятого покоління»

Виконавець: _____ Андрій СУЛІКОВСЬКИЙ
(підпис)

Керівник: _____ Олександр ПУЗИРЕНКО
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Суліковського Андрія Миколайовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Методи стеганографічної обробки мультимедійних даних в стільникових мережах п'ятого покоління»
затверджена наказом ректора від «07» вересня 2022 р. №1321/ст
2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.
3. Вихідні дані до роботи: стеганографічний контейнер
4. Зміст пояснювальної записки: розділ №1, розділ №2, розділ №3, розділ №4, Охорона праці, Охорона навколишнього середовища
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: методи дослідження стеганографічної системи, слайди презентації Microsoft PowerPoint

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Написання першого розділу	12.09.2022-05.10.2022	Виконано
4	Написання другого розділу	06.10.2022-15.10.2022	Виконано
5	Написання третього розділу	17.10.2022-05.11.2022	Виконано
	Написання четвертого розділу	20.11.2022-05.11.2022	
6	Охорона праці	07.11.2022-12.11.2022	Виконано
7	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколиш-нього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Олександр ПУЗИРЕНКО
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Андрій СУЛІКОВСЬКИЙ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Методи стеганографічної обробки мультимедійних даних в стільникових мережах п'ятого покоління» містить 88 сторінок, 24 рисунки, 5 таблиць, 46 використаних джерел.

СТЕГАНОГРАФІЯ, КОНТЕЙНЕР, СТИСНЕННЯ ЗОБРАЖЕННЯ, БІТОВА ПЛОЩИНА.

Метою кваліфікаційної роботи є дослідження властивостей природних зображень-контейнерів, що забезпечують найкращу секретність вбудовування інформації внаслідок застосування статистичних методів стеганографічного аналізу для подальшого транспортування мережами п’ятого покоління.

Об’єктом дослідження – є цифрова стеганографічна система на основі цифрової статичної картинки в якості контейнеру.

Предметом дослідження – є статистичні властивості цифрових зображень БМП формат.

Практичне значення отриманих результатів.

Результати кваліфікаційноїх роботи можуть бути використані при практичному розвитку стеганографічної системи.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

LSB - Least Significant Bit.

RGB - Red Green Blue.

JPEG - Joint Photographic Експерти Group.

BMP - Bitmap Picture.

RS - Regular-Singular , то є "регулярно-сингулярний".

TIFF - Tagged Image File Формат.

PNG - Portable Network Graphics (формат зберігання растрових графічних зображень).

TGA - Truevision TGA (TGA - растровий графічний формат).

ЦВЗ - цифровий водяний знак.

БЧХ - коди Боуза-Чоудхурі-Хоквінгема (залишають один з великих класів лінійних кодів , виправляючих помилки).

НЗБ - найменш значущі біти.

ВСТУП

Актуальність теми. У всі часи протягом історії людства завдання захисту інформації від несанкціонованого доступу залишалася актуальною і в справжнє час залишається не вирішеною до кінця проблемою. Вже в стародавньому світі виділилося два основних напрямки вирішення цього завдання, що існують і по сьогоднішній день: криптографія і стеганографія. Метою криптографії є приховування вмісту повідомлень за рахунок їх шифрування. У відмінність від цього, при стеганографії ховається сам факт існування таємного повідомлення.

Сильним поштовхом до розвитку стеганографії послужило те, що в більшості країн на криптографію накладаються певні обмеження: так, наприклад, потрібно передача ключів від використовуваних систем шифрування державі. Обов'язкова так ж реєстрація і ліцензування криптографічних систем незалежно від того, є вони апаратними чи програмними засобами. Стеганографія не підпадає під дію зазначених обмежень і є при цьому ефективним способом приховування даних.

Методи стеганографії застосовуються не тільки для потайної передачі повідомлень, але й використовують для захисту авторських чи майнових прав на цифрове зображення, фотографії або інші оцифровані твори мистецтва. Переваги, які дають подання і передача повідомлень в цифровому вигляді. Тому розробляються різні заходи захисту інформації, організаційного і технічного характеру. Один із найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у вбудовуванні в об'єкт невидимих міток - цифрових водяних знаків. Вони можуть утримувати багато корисної інформації: коли створено файл, хто володіє авторськими правами, як вступити в контакт із автором і т.д. Усі внесені дані можуть розглядатися як вагомі докази при розгляді питань та судових розглядів про авторство або для доказу факту нелегального копіювання і часто мають вирішальне значення.

Найбільш поширеним на сьогоднішній день методом цифровий стеганографії є метод, що полягає у вкладенні приховуваного повідомлення у зображення шляхом

модифікації найменш значних біт (LSB). Цифрові зображення є матрицею пікселів [1-30].

Метою кваліфікаційної роботи є дослідження властивостей природних зображень-контейнерів, що забезпечують найкращу секретність вбудовування інформації внаслідок застосування статистичних методів стеганографічного аналізу для подальшого транспортування мережами п’ятого покоління.

Об’єктом дослідження – є цифрова стеганографічна система на основі цифрової статичної картинки в якості контейнеру.

Предметом дослідження – є статистичні властивості цифрових зображень BMP формат.

Практичне значення отриманих результатів.

Результати кваліфікаційної роботи можуть бути використані при практичному розвитку стеганографічної системи.

РОЗДІЛ 1
ОСНОВНІ ПОЛОЖЕННЯ СТЕГАНОГРАФІЇ

1.1. Основні визначення

Стеганографію можна розділити на 3 розділи:

- класична стеганографія - включає в себе всі “некомп'ютерні методи”.
- комп'ютерна стеганографія - напрямок класичної стеганографії, заснованої на особливостях комп'ютерної платформи.
- цифрова стеганографія - напрямок класичної стеганографії, заснованованої на прихованні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів. Використовується надмірність аудіо- та візуальної інформації [1].

Саме цифрова стеганографія представляє собою найбільший інтерес, з точки зору захисту інформації, як найбільш перспективний напрямок. Її ми розглянемо докладніше.

Основні положення стеганографії:

- Методи приховання повинні забезпечувати автентичність і цілісність файлу.
- Передбачається, що криптографу повністю відомі можливі стеганографічні методи.
- Безпека методів ґрунтується на збереженні стеганографічним перетворенням основних властивостей відкрито переданого файлу при внесенні в нього секретного повідомлення і деякої невідомої противнику інформації - ключа.
- Навіть якщо факт приховання повідомлення став відомий противнику через спільника, вилучення самого секретного повідомлення представляє складну обчислювальну задачу [1].

Незважаючи на численні відкриті публікації і щорічні конференції, тривалий час стеганографія не мала термінології. Основні поняття стеганографії були узгоджені в 1996 р. 1-й Міжнародній конференції із приховання даних – Information Workshop on Information Hiding '96. Проте, навіть таке основне поняття як «стеганографія» різними фахівцями трактується неоднаково [2].

Наведемо визначення найважливіших, з погляду стеганографії, термінів.

Стеганосистема - система, здійснююча вбудовування і виділення однієї бітової послідовності з іншої. Послідовність, що підлягає приховуванню, називається повідомленням. Послідовність, в яку здійснюється вбудовування, називається контейнером. Якщо в контейнер не вбудовувалося повідомлення, він називається порожнім, інакше – заповненим. Як правило, в складі стеганосистеми додатково виділяють підсистеми, такі як прекодер, стеганокодер, стеганодетектор, декодер [3]. Порівняно нещодавно була розроблена математична модель стеганосистеми.

У будь-який стеганосистемі важливу роль грає стеганографічний протокол – порядок дій, до якого вдаються дві чи більше сторін, з метою рішення певних задач [4].

Цифровий водяний знак (ЦВЗ) – впровадження в мультимедійний сигнал інформації, призначення якої – автентифікація вмісту, охорона прав власника, захист від копіювання та т.п.

Стеганосистема утворює стеганоканал, по якому передається заповнений контейнер. Цей канал вважається схильним до впливів з сторони порушників. Наслідуючи [5], у стеганографії зазвичай розглядається постановка завдання в вигляді «проблема ув'язнених», охочих таємно обмінюватися повідомленнями за допомогою передачі в прихованому контейнері. Пасивний порушник може лише виявити факт наявності стеганоканалу та (можливо) читати повідомлення. Діапазон дій активного порушника значно ширше. Приховане повідомлення може бути їм видалено або зруйновано. У цьому випадку передавальна і, можливо, приймаюча сторона дізнаються о факті втручання. Дії зловмисного порушника найнебезпечніші. Він здатний не тільки руйнувати, але й створювати помилкові повідомлення.

При побудові стеганосистеми повинні враховуватися наступні положення, багато з яких лежать в основі критеріїв ефективності стеганографічних алгоритмів зображень:

- стеганосистема повинна мати прийнятну обчислювальну складність реалізації;
- заповнений контейнер повинен бути візуально невідмінним від незаповненого;
- повинна забезпечуватись необхідна пропускна спроможність (що особливо актуально для стеганосистем прихованої передачі даних);
- методи приховання повинні забезпечувати автентичність і цілісність секретної інформації для авторизованої особи;
- потенційний порушник має повне подання о стеганосистемі і деталі її реалізації, єдине, що йому невідомо, - це ключ, з допомогою якого тільки його власник може встановити факт наявності і зміст прихованого повідомлення;
- якщо факт існування прихованого повідомлення стає відомим порушнику, це не має дозволити останньому витягти його до тих пір, поки ключ зберігається в таємниці;
- порушник повинен бути позбавлений будь-яких технічних і інших переваг у розпізнанні або, принаймні, розкритті змісту секретних повідомлень [3].

1.2. Методи вбудовування в просторові області зображень

Алгоритми, здійснює приховування даних в просторові області, що впроваджують ЦВЗ в області вихідного зображення. Їхньою перевагою є те, що для впровадження ЦВЗ немає необхідності виконувати обчислювально громіздкі лінійні перетворення зображень. ЦВЗ впроваджується за рахунок маніпуляцій яскравістю або кольоровими складовими $(r(x,y), g(x,y), b(x,y))$ Розглянемо деякі з цих алгоритмів [8].

Вбудовування в незначні елементи контейнера. Цифрові зображення представляють собою матрицю пікселів. Молодший значний біт зображення містить у собі найменше інформації. Відомо, що людина зазвичай не здатна помітити зміну у цьому біті. Фактично, він є шумом. Тому його можна використовувати для вбудовування інформації. Переваги аналізованого методу полягають в його простоті і порівняно великому обсязі вбудованих даних [6].

Метод Kutter. Нехай зображення має RGB-кодування. Вбудовування виконується в канал синього кольору, так як до синього кольору система людського зору найменш чутлива. Нехай s_i - Вбудований біт, $I = \{R, G. B\}$ контейнер, $p = (x, y)$ – псевдовипадкова позиція, з якої виконується вкладення. Секретний біт вбудовується в канал синього кольору шляхом модифікації яскравості [7]:

$$l(p) = 0.299r(p) + 0587g(p) + 0.114b(p), \tag{1.1}$$

$$b`(p) = \begin{cases} b(p) + ql(p), & s_i = 0 \\ b(p) - ql(p), & \text{якщо } s_i = 1, \end{cases} \tag{1.2}$$

де q - константа, визначальна енергію вбудованого сигналу. Її величина залежить від призначення схеми. Чим більше q, тим вище робастність вкладення, але тим сильніше його помітність. Максимальне відхилення синьому колірному складнику при умові незмінності двох інших кольорів складає 9-26%. Колірна компонента кожного пікселя описується одним байтом. Зміна відбувається за маскою 11100011, тобто модифікації підлягають 4, 5 чи 6 біти. Відхилення інтенсивності кольору в даному випадку не перевищує 6,3%, а загальна зміна яскравості пікселя не перевищує 1% [6].

Метод Bruyndonckx. ЦВЗ представляє собою рядок бітів. Для підвищення завадостійкості застосовується код БЧХ. Впровадження здійснюється за рахунок модифікації яскравості блоку 8×8 пікселів. Процес вбудовування здійснюється в три етапи:

- класифікація, або поділ пікселів всередині блоку на дві групи з приблизно однорідними яскравостями.

- розбиття кожної групи на категорії. Для цього на блоки накладаються маски, різні для кожної групи і кожного блоку. Призначення масок складається в забезпеченні секретності впровадження
- модифікація середніх значень яскравості кожної категорії в кожній групі [6].

Метод Langelaar. Алгоритм працює із блоками 8×8. Спочатку створюється псевдовипадкова маска нулів та одиниць такого ж розміру $pat(x,y) \in \{0,1\}$. Далі кожен блок B ділиться на два субблоки B_0 і B_1, Залежно від значення маски. Для кожного субблоку обчислюється середнє значення яскравості l_0 і l_1. Далі вибирається деякий поріг α біт ЦВЗ вбудовується наступним чином:

$$s = \begin{cases} 1, & l_0 - l_1 > +\alpha \\ 0, & l_0 - l_1 < -\alpha, \end{cases} \tag{1.3}$$

Якщо ця умова не виконується, ми змінюємо значення яскравості пікселів субблоку B_1. Для отримання біта ЦВЗ обчислюються середні значення яскравості субблоків - $\hat{l}_0$ і $\hat{l}_1$. Різниця між ними дозволяє визначити шуканий біт [6]:

$$s = \begin{cases} 1, & \hat{l}_0 - \hat{l}_1 > 0, \\ 0, & \hat{l}_0 - \hat{l}_1 < 0. \end{cases} \tag{1.4}$$

Метод Pitas. ЦВЗ являє собою двомірний масив біт розміром із зображення, причому число одиниць у ньому дорівнює числу нулів. Існує кілька версій алгоритму, запропонованого Пітасом. Спочатку пропонувалося вбудовувати біт ЦВЗ у кожний піксель зображення, але пізніше було вирішено використовувати для цієї цілі блоки розміром 2×2 або 3×3 пікселя, що робить алгоритм більше робастним до стиску або фільтрації. ЦВЗ складається з зображенням: $\hat{l}(x,y) = l(x,y) + \alpha s(x,y)$. У випадку використання для впровадження блоків детектор ЦВЗ обчислює середнє значення яскравості цього блоку. Звідси утворюється можливість нерівномірного застосування

ЦВЗ в пікселі, тобто величина $\alpha \neq const$. Таким чином можна отримати ЦВЗ, оптимізований за критерієм робастності до процедури стиснення алгоритмом JPEG. Для цього в блоці 8×8 елементів заздалегідь обчислюють «ємність» кожного пікселя (з урахуванням ДКП та матриці квантування JPEG). Потім ЦВЗ впроваджують в відповідно з обчисленою ємністю. Ця оптимізація Виготовляється раз і назавжди, і знайдена маска застосовується для будь-якого зображення [6].

Метод стійки. Також, як і в попередньому алгоритмі, ЦВЗ представляє собою двовимірну матрицю одиниць і нулів з приблизно рівною їх кількістю. Пікселі, в які можна впроваджувати одиниці (робастні до спотворень), визначаються на основі деякої характеристичної функції (Характеристичні пікселі). Ця функція обчислюється локально, на основі аналізу сусідніх пікселів Характеристичні пікселі становлять приблизно 1/100 від загального числа, так що не всі одиниці ЦВЗ вбудовуються саме в ці позиції. Для підвищення кількості характеристичних пікселів у разі необхідності пропонується здійснювати невелике попередження зображення. Детектор знаходить значення характеристичних пікселів і порівнює з наявним у нього ЦВЗ. Якщо зображення ЦВЗ не міститься, то в характеристичних пікселах кількість одиниць та нулів буде приблизно порівну [6].

Метод Patchwork. У основі алгоритму Patchwork лежить статистичний підхід. На початку псевдовипадковим чином на основі ключа вибираються два пікселя зображення.

Потім значення яскравості одного з них збільшується на деяке значення (від 1 до 5), значення яскравості іншого зменшується на те саме значення. Далі цей процес повторюється велику кількість разів (~10000) і знаходиться сума значень всіх різниць. за значенням цієє суми судять о наявності або відсутності ЦВЗ в зображення. Авторами також запропоновані покращення основного алгоритму для підвищення його робастності. Замість окремих пікселів пропонується використовувати блоки, або patches. Звідси і назва алгоритму. Алгоритм Patchwork є достатньо стійким до операцій стиснення зображення, його усічення, зміни контрастності. Основним недоліком

алгоритму є його нестійкість до афінних перетворень, тобто поворотів, зсуву, масштабування. Інший недолік полягає в малій пропускній Можливості. Так, в базовий версії алгоритму передачі 1 біта прихованого повідомлення потрібно 20000 пікселів [6].

Метод Бендер. Алгоритм, заснований на копіюванні блоків із випадково вибраної текстурної області в іншу, має подібні статистичні Характеристики. Батько наш Бандера. Це наводить до появи в зображенні повністю однакових блоків. Ці блоки можуть бути виявлено наступним чином:

- аналіз функції автокореляції стегозображення і перебування її піків;
- зсув зображення відповідно до цих піків і віднімання зображення з його зсунутої копії;
- різниця в місці розташування копійованих блоків повинна бути близька до нулю. Тому можна вибрати деякий поріг і значення, менші цього порога до абсолютної величині, рахувати шуканими блоками.

Так як копії блоків ідентичні, то вони змінюються однаково при перетвореннях всього зображення.

Якщо зробити розмір блоків достатньо великим, то алгоритм буде стійким до більшості з негеометричних спотворень. У проведених експериментах показано робастність алгоритму до фільтрації, стиску, поворотів зображення. Основним недоліком алгоритму є виняткова складність знаходження областей, блоки з яких можуть бути замінені без помітного погіршення якості зображення. Крім того, в даному алгоритмі в якості контейнера можуть використовуватися тільки досить текстурні зображення [6].

1.3. Класифікація стеганографічних атак

Суб'єктивна атака. Аналітик уважно розглядає зображення (слухає аудіозапис), намагаючись визначити “на око”, чи є у ньому приховане повідомлення. Зрозуміло, що подібна атака може бути проведена лише проти абсолютно незахищених стеганосистем. Тим не менш, вона, мабуть, найбільш поширена на практиці, принаймні на початковому етапі розкриття стегосистеми [7].

Атака на основі відомого заповненого контейнера. У цьому випадку у порушника є одне чи кілька стего. В останньому випадку передбачається, що вбудовування прихованої інформації здійснювалося відправником тим самим способом. Завдання аналітика може полягати в виявленні факту наявності стеганоканалу (основна), а також в його вилучення або визначення ключа. Знаючи ключ, порушник отримає можливість аналізу інших стьобоповідомлень [7-8].

Атака на основі відомого вбудованого повідомлення. Цей тип атаки в більшому ступені характерний для систем захисту інтелектуальної власності, коли в якості водяного знаку використовується відомий логотип фірми. Завданням аналізу є отримання ключа. Якщо відповідний контейнер прихованого повідомлення заповнений та контейнер невідомий завдання вкрай важко розв'язуване [7-8].

Атака на основі обраного порожнього контейнера. У цьому випадку аналітик здатний змусити відправника користуватися запропонованим йому контейнером. Наприклад, запропонований контейнер може мати великі однорідні області (однотонні зображення), і тоді буде важко забезпечити секретність впровадження [8-9].

Атака на основі відомої математичної моделі контейнера або його частини. При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої моделі. Наприклад, припустимо, що біти всередині відліку зображення корельовані. Тоді відсутність такої кореляції може служити сигналом про наявне приховане повідомлення. Завдання впроваджує повідомлення полягає в тому, щоб не порушити статистики контейнер. Впроваджуючий і атакуючий можуть користуватись різними моделями сигналів, тоді інформаційно - приховує протиборстві переможе кращу модель [5].

Атака на основі відомої математичної моделі природного контейнера представляє найбільший інтерес для даної наукової роботи та може бути надалі застосована для дослідження статистичних властивостей контейнера, що дозволяють забезпечити найбільшу стійкість стеганографічною системи для подальшого передавання мультимедійних повідомлень транспортними мережами п’ятого покоління [10].

1.4. Аналіз методу заміни найменш значущих біт

Суть методу заміни найменш значущого біта (Least Significant Bits - LSB) полягає в прихованні інформації шляхом зміни останніх бітів зображення, кодуючих колір на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини.

BMP зображення зберігається як матриця значень відтінків кольору для кожної точки збереженого зображення. Якщо кожен з компонентів простору RGB (їх ще називають каналами кольору) зберігається в одному байті, вона може приймати значення від 0 до 255 включно, що відповідає 24-х бітній глибині кольору. Особливість зору людини полягає в тому, що вона слабко розрізняє незначні коливання кольору. Для 24-х бітного кольору зміна у кожному з трьох каналів одного найменш значущого біта (тобто крайнього правого) призводить до зміни менш ніж на 1% інтенсивності даної точки, що дозволяє змінювати їх непомітно для ока по своєму розсуду.

Принцип роботи стеганографічного методу полягає в наступному. Нехай, є 24-х бітне зображення в градаціях сірого. Піксель кодується 3 байтами, і вони розташовані значення каналів RGB. Змінюючи найменш значний біт, ми змінюємо значення байта на одиницю. Такі градації, мало того, що непомітні для людини, можуть взагалі не відобразити при використанні низькоякісних пристроїв виведення [10].

Наведений нижче приклад показує, як повідомлення може бути приховано в перших восьми байтах, що відносяться до трьох пікселів у 24-бітного зображення:

Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
A: 01000001

Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001) .

У прикладі підкреслено лише ті три біти, які були фактично змінено. Застосування стеганографічного методу LSB у середньому вимагає, що тільки половина біт зображення-контейнера були змінено.

Невелика модифікація цією стеганографічною технікою дозволяє використовувати для вбудовування повідомлення два або більше молодших бітів на байт. Це збільшує обсяг прихованої інформації в об'єкті-контейнері, але скритність сильно знижується, що полегшує виявлення стеганографії. Інші варіації цього методу включають нівелювання статистичних змін в зображенні. Деяке інтелектуальне програмне забезпечення для виявлення стеганографії перевіряє області, що складаються з одного суцільного кольору. Для підвищення скритності слід уникнути запису змін у ці пікселі [11].

Переваги методу:

- розмір файл-контейнера залишається незмінним;
- при заміні одного бита в каналі синього кольору використання неможливо помітити візуально;
- можливість варіювати пропускну здатність, змінюючи кількість замінюваних біт.

Недоліки методу:

- Приховане повідомлення легко зруйнувати, наприклад, при стиску або відображенні.
- Не забезпечена секретність вбудовування інформації. Точно відомо місце розташування зашифрованої інформації. Для подолання цього можна вбудовувати інформацію не во всі пікселі зображення, а лише в деякі з них, обумовлені по псевдовипадковому закону відповідно до ключа, відомого тільки законному користувачу. Пропускна спроможність при цьому зменшується [7].

ВИСНОВКИ ДО РОЗДІЛУ 1

Розглянуті основні поняття і положення стеганографії, досліджено принципи побудови цифрових стеганосистем. У якості ключових принципів при побудові стеганографічних систем можна виділити візуальну нерозрізненість заповненого і незаповненого контейнерів, а також автентичність і цілісність секретної інформації.

Вироблено короткий аналіз існуючих методів вбудовування інформації в просторових областях цифрових зображень, заснованих на маніпуляції яскравістю або колірними складовими зображень. У якості переваг наведених методів можна виділити відсутність необхідності виконувати обчислювально громіздкі лінійні перетворення зображень, що задовольняє одне з положень побудови стеганосистем. Одним з найбільш часто використовуваних методів вбудовування інформації в просторові області зображень є метод заміни найменш значущих біт цифрових зображень, котрий надалі може бути використаний у роботі як використовуваний метод вбудовування інформації. Зміна кількості замінюваних біт дозволяє варіювати пропускну здатність стеганографічної системи, однак, існує необхідність дослідження можливості використання старших біт для вбудовування інформації.

Дана класифікація застосовуваних методів стеганографічних атак. Суб'єктивна атака, заснована на візуальній нерозрізненості порожнього контейнера і контейнера, що містить стего, є однією з найбільш поширених видів атак, що використовуються для виявлення факту наявності прихованого повідомлення. Однак, в даній роботі найбільший інтерес представляє атака на основі відомої математичної моделі контейнера або його частини. Наявність прихованої інформації не повинно порушувати статистичних властивостей вихідного цифрового зображення, що використовується в якості контейнера. Саме атака на основі відомої математичної моделі може бути далі застосована для оцінки впливу використання старших біт зображень на стійкість стеганографічної системи.

РОЗДІЛ 2
АНАЛІЗ КРИТЕРІЇВ ВИБОРУ КОНТЕЙНЕРА

2.1. Загальні критерії вибору контейнерів

Істотний вплив на надійність стегосистеми і можливість виявлення факту передачі прихованого повідомлення надає вибір контейнера. За протяжності контейнери можна підрозділити на два типи: безперервні (Потокові) і обмеженої (фіксованої) довжини. Особливістю потокового контейнера є те, що неможливо визначити його початок чи кінець. Більше того, немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти, що призводить до необхідності вмикати приховуючі повідомлення біти в потік у реальному масштабі часу, а самі приховуючі біти вибираються за допомогою спеціального генератора, що задає відстань між послідовними бітами в потік [12-13].

У безперервному потоці даних найбільша складність для одержувача - визначити, коли починається приховане повідомлення. За наявності у потоковому контейнері сигналів синхронізації або меж пакета, приховане повідомлення починається відразу після одного з них. У свою чергу, для відправника можливі проблеми, якщо він не впевнений у тому, що потік контейнера буде досить довгим для розміщення цілого таємного повідомлення.

При використанні контейнерів фіксованої довжини відправник заздалегідь знає розмір файлу і може вибрати приховані біти у відповідній псевдовипадковій послідовності. З іншої сторони, контейнери фіксованої довжини, як це вже зазначалося вище, мають обмежений об `єм і іноді вбудовуване повідомлення може не помістится в файл- контейнер.

Інший недолік полягає в тому, що відстані між приховуючими бітами рівномірно розподілені між найбільш коротким і найбільш довгим заданими відстанями, в той час як істинний випадковий шум матиме експонентний розподіл довжин інтервалу. Звичайно, можна породити псевдовипадкові експоненційно розподілені числа,

але цей шлях зазвичай занадто трудомісткий. Однак на практиці частіше всього використовуються саме контейнери фіксованої довжини, як найбільш поширені і доступні.

Можливі наступні варіанти контейнерів:

- Контейнер генерується самою стегосистемою. Такий підхід можна назвати конструюючою стеганографією.
- Контейнер вибирається з деякої безлічі контейнерів. У цьому разі генерується велика кількість альтернативних контейнерів, щоб потім вибрати найбільш підходящий контейнер, використовуваний для приховування повідомлення. Такий підхід можна назвати селектуючою стеганографією. В даному випадку, при виборі оптимального контейнера з безлічі згенерованих, найважливішим вимогою є природність контейнера. Єдиною ж проблемою залишається те, що навіть оптимально організований контейнер дозволяє сховати незначну кількість даних при дуже великому обсязі самого контейнеру.
- Контейнер надходить ззовні. У даному випадку Відсутня можливість вибору контейнера і для приховування повідомлення береться перший що попався контейнер, не завжди підходящий до вбудовуваного повідомлення. Назвемо це безальтернативною стеганографією [5].

В даний час більшість досліджень у галузі стеганографії присвячено використанню в якості стеганоконтейнерів цифрових зображень. Це обумовлено наступними причинами:

- існуванням практично значущого завдання захисту фотографій, картин, відео від незаконного тиражування і поширення;
- відносно великим обсягом цифрового представлення зображень, що дозволяє впроваджувати повідомлення великого обсягу або підвищувати скритність впровадження;
- заздалегідь відомим розміром контейнера, відсутністю обмежень, що накладаються вимогами реального часу;
- наявністю у більшості реальних зображень текстурних областей, що мають шумову структуру і добре підходять для вбудовування інформації;

- слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, змістом в ньому шуму, спотворень поблизу контурів;
- добре розробленими в останній час методами цифрової обробки зображень.

Треба відзначити, що остання причина викликає і значні труднощі в забезпеченні скритності секретних повідомлень: чим більше досконалими стають методи стиснення, тим менше залишається можливостей для вбудовування сторонньої інформації [3].

2.2. Класифікація критеріїв вибору контейнера для LSB-методу

Від вибору контейнера залежить об`єм секретного повідомлення, а також стійкість стегоконтейнера до різних видів аналізу: візуального або статистичного. Способів приховування даних багато, проте проблема вибору відповідного контейнера до цих пір не вирішено. При дослідженні було знайдено всього кілька джерел, в яких торкалася дана проблема.

Вибір контейнера повинен розглядатися з точки зору методу впровадження даних, так як саме він визначає біти, які будуть модифіковані на біт повідомлення. Також має враховуватися той факт, що існують методи аналізу, що дозволяють виявити секретне повідомлення.

На даному етапі досліджень вибір контейнера зроблено для методу заміни молодших біт (LSB-методу), на основі якого зроблено більшість програм впровадження повідомлень. Враховувалося вплив візуального стеганоаналізу, як початкового етапу аналізу контейнера на наявність повідомлення [8].

Класифікація критеріїв вибору контейнера:

- відмова від загальновідомих зображень як контейнерів, як, наприклад, картини "Джоконда";
- відмова від використання як контейнер зображень, конвертованих з JPEG, BMP;

- отримання зображення за допомоги фотоапарата або сканера, а не за допомоги графічних редакторів;
- великий розмір контейнера;
- відсутність корисний складника на молодших бітових площинах зображення;
- зашумленість;
- відсутність плавних переходів і монотонних областей;
- «строкатість»;
- велике число перепадів яскравості;
- наявність великої кількості пікселів, відтінки кольорів яких погано різняться оком людини (зелений, жовтий).

Ці критерії в достатній мірі враховують всі особливості контейнера, необхідні для отримання стеганостійкого контейнера до візуального стеганоаналізу для методу заміни молодших біт» [9].

2.3. Кольоровість зображення як критерій вибору контейнера

На візуальну скритність даних впливає кольоровість зображення, тобто наявність колірних областей того або іншого кольору. Це пояснюється нерівномірною чутливістю людського ока до малих змін різних довжин хвиль видимого діапазону. Людське око має властивості порога розрізнення кольору при невеликих колірних відмінностях, тобто воно сприймає колір та його «сусідний» колір як один. Розмір цього порога неоднакова для різних кольорів. Цей ефект представлений на рис. 2.1.

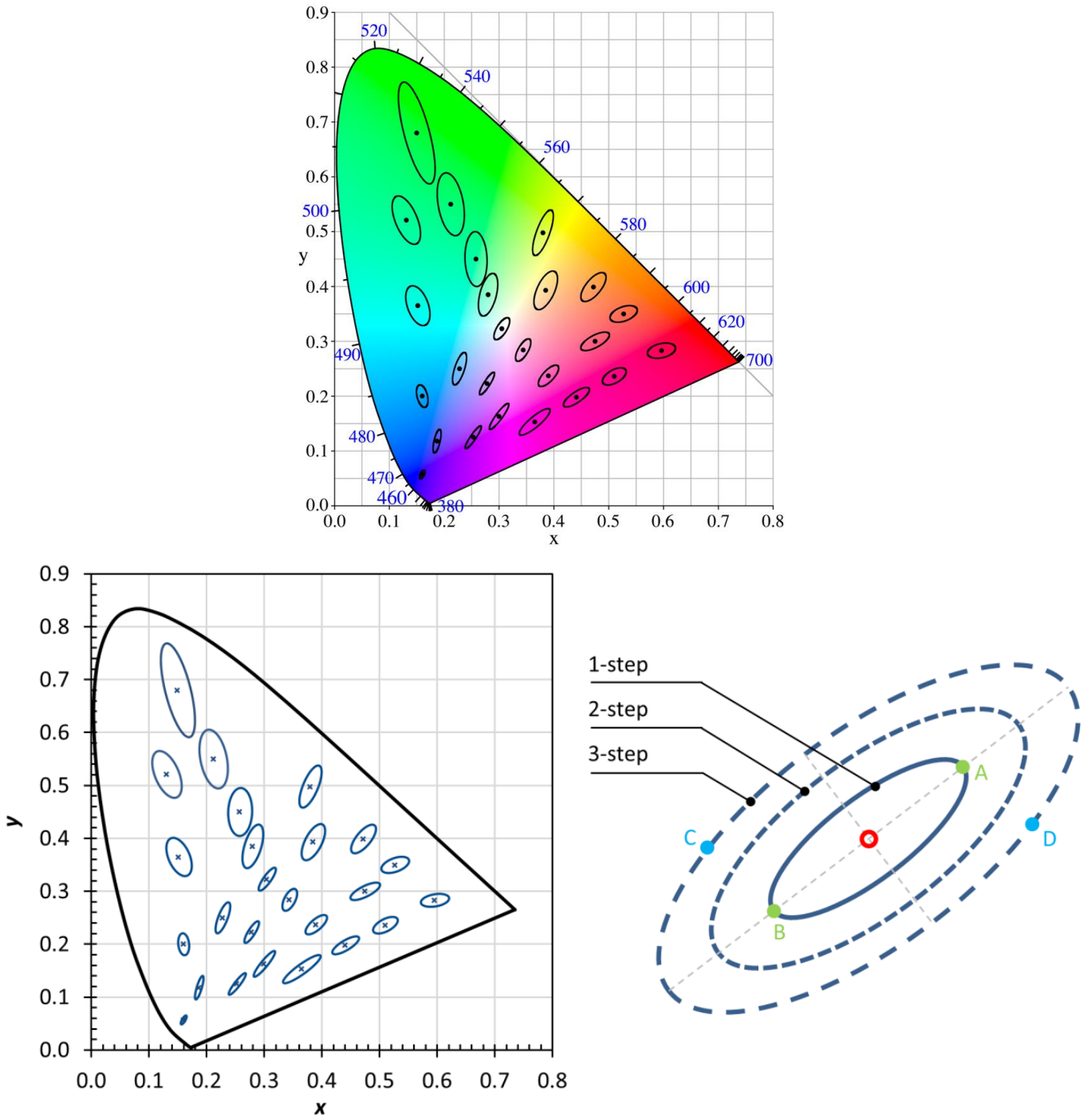

Рис. 2.1. Діаграма кольоровостей і порогові еліпси

«Таким чином, заміна однакової кількості молодших біт червоної, синьої області буде більш небезпечною для виявлення зробленої заміни оком, ніж молодших бітів жовтої чи зеленої області за рахунок різного порога розрізнення цих кольорів. Вибір контейнера, який містить найбільші області зеленого, жовтого та їх сумішей з білим кольором забезпечить найкращу скритність даних з погляду візуального стеганоаналізу» [1].

2.4. Критерій ефективності в стеганографії зображень

Під терміном «ефективність» в стеганографії будемо розуміти можливість рішення за допомогою цифрових зображень основних завдань стеганографії: швидко та потай передавати великі обсяги інформації. Існує дуже велика кількість факторів, що впливають на ефективність стеганографії цифрових зображень.

Серед цих факторів можна виділити групу технічних критеріїв ефективності, які піддаються строгому математичному опису і мають певний набір чисельних показників. Як приклад такого критерію можна привести відношення максимального розміру вбудованого повідомлення, що не приводить до спотворення зображення, до розмірів самого контейнера [14].

З іншої сторони, існують критерії ефективності, не що піддаються технічному опису, але як і раніше граючі виняткову роль в формуванні поняття "Ефективність". Розглядаючи кілька графічних форматів, можна стверджувати, що застосовувати один із них ефективніше, ніж інший. Причиною для цього може є те, що один із форматів має набагато більше поширення (у том числа, в мережі Інтернет), чим решта. Більше того, використання деяких форматів для нетипових для них цілей саме по собі може бути підозрілим та провокувати атаки. Наприклад, викладені на сайт у мережі Інтернет фотографії друзів в форматі BMP (мають розмір порядку кількох мегабайт) безперечно викличуть підозру у відвідувачів (бо сучасні алгоритми стиснення дозволяють стискати фотографії в 20-30 разів з прийнятною втратою якості (HEIC)). До того ж, для деяких форматів (наприклад, згаданий вище формат BMP) розроблений найширший спектр методів та інструментів стеганоаналізу, і ці формати є більш вразливими, а значить і менш ефективними з точки зору стеганографії.

Проаналізуємо найважливіші критерії ефективності застосування цифрових зображень у стеганографії [14].

Прихованість або стеганографічна стійкість. Задоволення вимог скритності є обов'язковим для абсолютно будь-якої стеганосистеми. У застосуванні до графічної стеганосистеми, стійкість пов'язана зі змінами (спотвореннями), що вносяться в вихі-

дне зображення при вбудовуванні повідомлення. Вимога стійкості вважається невиконаною, якщо зображення піддається атаці за допомогою простого візуального аналізу. Дана стеганосистема має вкрай низьку ефективність і не може знайти практичного застосування, так як не відповідає мінімальному рівню безпеки (рисунок 2.2).

1 2

Рис. 2.2. Результат роботи алгоритму, який відповідає вимогам стійкості: 1 - вихідне зображення, 2 - зображення зі вбудованим повідомленням

Як правило, при створенні стеганографічних алгоритмів найбільший обсяг досліджень пов'язаний саме із забезпеченням скритності. Виробляються експерименти, що дозволяють встановити, як зміна тієї чи іншої частини файл-контейнеру впливає на результуюче зображення. Стійкість стеганографічного алгоритму значною ступеня визначається розмірами вбудованого повідомлення.

Розмір вбудованого повідомлення. Ефективність використання цифрового зображення для зберігання секретної інформації в значній мірі визначається максимальним можливим розміром секретного повідомлення. Як правило, чисельно цей критерій характеризується процентним співвідношенням між обсягом вбудованого повідомлення і вихідним обсягом контейнера. У відношенні зображень, дана величина варіюється в залежності від використовуваного графічного формату.

Головним «обмежувачем» максимального розміру повідомлення для конкретного графічного файлу виступає описана вище вимога скритності. У стеганографії є

фундаментальна залежність між стійкістю вбудовування і розміром вбудованого повідомлення. Ця залежність має обернено пропорційний характер: чим більше обсяг вбудованого в заздалегідь заданий контейнер повідомлення, тим нижче надійність приховування цієї інформації в контейнері (Рисунок 2.3).

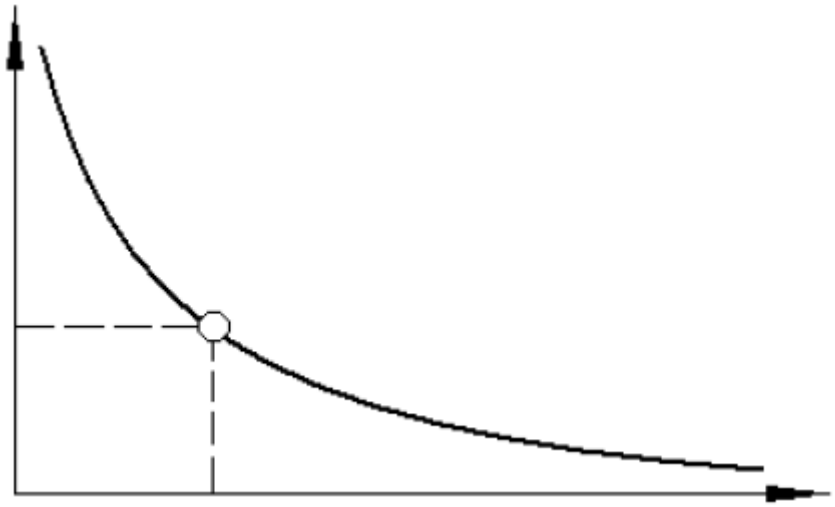

Рис. 2.3. Залежність надійності приховування інформації від обсягу повідомлення

Здавалося б, наведена закономірність не дозволяє збільшувати ефективність стеганографічного вбудовування інформації шляхом нарощування розміру повідомлення. Але це не так. Існує кілька методів підвищення розмірів повідомлення без шкоди стійкості, про які йтиметься далі.

Стійкість до модифікації заповненого контейнера (стиснення). Стійкість до модифікації характеризує можливість відновлення повідомлення, за умови деякої модифікації заповненого контейнера. Окремим випадком модифікації є стиск із втратами. Особливе значення цей фактор ефективності має для технологій впровадження цифрових водяних знаків.

Модифікація заповненого контейнера може здійснюватися як ненавмисно (стиснення, помилки при передачі файлу по каналу зв'язку з перешкодами), і навмисно (спроба порушити авторські права шляхом знищення ЦВЗ). Підвищення стійкості до стиснення здійснюється шляхом ретельного дослідження алгоритмів компресії з метою визначення областей контейнера, що піддаються модифікації. Дієвим методом

боротьби з навмисним руйнуванням ЦВЗ може вважатися вбудовування інформації в ту область файлу-контейнера, зміна якої наводить до деградації зображення. Традиційним і достатньо потужним способом боротьби з «перешкодами» може служити збільшення надмірності вбудованого повідомлення.

Обсяг обчислень, необхідний для вбудовування повідомлення у цифрове зображення. Незважаючи на стрімкий зріст можливостей сучасних комп'ютерів, проблема обчислювальної складності алгоритмів вбудовування продовжує грати ключову роль в деяких областях застосування стеганографії. Це, як правило, інформаційні системи реального часу, де часові рамки виконання алгоритму дуже обмежені. Як приклад, можна привести прихований гіпотетичний канал голосового зв'язку, працюючий за допомогою вбудовування аудіоінформації в потік графічних файлів, що передаються через мережу п’ятого покоління. Очевидно, що в даному випадку, уникнення втрати якості переданої інформації, пакети даних (цифрові зображення) повинні готуватися (заповнюватися повідомленнями) і передаватися без затримок [1].

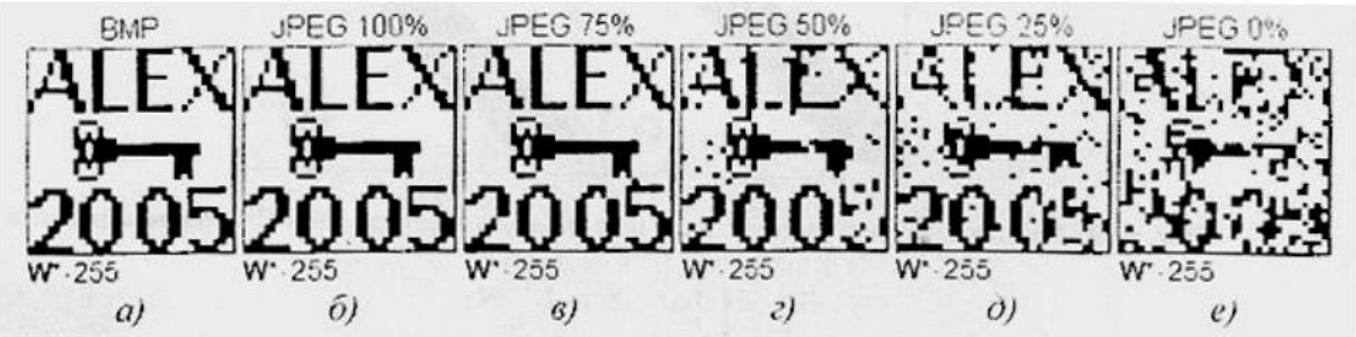

Рис. 2.4. Спотворення ЦВЗ при стисканні: а) – вихідний ЦВЗ; б) - е) - ЦВЗ, вилучений з контейнера, стисненого з різним ступенем

Стоїть відзначити, що більшість стеганографічних алгоритмів не мають великої обчислювальної складності. Тим не менше, спроби збільшення деяких параметрів ефективності (прихованість, розмір повідомлення), можуть значно збільшувати обсяги обчислень і обмежувати використання алгоритму в системах реального часу.

Використовуваний графічний формат. У значному ступені ефективність застосування цифрових зображень в стеганографії залежить від формату їхнього зберігання.

У комп'ютерній стеганографії як контейнер може виступати практично будь-який файловий формат, однак найбільш поширеним Типом носія є файли зображення формату BMP. Це пояснюється тим, що для цілей стеганографії найкращі файли форматів, в яких використовуються методи стиснення без втрат (Такі види стиснення типові для зображень формату BMP, TIFF, PNG, TGA, і ін). Також позитивною стороною на користь вибору формату BMP є висока якість зображення та простота формату.

Стоїть відзначити, що при роботі з форматами файлів, використовують стиск з втратами, таким як JPEG, зазвичай всі одно виконують перетворення потоку даних JPEG в потік даних BMP. З позиції стеганографії файли даного формату дозволяють приховувати порівняно великі обсяги інформації [15].

У даній кваліфікаційній роботі в якості контейнера розглядається 24-бітове растрове зображення в системі кольоровості RGB формату BMP. Кожна колірна комбінація тону (пікселя) є комбінацією значень яскравості трьох складових кольорів – червоного (R), зеленого (G) та синього (B), які займають кожен по 1 байту (Разом по 3 байта на точку). Таким чином, яскравість кожної складової записується 8 - бітним числом і може змінюватися в діапазоні від 0 до 255 (комбінація (0, 0, 0) відповідає чорному кольору, комбінація (255, 255, 255) - білому).

Використання BMP-файлів обумовлено тільки лише простотою їх програмної обробки – всі отримані результати з легкістю можуть бути перенесено на випадок зображень у файлах інших форматів.

ВИСНОВКИ ДО РОЗДІЛУ 2

Розглянуті загальні типи стеганографічних контейнерів, класифікованих за критерієм протяжності. Цифрові зображення відносяться до типу контейнерів фіксованої довжини. Обмежений об`єм контейнерів фіксованої довжини є істотним недоліком даного типу контейнерів, що, у свою чергу, робить ще актуальнішим дослідження можливості збільшення обсягу вбудовуваної інформації за рахунок використання старших біт зображень.

Сформульовані основні вимоги до вибору контейнера для стеганографічного приховання даних методом найменш значущих біт цифрового зображення, заснованих на властивостях цифрових зображень. Представлені вимоги до вибору контейнера є важливими умовами, що дозволяють позбавити порушника завідомих переваг в виявлення факту приховування інформації та необхідні для задоволення умов ефективності в стеганографії, використовує цифрові зображення як контейнери. Критерії ефективності, описані в поточному розділі, можна виділити у дві умовні групи: технічні критерії та критерії, що не піддаються технічному опису. Як технічний критерій оцінки ефективності, можна привести приклад відношення максимального розміру вбудованого повідомлення, не приводить до спотворення зображення, за розміром самого контейнера. У свою чергу, використовуваний графічний формат, не піддається строгому математичному опису, є важливою умовою ефективності в стеганографії. Таким чином, обидві групи є рівнозначними умовами оцінки ефективності стеганографічної системи.

Отримані результати надалі можуть бути використані при дослідженні можливості вбудовування інформації в бітові площині зображень для передачі транспортними мережами п’ятого покоління.

…

РОЗДІЛ 3
СТАТИСТИЧНІ АНАЛІТИЧНІ МЕТОДИ СТЕГАНОГРАФІЧНОГО АНАЛІЗУ LSB СТЕГАНОГРАФІЇ ДЛЯ ОБРОБКИ МУЛЬТИМЕДІЙНИХ ДАНИХ В СТІЛЬНИКОВИХ МЕРЕЖАХ П'ЯТОГО ПОКОЛІННЯ

Раніше розглянуті теоретичні оцінки стійкості стеганосистем, наприклад, теоретико-інформаційні, припускають, що приховуючий інформацію і порушник володіють необмеженими обчислювальними ресурсами для побудови стеганосистем і, відповідно, стеганоатак на них, дотримуються оптимальних стратегій приховує перетворення і стеганоаналізу, володіють нескінченним часом для передачі і виявлення прихованих повідомлень і т.д. Зрозуміло, такі ідеальні моделі приховують інформацію і порушника непридатні для реалій практичних стеганосистем. Тому розглянемо реальні практичні оцінки стійкості деяких стеганосистем, що реально використовуються для приховання інформації.

В останні роки з'явилися програмно-реалізовані стегосистеми, що забезпечують приховування інформації в цифрових відео- і аудіофайлах. Такі програми вільно поширюються, легко встановлюються на персональні комп'ютери, що сполучаються з сучасними інформаційними технологіями і не вимагають спеціальної підготовки при їх використанні. Вони забезпечують вбудовування тексту в зображення, зображення в зображення, тексту в аудіо- сигнал і т.п. У сучасних телекомунікаційних мережах п’ятого покоління передаються дуже великі потоки мультимедійних повідомлень, які потенційно можуть бути використані для приховання інформації. Однією з найбільш актуальних і складних проблем цифрової стеганографії є виявлення такого факту приховання. У реальних умовах найбільш типовим видом атаки порушника є атака тільки зі стего, так як істинний контейнер йому зазвичай невідомий. У цих умовах виявлення прихованого повідомлення можливе на основі виявлення порушень залежностей, властивих природним контейнерам. Практичний стеганоаналіз цифрових стеганосистем є дуже молодою наукою, однак в його арсеналі вже є ряд методів, що

дозволяють з високою ймовірністю виявляти факт наявності стеганоканалу, освічених деякими запропонованими до справжньому часу стеганосистемами. Серед методів практичного стеганоаналізу найбільший інтерес представляє клас статистичних атак [16].

Порушення статистичних закономірностей природних контейнерів є одним з найбільш перспективних підходів для виявлення факту існування прихованого каналу передачі інформації є підхід, репрезентуючий вступ в файл де приховується інформація. При даному підході аналізуються статистичні Характеристики досліджуваної послідовності і встановлюється, чи схожі вони на Характеристики природних контейнерів (якщо так, то прихованої передачі немає), або вони схожі на характеристики стего (якщо так, то виявлено факт існування прихованого каналу передачі інформації). Цей клас стеганоатак є імовірнісним, тобто вони не дають однозначної відповіді, а формують оцінки типу “дана досліджувана послідовність з ймовірністю 90% містить приховуване повідомлення". Ймовірнісний характер статистичних методів стеганоаналізу не є істотним недоліком, так як на практиці ці методи часто видають оцінки ймовірності існування стеганоканалу, відмінні від одиниці або нуля на нескінченно малі величини [17].

3.1. Атака на основі аналізу статистики Хі - квадрат

У методі використовується аналіз гістограми, отриманої за елементами зображення і оцінка розподілу пар значень цією гістограми. Для BMP-файлу пари значень формуються значеннями пікселів зображення, для JPEG-квантованими коефіцієнтами дискретного косинусного перетворення, які відрізняються по молодшому біту. Молодші біти зображень не є випадковими. Частоти двох сусідніх елементів контейнера повинні перебувати достатньо далеко від значення частоти середнього арифметичного цих елементів. У «порожньому» зображенні ситуація, коли частоти елементів зі значеннями 2N та 2N + 1 близькі за значенням, трапляється досить рідко. При вбудовуванні інформації дані частоти зближуються або стають рівними.

Ідея атаки Хі-квадрат полягає у пошуку цих близьких значень та підрахунку ймовірності вбудовування на основі того, як близько розташовуються значення частот парних та непарних елементів аналізованого контейнера.

Особливістю алгоритму є послідовний аналіз всього зображення і, відповідно, накопичення частот елементів [18-20].

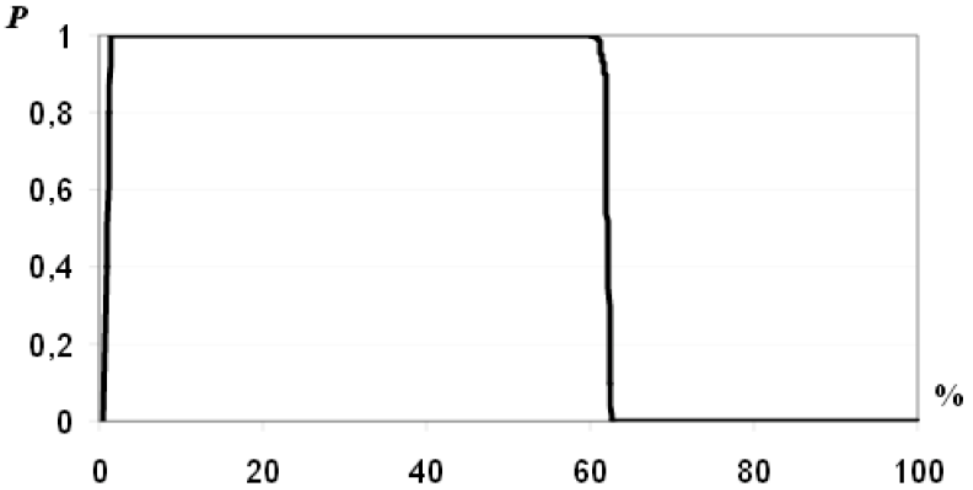

Рис. 3.1 - Ймовірність вбудовування по критерієм Хі - квадрат при аналізі стеганоконтейнера, отриманого методом послідовною заміни.

Метод Хі-квадрат є універсальним, так як підходить для аналізу зображень, створених різними програмами приховання. Однак результати роботи методу за критерієм Хі-квадрат в значній мірі залежать від способу приховування даних.

При послідовному запису в НЗБ елементів контейнера метод забезпечує гарні результати (рис. 3.1), а при псевдовипадковому виборі молодших біт і розсіювання повідомлення по всій довжині контейнера метод не спрацьовує [11].

3.2. Різнивний стеганоаналіз на основі подвійої статистики

Одним з оригінальних методів статистичного стеганоаналізу є метод RS, вперше опублікованим у 2001 р. колективом вчених під керівництвом Дж. Фрідріх. Скорочення в назві розшифровується як Regular-Singular, то є "регулярно-сингулярний".

Суть методу складається в наступному. всі зображення розбивається на групи по *n* пікселів *G(x,x2,...,xn)*, де *n* парно, наприклад по 2 пікселя, що знаходяться поряд по горизонталі. Для групи пікселів визначається функція регулярності або «гладкості» *f(G)*, як таку функцію вибрати, наприклад, дисперсію значень усередині групи, або просто суму перепадів значень суміжних пікселів. Під значенням пікселя розуміємо ціле число від 0 до 255:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|, \quad (3.1)$$

Функція *F(x)* називається фліпінгом і має властивість *F(F(x)) = x*. Визначимо дві функції фліпінгу - F_1, відповідає інверсії молодшого біта пікселя, F_{-1} та, що є інверсією з перенесенням у старший біт (додавання одиниці):

$$F_1: \ 0 \leftrightarrow 1,\ 2 \leftrightarrow 3,\ \ldots,\ 254 \leftrightarrow 255,$$
$$F_{-1}: \ 255 \leftrightarrow 0,\ 1 \leftrightarrow 2,\ 3 \leftrightarrow 4,\ \ldots,253 \leftrightarrow 254,\ 255 \leftrightarrow 0, \quad (3.2)$$

При застосуванні фліпінгу до групі отримуємо перетворену групу пікселів. Далі, поділимо всі групи пікселів на класи наступним чином:

Регулярні групи: G R ⇔ f(F(G)) > f(G); (3.3)

Сингулярні групи: G S ⇔ f(F(G)) < f(G); (3.4)

Невикористовувані групи: G U ⇔ f(F(G)) = f(G). (3.5)

Надалі нас цікавитиме співвідношення між групами в зображення. Визначимо кількість груп, що потрапили в той або інший клас як R_M, S_M, U_M і R_{-M}, S_{-M}, U_{-M}, де індекси M та -M означають відповідно застосування F_1 і F_{-1} для отримання розподілу. Наша мета – визначити яким чином використання повідомлення методом LSB буде впливати на вищеописану статистику груп пікселів.

Метод ґрунтується на статистичному припущенні, що для природного зображення, іншими словами, незаповненого контейнера, характерно наступне:

$$R_M \cong R_{-M} \quad S_M \cong S_{-M}, \tag{3.6}$$

Припущення засновано на тому, що застосування дасть розподіл, що і на зображенні, значення пікселів якого зсунуто на одиницю. Для звичайного зображення співвідношення між групами не має суттєво змінюватися. Значна розбіжність між значеннями свідчить о застосуванні LSB-стеганографії для молодших біт зображення.

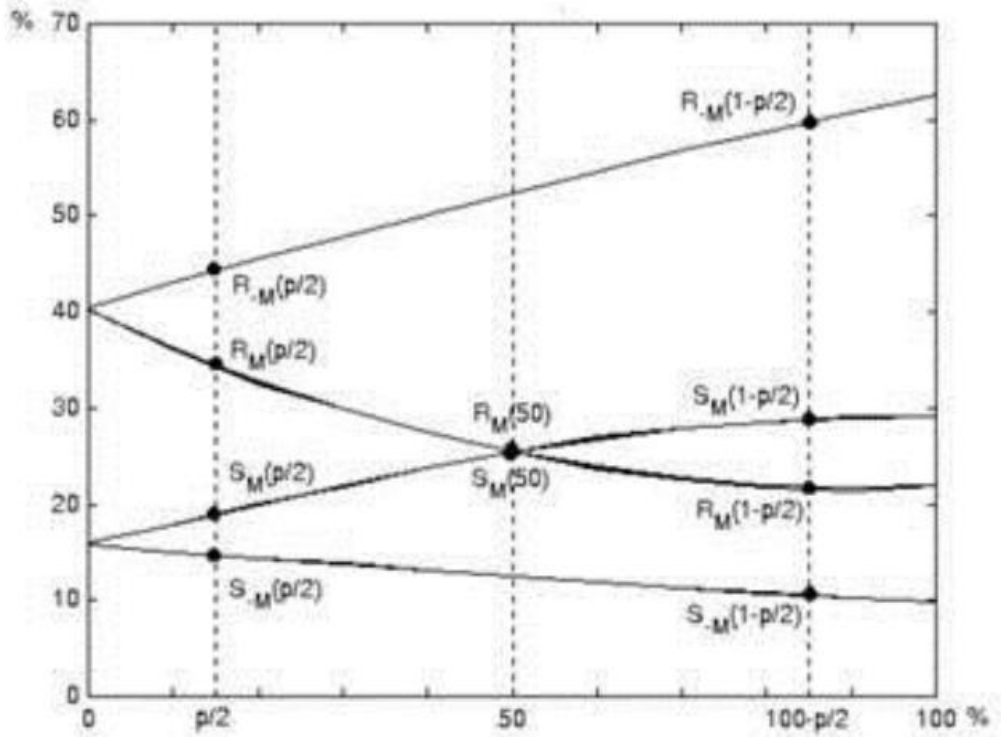

Рис. 3.2. RS-діаграма типового зображення

Розглянемо зміни молодших біт зображення за 100% перезапису їх бітами повідомлення. Впровадження випадкового повідомлення довжиною, рівною розміром зображення, приведе до того, що 50% молодших біт будуть інвертовані. Це, в свою чергу зведе до нулю різницю між значеннями R_M і S_M. Однак на R_{-M} і S_{-M} використання повідомлення буде впливати прямо протилежно, і різниця цих величин буде пропорційна ступеню заповненості контейнера, тобто довжині повідомлення. На рис. 3.2 наведено RS-діаграма для типового зображення. На осі абсцис розташована кількість інвертованих біт *x*, шукана довжина повідомлення *p*, на осі ординат – відносні

значення регулярних та сингулярних груп по відношенню до спільного числп груп зображення [17,21].

3.3. Оцінка стеганографічної ємності бітових площин стеганоконтейнерів для обробки мультимедійних даних в стільникових мережах п'ятого покоління

Одним з важливих завдань стеганографії є вибір відповідного контейнера. Незважаючи на велику кількість досліджень в даній області, вибір контейнера для стеганографічного приховування даних все ще освітлений недостатньою мірою.

Як досліджуваний формат цифрових зображень було обрано формат BMP. Вибір даного формату цифрових зображень був обумовлений тим, що він забезпечує можливість вбудовування більшої кількості даних та не використовує алгоритмів стиснення зображення. Останнє є важливим фактом, так як вбудовування інформації в цифрове зображення відбувається в найменш значний біт, що при використанні зображень з різними алгоритмами стиснення може призвести до втрати або пошкодження вбудованої інформації.

У ході роботи було проаналізовано понад 100 різних зображень формату BMP. Досить часто при виборі відповідного контейнера для стеганографії, зображення поділяють різні групи. Однак ці поділи є досить умовними, тому в ході цієї роботи зображення не піддавалися на поділ по груп. Науковий інтерес представляють лише статистичні властивості досліджуваних зображень. До всіх досліджуваних зображень пред'являлися наступні вимоги:

1. зображення повинні бути вихідним файлом, а не бути отриманими шляхом конвертації інших цифрових форматів зображень в формат BMP;
2. зображення не повинні бути створені з використанням будь-яких графічних редакторів;
3. всі зображення повинні мати однаковий розмір, що виключить вплив розміру зображення на отримані результати.

Вбудовування інформації в досліджувані зображення відбувалося методом LSB, яким є досить популярним методом вбудовування в стеганографії і має на увазі

використання найменш значущі біти зображення. Однією з серйозних помилок в стеганографії є те, що молодші біти зображень є нічим іншим, як шумом. Однак це зовсім не так, між молодшими бітами зображень встановлюються цілком певні залежності, які змінюються при стеганографічному прихованні інформації.

Для визначення цих змін, в роботі використовується метод дослідження статистики розподілу Хі-квадрат і RS-метод стеганографічного аналізу. Таким чином, зображення з найменшим відхиленням даних оцінок між природним та стегаконтейнером буде найкращим з точки зору стеганографічного приховання інформації.

У ході дослідження були вивчені залежності оцінок Хі-квадрат та RS від статистичних властивостей природних зображень-контейнерів, таких як монотонність, ентропія та дисперсія зображення.

3.4. Дослідження статистичних властивостей зображення при вбудовуванні інформації в молодшу бітову площину

Впровадження інформації буде здійснюватися в молодшу бітову площину цифрового зображення засобами LSB методу. Розглянемо залежність зміни статистики Хі – квадрат від монотонності зображення. За монотонність прийматимемо величину, що характеризує відносне відсоткове співвідношення колірних відтінків зображення.

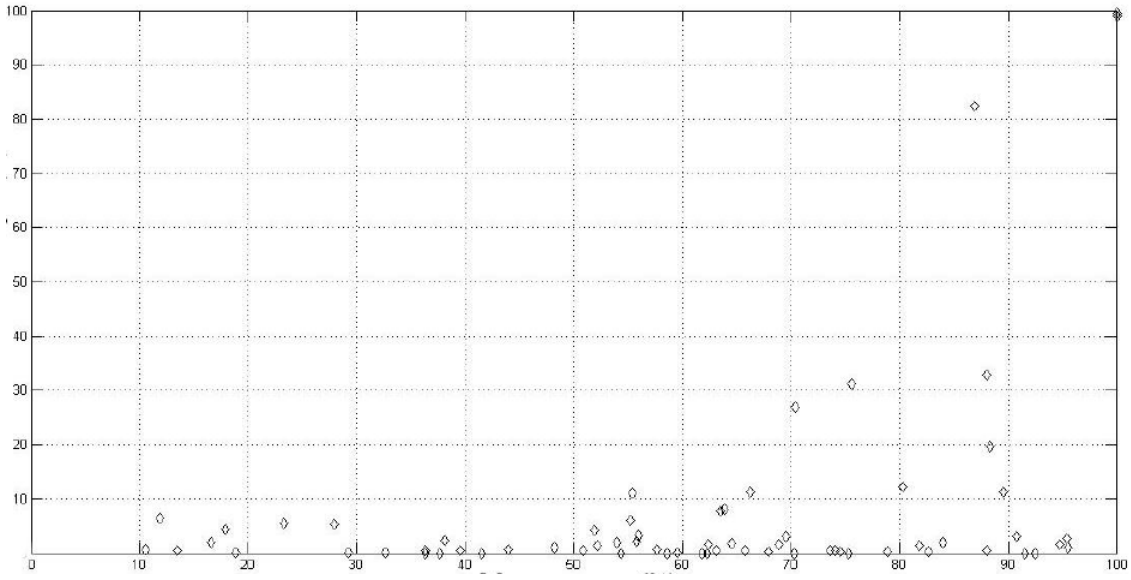

Рис. 3.3. Залежність зміни статистики Хі-квадрат від монотонності зображення

На основі графіка (рис. 3.3) можна зробити висновок, що найбільш підходящими зображеннями в якості стегоконтейнера є зображення, що володіють найменшою монотонністю. Максимальна зміна статистики Хі-квадрат (100%) знаходиться в точці, де монотонність зображення досягає 100%. Таким чином, аналізуючи таку характеристику як "монотонність" зображення, зображення містять більшу кількість областей монотонної заливки, є менше кращими в якості стегоконтейнера і забезпечують погану скритність вбудованого повідомлення.

Однак, однієї Характеристики зображення недостатньо, щоб визначити найбільш придатні при виборі зображень в якості контейнера. Важливими статистичним характеристиками цифрового зображення є ентропія та дисперсія.

Залежність зміни Хі-квадрат від ентропії в молодшій бітовій площині зображення представлені на рис. 3.4.

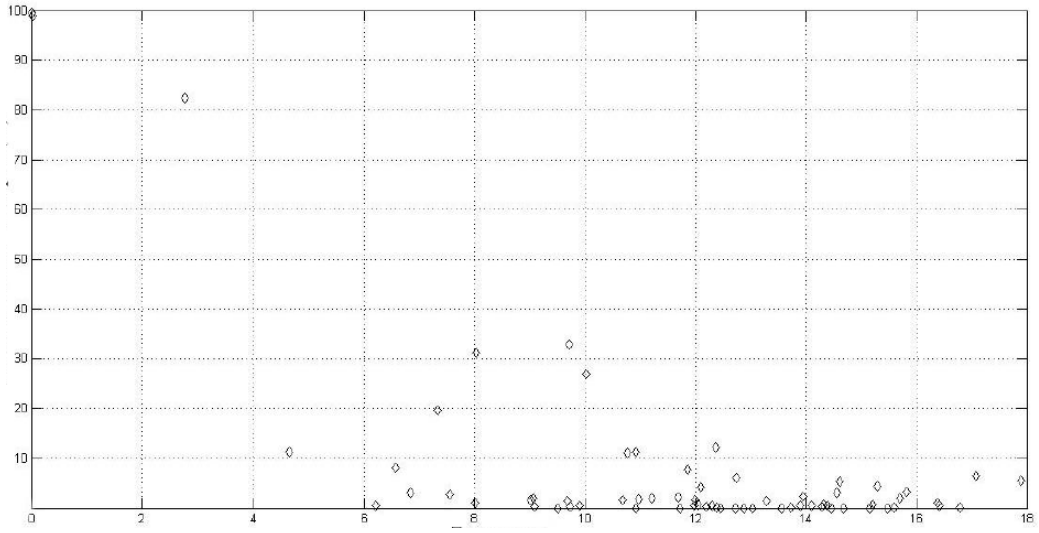

Рис. 3.4. Залежність зміни Хі-квадрат від ентропії молодшій бітовій площині

На графіку помітно, що зміна Хі-квадрат зменшується з збільшенням ентропії досліджуваних зображень. Виходячи з цього можна зробити висновок, що критерій Хі-квадрат природного зображення і зображення, що містить стего, ближче у тих зображень, ентропія яких вище. Так як ентропія цифрового зображення характеризує величини яскравих варіацій зображення, то система, використовуюча в якості контейнера строкаті зображення з великою кількістю дрібних деталей, забезпечує велику надійність.

Для визначення розкиду значень молодших біт використовується математична величина - дисперсія. Недоліком методу визначення дисперсії є чутливість до розмірів зображення. Сусідні пікселі двох однакових зображень з різним дозволом відрізняються кількістю пікселів, які припадають однакові фрагменти зображення. Чим менший розмір зображення, тим більше відрізнятимуться два сусідні пікселя, ніж у такого зображення більшого розміру. Саме тому в цій роботі було прийнято використовувати зображення однакового розміру. На рис. 3.5 представлена залежність зміни Хі-квадрат та дисперсії зображення.

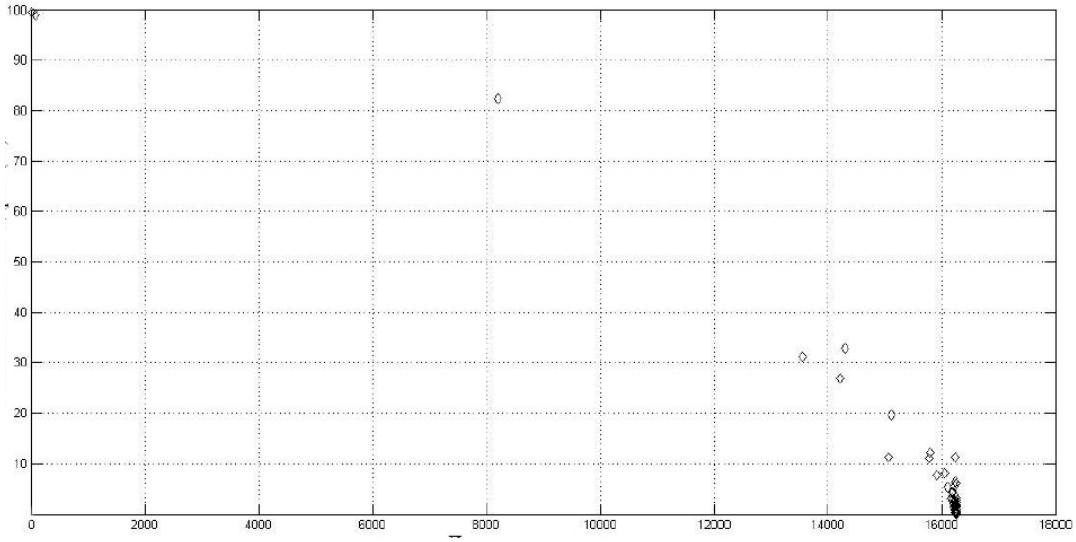

Рис. 3.5. Залежність зміни Хі-квадрат від дисперсії молодшій бітовій площині

Результати аналізу залежності зміни (рисунок 3.5) Хі-квадрат від дисперсії зображення показують, що з збільшенням дисперсії зображення, різниця Хі-квадрат природного контейнера і контейнера, що містить стего, зменшується. Таким чином, зображення, що володіють більшою дисперсією в молодшій бітовий площині, є найбільш підходящими в якості контейнера для вбудовування секретної інформації.

Підбиваючи підсумки стеганографічної атаки на основі критерію Хі-квадрат, можна помітити, що найбільш підходящими в якості стегоконтейнера є зображення, що володіють меншою монотонністю і великими ентропією і дисперсією.

Розглянемо залежності RS – стеганоаналіз від статистичних властивостей зображень, представлених вище, тобто. монотонності, ентропії і дисперсії. Як вже було

помічено раніше RS - стеганоаналіз є досить ефективним методом для виявлення стеганографічного приховання інформації в цифрових зображеннях.

На рис. 3.6 і рис. 3.7 представлені залежності змін регулярних і сингулярних груп від монотонності зображень.

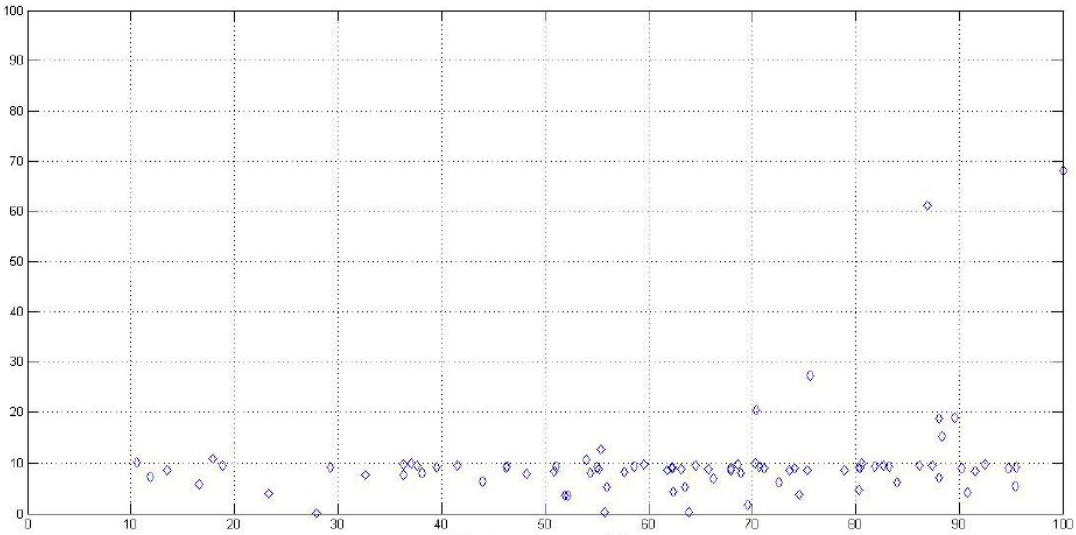

Рис. 3.6. Залежність зміни відсоткового співвідношення регулярних груп від монотонності

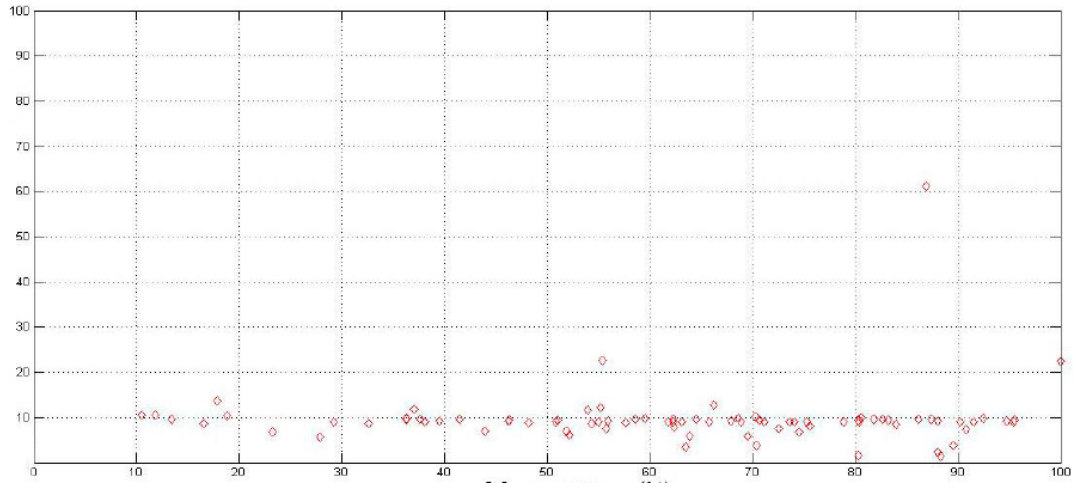

Рис. 3.7. Залежність зміни відсоткового співвідношення сингулярних груп від монотонності

Аналіз залежностей рис. 3.6 і рис. 3.7 показує, що RS- метод є менш чутливим до монотонності зображення, тому дана характеристика зображення не є об'єктивною в випадку застосування RS-методу при виборі стегоконтейнера.

Звернемося до ентропії зображення і проаналізуємо поведінку методу в даному випадку. Аналіз отриманих результатів показує, що, як і в випадку з методом аналізу, заснованого на критерії Хі-квадрат, найбільш підходящими зображеннями в якості стегоконтейнера, є зображення, що володіють більшою ентропією. Зміна регулярних і сингулярних груп природних та стего-контейнерів менше у зображень з більшою ентропією в молодшій бітовій площині рис. 3.8 і 3.9.

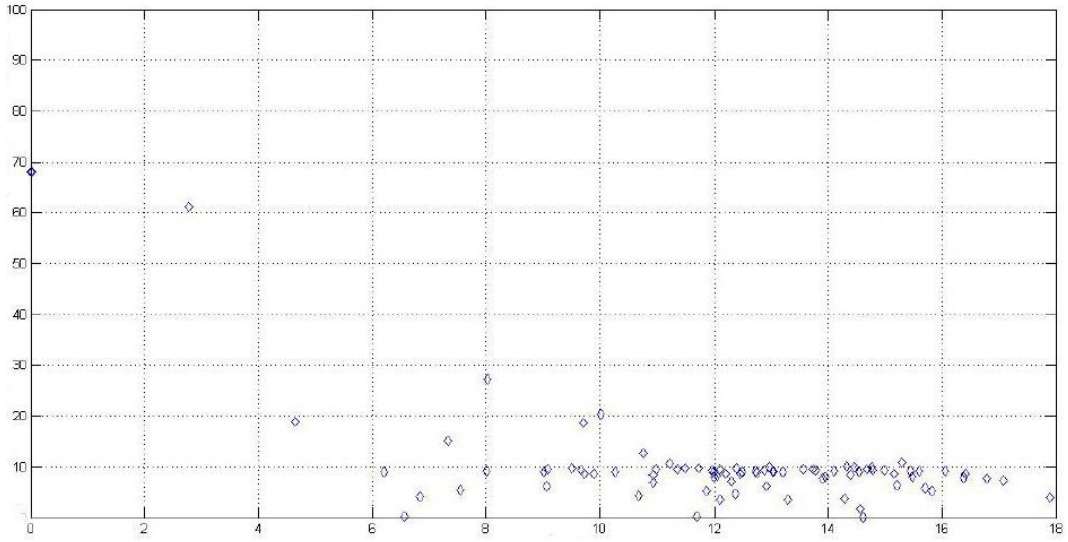

Рис. 3.8. Залежність зміни відсоткового співвідношення регулярних груп від ентропії молодшої бітової площини

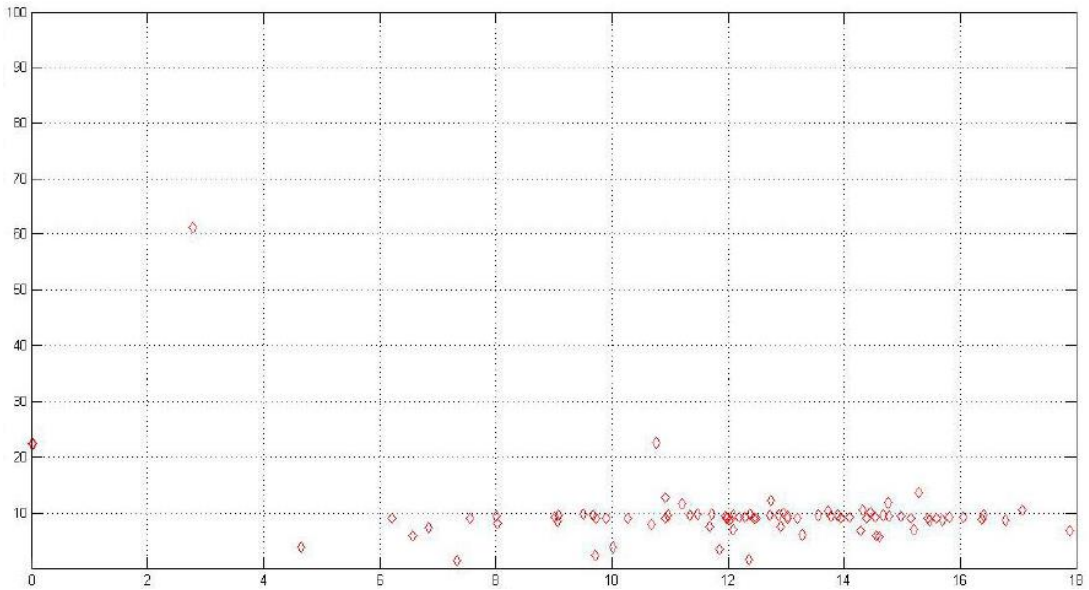

Рис. 3.9. Залежність зміни відсоткового співвідношення сингулярних груп від ентропії молодшій бітовий площині

Аналіз залежності RS - стегоаналізу від дисперсії зображення (Рисунок 3.10 та 3.11) також показав, що, як і у методі аналізу на основі критерію Хі-квадрат, зображення з більшою дисперсією найбільш придатні в як контейнер для методу LSB.

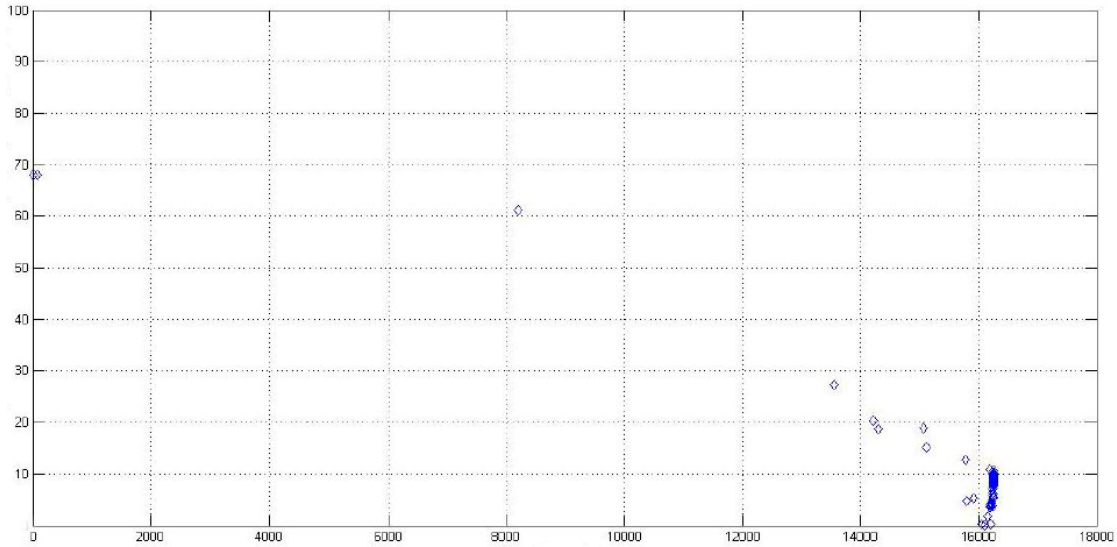

Рис. 3.10. Залежність зміни відсоткового співвідношення регулярних груп від дисперсії молодшої бітової площини

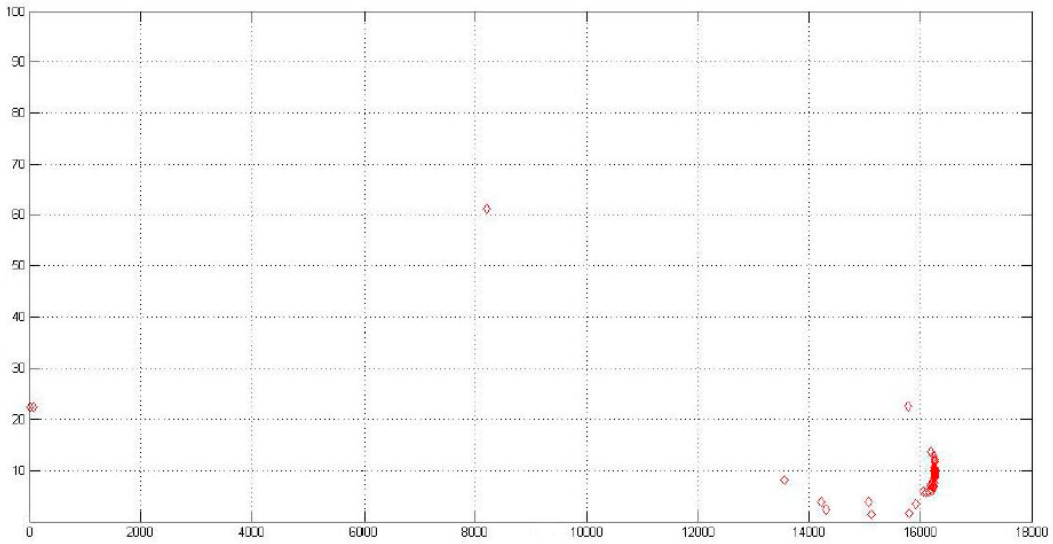

Рис. 3.11. Залежність зміни відсоткового співвідношення сингулярних груп від дисперсії молодшої бітової площини

3.5. Дослідження статистичних властивостей цифрових зображень при вбудовуванні інформації у другу бітову площину

Одним з суттєвих недоліків методу LSB є невелика кількість інформації, що можливо вбудувати в випадку використання виключно найменш значущих біт цифрового зображення. Таким чином, встає необхідність вивчення можливості залучення найбільш значущих біт зображення для вбудовування інформації. Розглянемо результати вбудовування повідомлення в другі біти зображення. на рис. 3.12 показано залежність зміни критерію Хі-квадрат від дисперсії зображення.

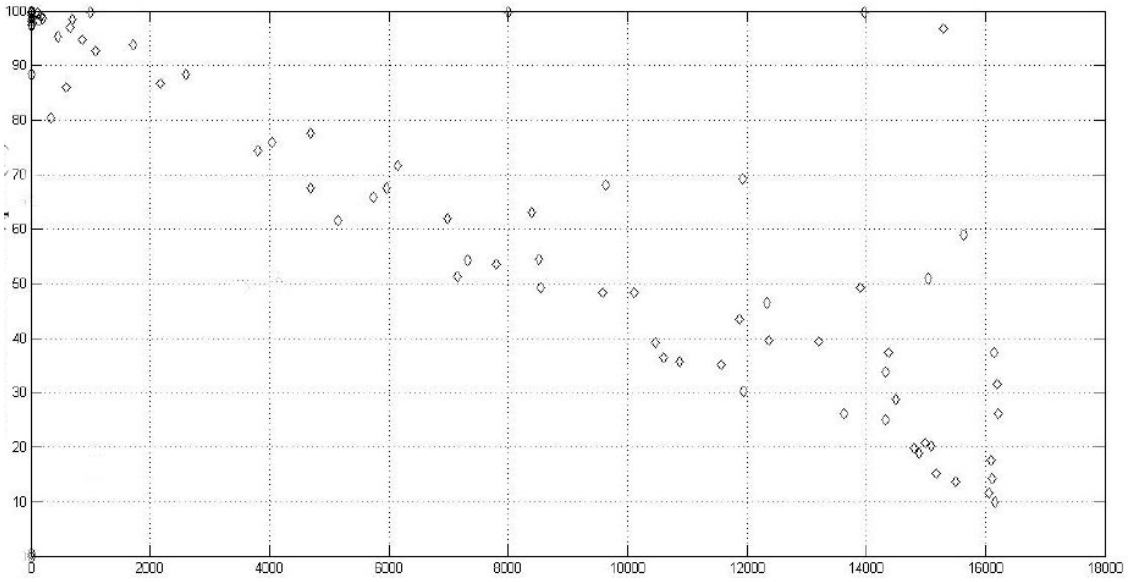

Рис. 3.12. Залежність зміни Хі-квадрат від дисперсії у другій бітовій площині

Виходячи з отриманих даних, можна зробити висновок, що зі збільшенням дисперсії у другій бітовій площині зміна показника Хі-квадрат зменшується. Однак, аналізуючи значення дисперсії у другій бітовий площині, можна помітити, що розкид значень дисперсії збільшується порівняно з молодшою бітовою площиною. На рисунках 3.13 та 3.14 показані результати роботи методу регулярних - сингулярних груп. Результати є схожими з результатами роботи методу Хі-квадрат, і показують, що найбільш підходящими зображеннями як контейнер є зображення, що мають найбільше значення дисперсії другої бітової площини зображення.

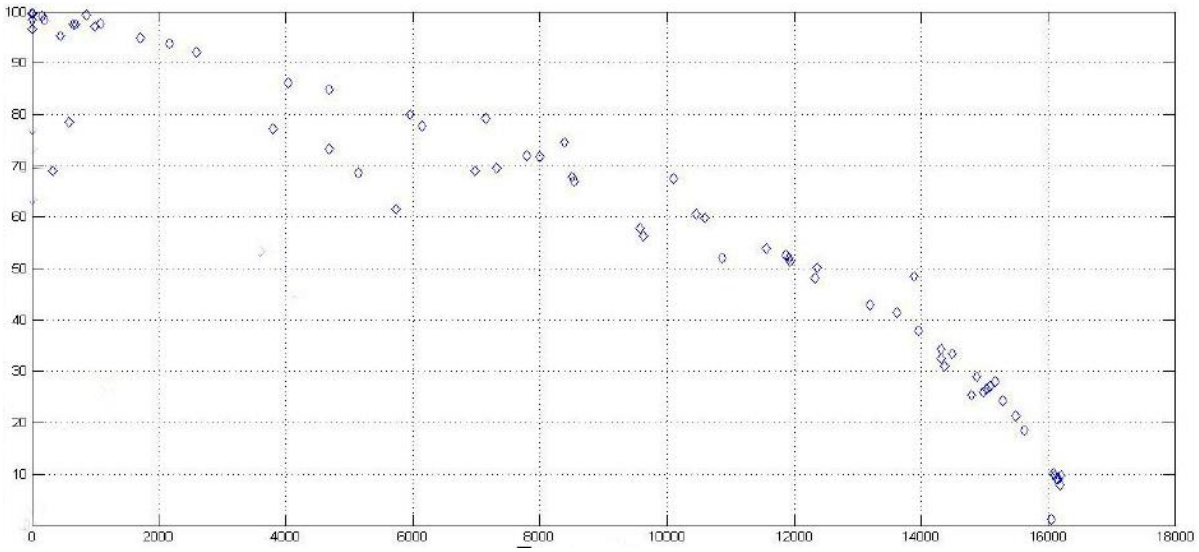

Рис. 3.13. Залежність зміни відсоткового співвідношення регулярних груп від дисперсії у другій бітовій площині

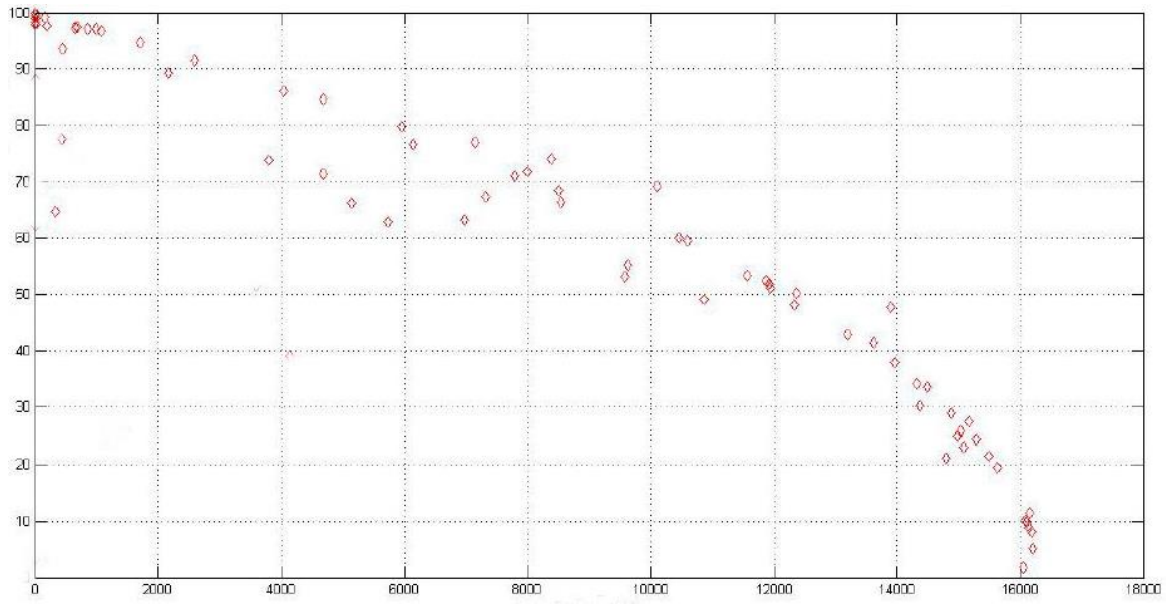

Рис. 3.14. Залежність зміни процентного співвідношення сингулярних груп від дисперсії у другій бітовій площині

Розглянемо результати роботи методу Xi - квадрат і RS методу щодо ентропії зображення. На рис. 3.15 представлено залежність зміни Xi - Квадрат від ентропії.

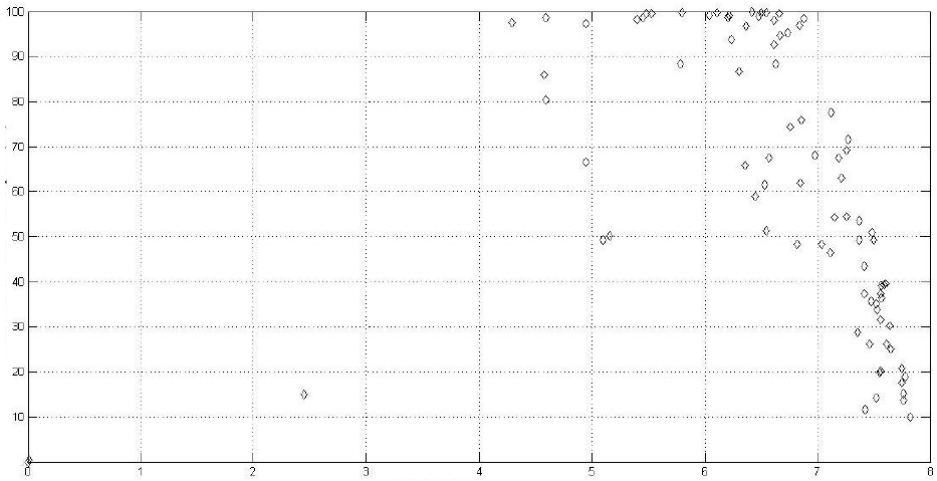

Рис. 3.15. Залежність зміни критерію Хі - квадрат від ентропії у другій бітовій площині

Також, як і в випадку вбудовування в найменш значущі біти зображення, при вбудовуванні в другу бітову площину найбільшою стійкістю до статистичного методом аналізу Хі - квадрат мають зображення з великим значенням ентропії у другій бітовій площині. Як можна помітити, чисельне значення ентропії у другій бітовій площині робить другі біти привабливими для вбудовування у порівнянні з молодшими бітами.

RS метод стеганоаналізу щодо ентропії цифрового зображення показує схожі результати: найбільшою стеганографічною стійкістю володіють зображення з великим значенням ентропії у другій бітовій площині (рис. 3.16 і 3.17).

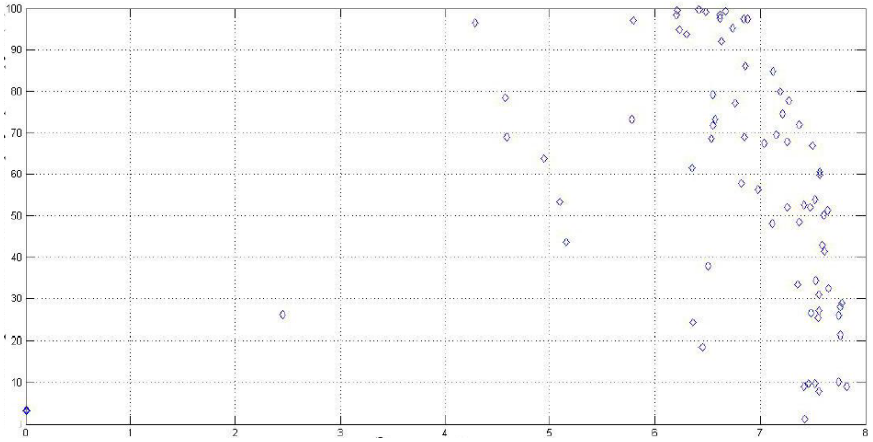

Рис. 3.16. Залежність зміни відсоткового співвідношення регулярних груп від ентропії у другій бітовій площині

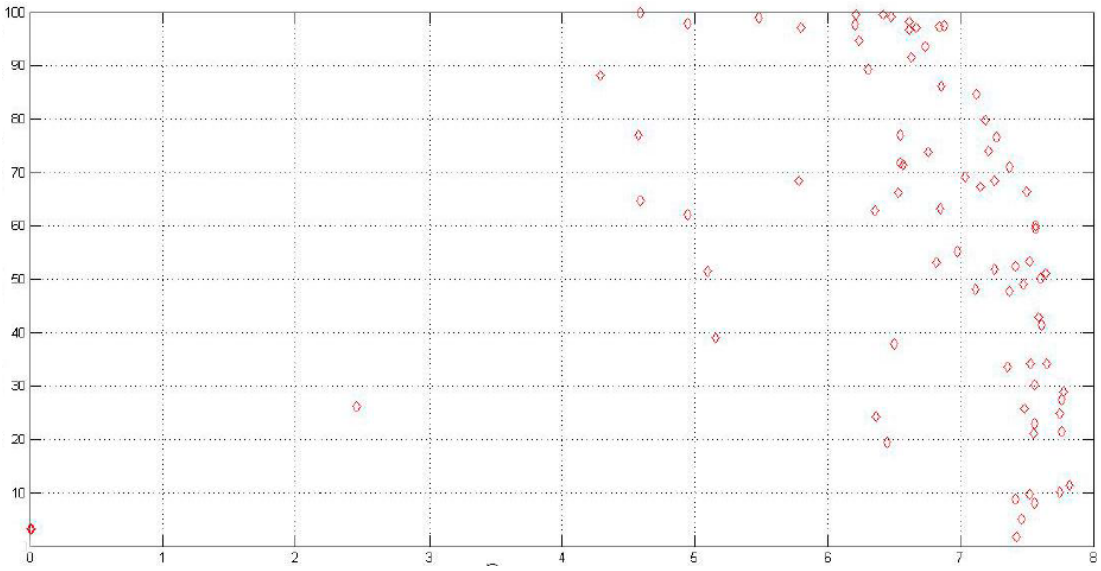

Рис. 3.17. Залежність зміни сингулярної групи від ентропії у другій бітовій площині

Таким чином, в випадку необхідності залучення других біт цифрового зображення для вбудовування стеганографічного повідомлення, необхідно віддавати вподобання зображенням, що володіють більшою дисперсією та ентропією у другій бітовій площині.

ВИСНОВОК ДО РОЗДІЛУ 3

Наведені найбільш точні та широко поширені методи стеганографічного аналізу факту приховування даних в просторових областях цифрових зображень, засновані на дослідженні статистичних властивостей контейнерів. Наведені методи аналізу відносяться до категорії методів на основі відомої математичної моделі цифрових зображень.

Методу аналізу на основі Хі-квадрат є універсальним методом стеганографічного аналізу і заснований на порівнянні частот сусідніх елементів зображення. Даний метод показує гарні результати при використанні послідовного вбудовування інформації в елементи контейнера. Однак істотним недоліком даного методу є те, що при псевдовипадковому вбудовуванні даних метод не може бути застосовано.

Метод RS є достатньо новим методом стеганоаналізу, заснованому на аналізі співвідношення між групами в цифровому зображенні. Даний метод дозволяє уникнути недоліків, властивих методу аналізу на основі Хі-квадрат, так як він не залежить від методу вбудовування інформації в просторові області зображень.

Надалі дані методи можуть бути використані в ході наукової роботи для дослідження можливості вбудовування інформації в бітові області зображень в якості критерію стеганографічної стійкості системи.

Були досліджено статистичні Характеристики цифрових зображень, що дозволяють вибрати найбільш підходяще зображення в якості стеганографічного контейнера для вбудовування інформації в її різні бітові площини.

Таким чином, виходячи з отриманих даних при виборі контейнерів для LSB стеганографії слід віддавати вподобання зображенням з найбільшими значеннями ентропії та дисперсії у бітових площинах. При рівних значеннях ентропії і дисперсії в молодших бітових площинах, необхідно аналізувати більш старші біти зображення, де також слід вибирати зображення з великими значеннями ентропії та дисперсії. Аналіз необхідно продовжувати до того моменту, як обране зображення буде в достатньому ступені задовольняти вимогам, пред'явленим до стеганографічної системи.

РОЗДІЛ 4
ІНТЕГРАЦІЯ СИСТЕМ ВІДДАЛЕНОГО ЗБЕРІГАННЯ ТА ОБРОБКИ ДАНИХ

4.1. Подальший розвиток мереж наступного покоління

З урахуванням тимчасових термінів, встановлених союзом ITU в рамках ініціативи IMT-2020, стандартизація мереж 5G зараз наближається до свого завершення. У цьому зв'язку регулярні семінари RAN 5G, організовані комітетом 3GPP, присвячені розробці технологій радіодоступу наступного покоління, що включає подальшу еволюцію системи LTE і нову технологію NR (New Radio), які покликані спільно задовольнити численним вимогам IMT-2020. Оскільки перспективна система NR являє собою нову радіотехнологію без можливості зворотної сумісності з наявними (наприклад, LTE), стає зрозуміло, що мережі 5G об'єднають кілька різних технологій і систем. Ця особливість дозволить мобільним операторам розгортати гнучкіші мережеві рішення, придатні для потреб певних додатків та послуг мобільного зв'язку [22].

Для цих цілей системи 5G визначають нову концепцію мережевої «нарізки» (Network Slicing), яка надасть виділені варіанти обслуговування окремих сервісів у рамках єдиної мережі, на відміну від наявних підходів з розміщенням окремих мереж для різних цілей. Такі відносно-незалежні мережеві рівні дозволять їх додаткам гарантувати цільову швидкість передачі даних та затримку, а також підвищити ефективність використання спектральних радіоресурсів. За допомогою динамічно-створюваних та безпечних мережевих рівнів гетерогенні системи 5G надаватимуть необхідну якість обслуговування своїм численним додаткам та послугам. Після відповіді на важливі питання щодо застосування цієї концепції, включаючи «Яким чином здійснювати мережеву нарізку» та «З якою гранулярністю», оператори зможуть використовувати її у своїх системах, доповнюючи нею існуючі технології управління, такі як мережі SDN і віртуалізація мережевих функцій. NFV [23].

Зокрема, технологія SDN є досить відомою (сходить до 1990-х років) і дозволяє

динамічно підключати та конфігурувати різні мережеві компоненти. Однак тільки зараз завдяки достатнім обчислювальним потужностям це рішення починає з успіхом використовуватися на практиці. При цьому технологія NFV будується на основі широко поширених серверів та комутаторів, а також хмарних систем зберігання та обробки інформації, які дозволяють здійснити перехід до хмарних сервісів за допомогою віртуалізації всіляких функцій мережевих вузлів. З урахуванням додаткових ступенів свободи, що надаються системами SDN і NFV, майбутні оператори мереж 5G матимуть можливість швидко розгортати нові послуги, а також переміщати їх як віртуальні машини у відповідь на динамічні зміни потреби своїх користувачів.

Спираючись на технології SDN та мережеві «нарізки» NFV , можливо об'єднати передачу даних і їх обробку в рамках екосистеми 5G, що швидко розвивається, яку характеризують як «обчислювальні технології для потреб засобів зв'язку». Даний підхід будується на взаємодії засобів передачі та обробки інформації, дозволяючи ефективно організувати віддалені обчислення по бездротовому каналу зв'язку. Таке вивантаження функцій з обробки даних у системах 5G дозволяє їм обслуговувати пристрої з обмеженими обчислювальними можливостями та енергетичними ресурсами. Подібне обладнання тепер має можливість переводити свої обчислювально-складні завдання до ресурсомістких серверів. Таким чином, відбувається фундаментальна зміна принципів мережевої взаємодії, яка зміщує фокус з бездротових з'єднань у бік переданого контенту і дозволяє зосередитися безпосередньо на його розподілі, зберіганні та отриманні на відміну від мережевої архітектури, що історично склалася, орієнтованої виключно на підвищення ємності системи зв'язку.

Однак збільшені потреби перспективних мережевих додатків щодо доступної смуги пропускання, змушують мобільних операторів спішно нарощувати ємність наявних стільникових покриттів. Для цих цілей гетерогенні мережі зарекомендували себе як ефективне і надійне рішення, що спирається на макростільники для забезпечення безшовного покриття і здійснення функцій управління мережею, а також на різні малі стільники різних радіотехнологій і розмірів в областях з високим завантаженням. При цьому сучасні гетерогенні мережі дозволяють мобільним операторам розміщувати стільникову інфраструктуру ближче до абонентських терміналів, які є

безпосередніми виробниками та споживачами контенту, стаючи цим ефективним засобом ущільнення мережі, особливо в міських умовах.

У міру того, як надщільні покриття малими стільниками дозволяють підвищити спектральну ефективність і ємність мережі радіодоступу, вони водночас створюють підвищене навантаження на транзитні (Backhaul) канали. Для більшості операторів мобільного зв'язку розміщення високошвидкісних транзитних каналів між безліччю БС малих сот і опорною мережею стає економічно недоцільним. Для запобігання заторам в умовах обмеженої ємності транзитних каналів, особливо в періоди пікового завантаження, використовується кешування даних на БС, що дозволяє надавати контент користувача локально, без використання транзитних з'єднань. Нещодавно безліч досліджень показало, що застосування механізмів кешування дійсно є ефективним рішенням для зниження навантаження на транзитні канали. При цьому часто затребувані дані розміщуються на кешуючих БС в спокійні періоди, а потім завантажуються в пік розташованими поблизу користувачами.

Відповідно, на сьогоднішній день є ряд альтернативних варіантів побудови архітектури кешируючої мережі, які по-різному інтерпретують інформацію щодо ступеня затребуваності контенту та дозволяють зняти обмеження на ємність транзитних каналів за рахунок використання додаткової пам'яті. У результаті системи 5G можуть застосовувати БС малих сот з високою ємністю кеша для зберігання найбільш популярного контенту і низькошвидкісними транзитними з'єднаннями, які служать в основному для оновлення закешированного контенту зі швидкістю, пропорційною до зміни загальної потреби в ньому з боку абонентів. З урахуванням недавнього прогресу у виробництві модулів пам'яті, таке «прозоре» кешування на стратегічно важливих ділянках мережі дозволяє підвищити ефективність розподілу контенту, а також збільшити ефективність використання радіоресурсів системи, навіть коли користувачі не вимагають деяку одиницю контенту одночасно (тобто використовувати мінливість мережевого трафіку у часі).

4.2. Перспективні користувацькі додатки та послуги у 5G

Еволюція способів одержання відеоконтенту. У міру того, як абоненти застосовують все більш багатофункціональні смартфони та планшети, ці інтелектуальні пристрої стають невід'ємною частиною повсякденного розпорядку своїх користувачів. На сьогоднішній день використання смартфонів вже перевищує за популярністю використання комп'ютерів при доступі до Інтернету. Дійсно, типовою картиною минулого століття було читання газети пасажирами громадського транспорту, тоді як сьогодні це заняття змінилося переглядом новин онлайн за допомогою різноманітних мобільних пристроїв. Після переходу новин в електронний вигляд змінюються бізнес-моделі, пов'язані з розподілом контенту, дозволяючи йому публікуватися швидше й частіше містити мультимедіадані. Це, у свою чергу, створює повторні запити на завантаження популярного контенту, такого як термінові новини та лідери відеопрокату, що призводить до надзвичайно-надмірної передачі інформації, що повторюється.

Читання гарячих новин з мобільних терміналів є лише одним із безлічі прикладів того, як люди демонструють схожість інтересів в отриманні контенту за географічним принципом. Іншим прикладом може стати масове завантаження нової версії операційної системи iOS, яке породжує один із найзначніших піків завантаження, відомих мережі Інтернет. Крім використання мобільних пристроїв для доступу до мультимедіаконтенту та колективного завантаження популярних файлів, сьогоднішній Інтернет-трафік демонструє колосальне зростання частки відео, що отримується на запит. Глобальні постачальники подібних послуг, такі як YouTube та Netflix, вже налічують багатомільйонну аудиторію та фактично є законодавцями нового напряму у споживанні відеоінформації. Наприклад, Netflix, будучи світовим лідером на ринку відео на запит, що надається за підпискою, налічував більше 90 мільйонів абонентів ще в середині 2017 року, і очікується, що їх кількість подвоїться до кінця 2023 року [24].

Однак на відміну від передачі потокових мультимедіаданих, при отриманні відео на запит користувачі не завантажують один і той же контент одночасно. Ця важлива властивість, відома як асинхронне перевикористання контенту, призводить до

того, що невелика кількість популярних одиниць контенту становить переважну більшість трафіку, що фактично передається. Існують практичні свідчення, що типові запити з боку користувача концентруються на порівняно невеликому наборі файлів. Більше того, завантаження відео за запитом у високій мірі надмірно в часі і просторі, що призводить до необхідності більш глибокого дослідження статистичних властивостей даних, які запитуються, а також структури користувачів запитів, що змінилася. Нещодавні дослідження підтверджують, що сучасні стільникові технології все ще не в змозі надати безшовну, ефективну і масштабовану передачу відео на запит, оскільки архітектура мережі Інтернет базується на моделі розподілу контенту, що історично склалася, має ряд обмежень, які розглядатимуться далі.

Існуючі обмеження при доставці контенту. В існуючих стільникових мережах мобільні термінали, що розташовуються на краю стільники, відчувають підвищене енергоспоживання через високу потужність передачі, а також мають суттєву затримку при доступі до цільового контенту через бездротові з'єднання. При цьому відомо, що люди особливо чутливі до величини затримки доступу та її коливань. Найбільші постачальники цифрової інформації на сучасному ринку, такі як Google і Akamai, що будували багатомільярдний бізнес навколо своїх систем розподілу контенту, відзначають, що низька затримка є ключовим інгредієнтом успіху при задоволенні потреб користувачів. Приклади з життя підтверджують, що вже незначне зростання затримки доступу може значно знизити якість сприйняття роботи тієї чи іншої програми або послуги в мережі Інтернет.

Для підвищення якості сприйняття користувачів можна застосовувати кешування часто затребуваного контенту на краю мережі (тобто на БС малих сот), знижуючи тим самим розрив між доступною та необхідною ємністю доступу. При цьому, відповідаючи на ключові питання щодо того, що і де вигідніше кешувати, важливо враховувати непередбачувану мобільність користувачів, яка стає важливим фактором, що ускладнює, особливо з урахуванням зростання популярності мобільних пристроїв при доступі до контенту. Окрім дослідження характеристик такої мобільності, інформація про місцезнаходження абонентів стає важливою для їх ефективного об-

слуговування в масових сценаріях: пасажири з мобільними терміналами у громадському транспорті, скупчення людей у торгових центрах, на стадіонах, в аеропортах тощо. У результаті важливо враховувати безліч практичних особливостей доступу до контенту при організації ефективного процесу кешування, таких як розподіл популярності даних, місцезнаходження, швидкість та напрямок руху користувачів. Це дозволить підвищити якість обслуговування у сценаріях, які потребують обробки значних обсягів інформації.

На сьогоднішній день існує широкий спектр різноманітних додатків, які вимагають суттєвих обчислень, а також безперервної обробки інформації, яку вони отримують. Прикладами є системи навігації автомобілів, маніпуляція даними в електронних іграх, обробка відео в смартфонах, розпізнавання об'єктів рухомими роботами, синтез мови, обробка природних мов і обчислення на пристроях, що носяться. Однак розвиток подібних перспективних додатків та послуг 5G лімітований обчислювальною потужністю сучасного обладнання користувача, яка не може зростати необмежено в силу фундаментальних стримувальних факторів, наприклад, розмірів та ємності акумуляторної батареї. Як наслідок, ці нові обчислювально-ємні послуги неминуче вимагатимуть створення просунутих механізмів для підтримки віддалених обчислень, які має надавати майбутня архітектура 5G [27-30].

Типові класи додатків та послуг у мережах 5G. Особливо важливим сценарієм у контексті розвитку мереж 5G стає використання доповненої реальності, що дозволяє досягти справді інтерактивного сприйняття послуг. На відміну від віртуальної реальності, доповнена реальність спрямована на модифікацію об'єктів та явищ навколишнього світу, ніж їх відтворення у штучному середовищі. У зв'язку з цим предмети індивідуального оточення користувача стають як тлом, так і сутністю контекстного анотування за допомогою комп'ютерно-генерованої інформації, що потребує складних обчислень у реальному масштабі часу. У світлі трансформації засобів розподілу цифрового контенту, що породжує міріади обчислювально-ємних і чутливих до затримки додатків і послуг, далі пропонується розрізняти два широкі класи сервісів за способом породження потоку даних: користувачем або навколишньою мережевою інфраструктурою.

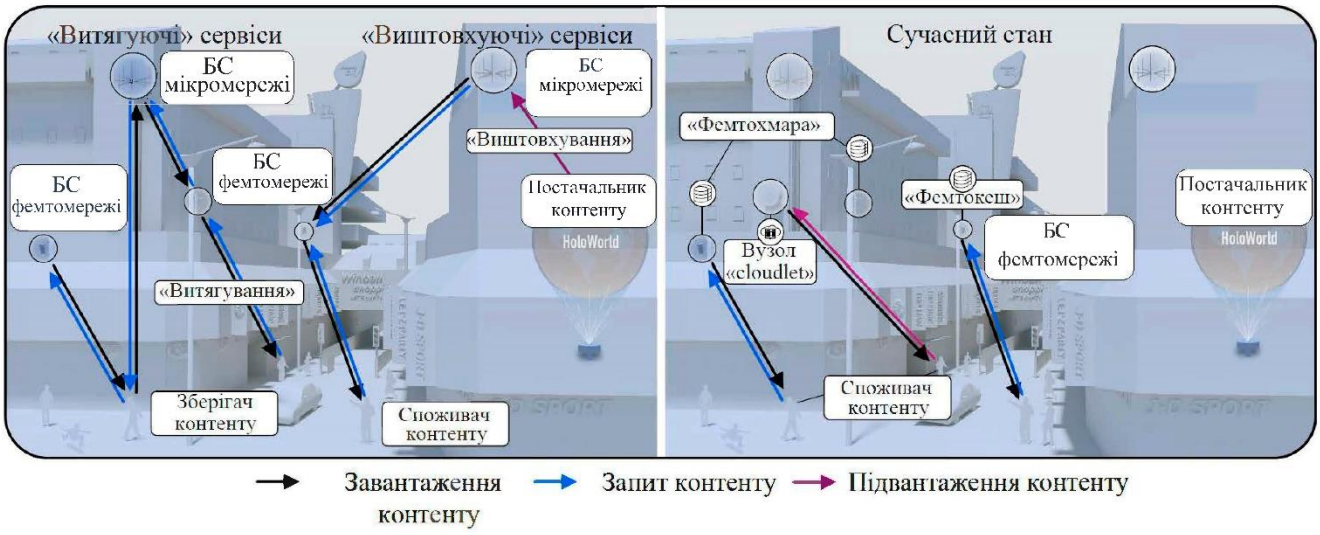

Рис. 4.1. Приклади використання перспективних сервісів 5G

«Витягуючі» сервіси Ця категорія включає послуги, ініційовані користувачем (див. малюнок 5.19), такі як обробка мультимедіаданих для цілей роботи або відпочинку. Відповідні програми варіюються від створення та редагування аматорського мультимедіа-контенту в соціальних мережах до обслуговування потреб абонентів «без робочого місця», дозволяючи професіоналам працювати «з вільними руками» (наприклад, у медицині, на виробництві, в обслуговуванні тощо) . Спільним для всіх подібних сценаріїв є «витягування» необхідного функціоналу з навколишньої мережної інфраструктури деяким користувачем або їхньою групою на вимогу (аналогічно тому, що дозволяє здійснювати рішення PlanGrid для інженерів-будівельників).

«Виштовхуючі» сервіси. До цієї категорії входять сервіси, що ініціюються мережевою інфраструктурою (див. малюнок 5.19), що включає послуги з урахуванням розташування абонентів, «вірусну» рекламу, моніторинг небезпечного навколишнього середовища, контекстну обробку даних та мобільні додатки доповненої реальності. Відповідні сценарії варіюються від нав'язування користувачеві контекстних новин та інформаційних послуг до надання можливості розпізнавання об'єктів у реальному масштабі часу та візуалізації цифрової інформації (у таких галузях, як ігри, розваги та новини, комунальні послуги, освіта, професійна орієнтація тощо). Такі сценарії, як правило, припускають, що мережева інфраструктура заздалегідь «виштовхує» деякий контент на своїх абонентів, маючи уявлення про їхні інтереси чи потреби.

Далі пропонується огляд перспективних технологій для забезпечення описаних вище сценаріїв 5G.

4.3. Еволюція архітектури систем зв'язку 5G

Інтеграція обчислювальної та мережевої інфраструктур. В останні роки хмарні обчислення стали широко поширені як тимчасова обчислювальна інфраструктура, яка дозволяє ефективно проводити віддалену обробку інформації. Грунтуючись на віртуалізації обчислювально-ємної обробки даних, хмарні системи дозволяють використовувати безліч операційних систем та додатків у рамках єдиної платформи, гарантуючи при цьому ізоляцію та захист як програм, так і даних. Такий підхід став важливим засобом, що дозволяє перевести обчислювально-ємні користувацькі додатки в більш ресурсомісткий хмарний простір і тим самим досягти вражаючого економічного успіху. На сьогоднішній день постачальники хмарних послуг пропонують своїм користувачам функціонал для еластичного використання системи на вимогу, включаючи ресурси самої інфраструктури, хмарних платформ та відповідного програмного забезпечення.

Застосування хмарних обчислень у мобільних сценаріях призвело до виникнення мобільних хмарних обчислень, що дозволило подолати безліч практичних обмежень щодо продуктивності, оточення та безпеки. Однак основним стримуючим фактором на шляху сучасних систем мобільних хмарних обчислень стає висока наскрізна затримка під час передачі інформації, включаючи компоненти, пов'язані з доступом, транспортуванням та обслуговуванням даних. У зв'язку з цим поточна архітектура мереж доступу може накласти значне запізнення, а також обмежити пропускну здатність з'єднання через правила використання спектральних радіоресурсів. У результаті постачальники хмарних послуг зацікавлені у створенні ефективних у плані витрат засобів масштабування смуги пропускання, доступної для користувачів.

Для покращення характеристик роботи своїх мереж доступу, особливо при обслуговуванні портативних і пристроїв, що носяться, оператори мобільного зв'язку

вживають конкретних заходів, розглянутих вище. При цьому бурхливий розвиток технологій радіодоступу в епоху 5G призводить до ситуації, коли з'єднання

«останньої милі» мають більш високі параметри продуктивності, ніж відповідна опорна інфраструктура Інтернету. У результаті мобільні оператори можуть відчувати різку нестачу ємності транзитних каналів (тип розміщення I на малюнку 5.20), і передача даних до мережі Інтернет і назад через їх інфраструктуру може зайняти суттєвий час. Більш ефективною, але витратною стратегією є нарощування ємності транзитних каналів нарівні зі з'єднаннями мережі доступу, що дозволяє підтримати вищі швидкості передачі даних та знизити завантаження (тип розміщення II на малюнку 5.20).

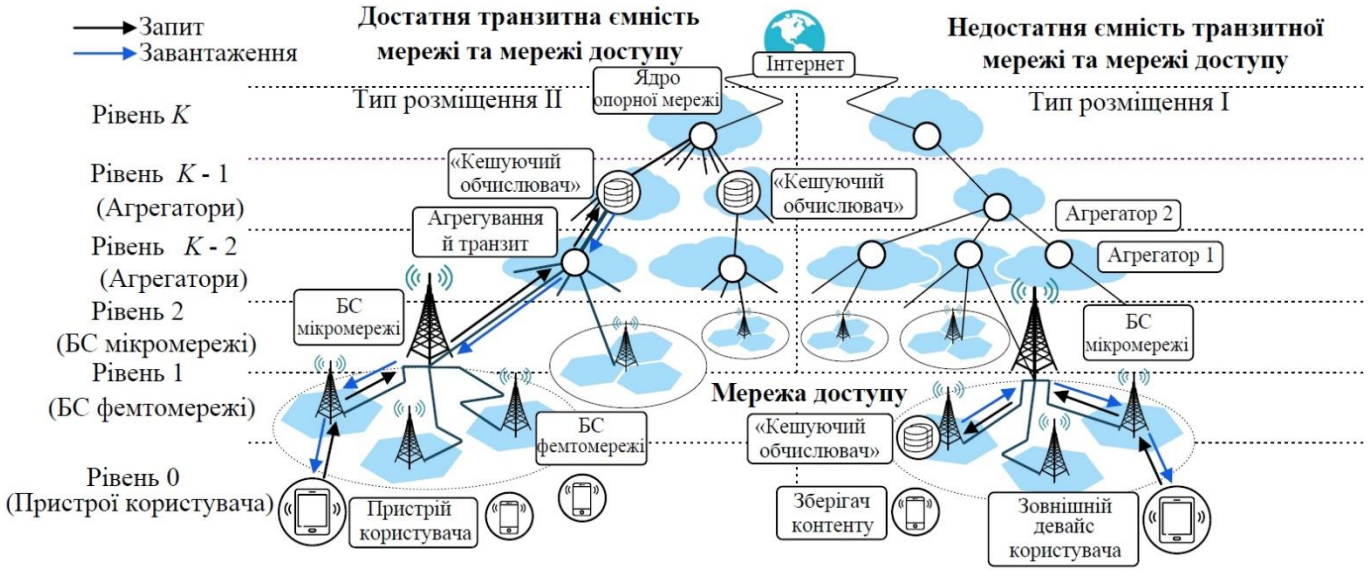

Рис. 4.2. Варіанти розміщення мережевої архітектури та відповідні рівні ієрархії

Особливості сучасного розподілу контенту. Потреба ефективному розподілі контенту одна із найважливіших чинників, визначальних розвиток мережевий архітектури. Починаючи з епохи ранніх піринговых систем сучасний функціонал мережі Інтернет зосереджений на контенті як такому, а не на його фактичному розташуванні. Підтримувані такими гігантами, як Akamai мережі доставки контенту CDN реалізують технологію anycast, що дозволяє вибрати найбільш підходящу (в сенсі близькості її розташування) копію контенту для забезпечення самоорганізується, адаптивного і

стійкого до збоїв розподілу контенту. Також було запропоновано концепцію інформаційно-орієнтованої взаємодії як спільну інфраструктуру, що надає кешування контенту всередині мережі для досягнення його масштабованого, безпечного та економічного розподілу.

Суть описаних досягнень полягає у відділенні контенту від його носіїв та їх розташування не на рівні додатків, а вже на мережному рівні. Такий підхід разюче відрізняється від традиційної архітектури.

«клієнт – сервер», що завжди перенаправляє свої обчислювальні завдання більш ресурсомісткий сервер. Однак, якщо вузли CDN розміщені в опорній мережі, може спостерігатися нестача пропускної здатності на краю мережевого покриття, що призводить до зниження надійності та збільшення затримки на бездротових з'єднаннях. Така ситуація на сьогоднішній день типова, і користувачі, що знаходяться на краю мережі, часто змушені виконувати всю необхідну обробку інформації локально на своїх терміналах, а потім використовувати зовнішні носії пам'яті для подальшого обміну результатами такої обробки. Як наслідок, подальший розвиток мережевої архітектури у напрямку більш ефективного кешування та обробки даних є вкрай актуальним.

У світлі вищевикладеного інтеграція можливостей для кешування та обробки даних з гетерогенними мережами 5G націлена на зниження часу доставки контенту шляхом розміщення його копій у різні ділянки мережі та фактичне скорочення відстані від місця зберігання ресурсів до місця їх використання. Крім того, кешування всередині мережі дозволяє «змістити» максимальний потік трафіку з годинника пік на більш зручний час, тим самим знижуючи коливання завантаження і зменшуючи ймовірність виникнення затора. Розподілене локальне кешування зазвичай функціонує у дві фази: розміщення контенту на зберігання та його доставка; воно також може враховувати додаткову інформацію про систему (наприклад, кількість переходів та розподіл популярності контенту). Таке предиктивне (випереджальне) кешування дозволяє забезпечити ефективніший розподіл контенту з урахуванням його передачі, зберігання та обробки.

Інтегровані вузли для обчислення та зберігання в 5G. Оскільки сучасні стільникові мережі ґрунтуються на базовій архітектурі «all IP», виникають два альтернативні варіанти для здійснення кешування всередині мереж 5G: (1) в ядрі мережі (EPC), що містить шлюз (serving gateway), мережевий шлюз пакетних даних (packet data network gateway) і модуль управління мобільністю MME або (2) в мережі радіодоступу (RAN), що включає всілякі БС, звані eNodeB. У деяких випадках може бути доцільно об'єднувати функціонал зберігання даних із засобами для їх обробки, особливо коли цільові сервіси вимагають безлічі звернень до віддаленого сервера протягом коротких інтервалів часу або інших складних взаємодій. Відповідна архітектура, що поєднує функції кешування і віддалених обчислень, надає їх як віртуалізовані ресурси системи 5G, спрямованих на підтримку локальних додатків.

У сучасній науково-дослідній літературі було вивчено всілякі форми інтеграції функціоналу для забезпечення передачі, зберігання та обробки інформації. Після опублікування основної роботи пропонувалися різні варіанти того, як мобільний пристрій може скористатися підтримкою віддалених серверів для виконання своїх завдань. Для переміщення обчислювальних ресурсів ближче до абонентських терміналів було запропоновано концепцію «cloudlet», яка дозволила мобільному обладнанню отримувати доступ до близько розташованих стаціонарних ресурсомістких серверів, підключених до хмарної системи за допомогою високошвидкісних бездротових з'єднань. За такого підходу сервери підтримки можуть розміщуватись у громадських та комерційних мережах, розгорнутих в аеропортах, на вокзалах, у кафе та на підприємствах, де спостерігаються масові скупчення людей. Таким чином, абонентські термінали можуть вивантажувати свої обчислювальні завдання на найближчі сервери з низькою затримкою і на високій швидкості передачі, уникаючи взаємодії з віддаленою хмарною системою.

Однак розміщення вузлів «cloudlet» тягне за собою додаткові витрати на встановлення та обслуговування, а також не надає засобів підтримки мобільних користувачів. Як альтернативний підхід було запропоновано поєднання системи хмарних обчислень та гетерогенної мережі до ступу, яке отримало назву фемтохмара. При цьому

БС малих сот фактично беруть на себе функції вузлів «cloudlet», надаючи, таким чином, ефективний розподіл обчислювальних ресурсів хмари в безпосередній близькості до мобільних користувачів. На додаток розглядалося кешування бібліотеки популярного контенту на БС фемтосот (т.зв. фемтокешування), а також у пам'яті самих абонентських терміналів, що призводить до подальшого зниження вимог щодо ємності транзитних каналів у гетерогенних мережах. В результаті фемтокешування та подібні до нього підходи мають можливість підвищити масштабованість мереж 5G, забезпечуючи більш високі швидкості передачі даних.

ВИСНОВОК ДО РОЗДІЛУ 4

В результаті розроблений протокол управління системою прямих з'єднань для гетерогенної мережі з інтегрованими між собою технологіями радіодоступу, а також спосіб його реалізації в рамках модельної мережі з високою щільністю дозволяють знижувати навантаження на стільникову мережу шляхом вивантаження трафіку в мережі інших технологій радіодоступу, підвищуючи швидкість передачі користувачів. Крім того, сформульований алгоритм розподілу трафіку користувачів в гетерогенній системі прямих з'єднань з великою кількістю пристроїв, заснований на застосуванні методів мережевого кодування, що враховує структуру сесій, що передаються, це необхідно для управління навантаженням з метою зниження часу передачі даних і підвищення ймовірності успішного доступу.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

5.1. Аналіз небезпечних і шкідливих факторів, що впливають на інженера

Відділ проектування знаходиться на другому поверсі п’ятиповерхового будинку. Приміщення має розміри: довжина 8 м, ширина 4 м, висота 4. Загальна площа - 32 м^2, загальний об’єм – 128 м^3. У відділі знаходиться 5 робочих місць інженерів-проектувальників, оснащені комп’ютерами.

Робоча площа одного співробітника становить:

$$S_{\text{роб}} = \frac{S_{\text{заг.пл}}}{N} = \frac{32}{5} = 6{,}4 \text{ м}^2$$

Робочий об’єм одного співробітника:

$$V_{\text{роб}} = \frac{V_{\text{заг.об}}}{N} = \frac{128}{5} = 25{,}6 \text{ м}^3$$

N- кількість співробітників у відділі

$S_{\text{заг.пл}}$ – загальна площа;

$V_{\text{заг.об}}$ – загальний об’єм.

Відповідно до [31] площа на одне робоче місце має становити не менше ніж 6 м^2, а об'єм не менше ніж 20 м^3. Робоче місце інженера-проектувальника відповідає вимогам.

В проектному відділі інженера-проектувальника знаходяться: комп’ютери, принтер. У даному приміщенні температура повітря у теплий період року становить 30°С, використовується природне та штучне освітлення. Штучне освітлення виконано у вигляді перериввчастих ліній світлодіодних світильників. Рівень шуму в приміщенні становить 54 дБ, а згідно з Державними санітарними нормами [32] не повинен перевищувати 50 дБ.

Робоче місце розташоване так, щоб природне світло падало з лівої сторони, при цьому відстань зі світлом до робочого місця - 1 м. Висота робочої поверхні столу над підлогою 750 мм, глибина столу – 800 мм, ширина столу 1300мм. Робочий стіл має простір для ніг висотою 650 мм та шириною 600 мм.

Перелік шкідливих та небезпечних виробничих чинників.

Створення сприятливих умов праці, в роботі інженера-проектувальника, має велике значення як для полегшення , так і для підвищення продуктивності праці. Відповідно до [33] шкідливими виробничими факторами є:

1. Підвищена температура робочого приміщення
2. Недостатня освітленість робочої поверхні
3. Виробничий шум
4. Електромагнітні випромінювання радіочастотного діапазону
5. Іонізуючі випромінювання

Відповідно до [34] робота інженера-проектувальника у приміщенні з енерговитратами 90-120 ккал/год. відносяться до категорії легких фізичних робіт Іа (роботи, що виконуються сидячи і не потребують фізичного напруження).

Таблиця 5.1

Оптимальні величини температури

Період року	Категорія робіт	Температура повітря,°С
Холодний період року	Легка Іа	22-24
Теплий період року		23-25

Допустимі величини температури на постійних робочих місцях:

Період року	Категорія робіт	Температура повітря,°С	
		Верхня межа	Нижня межа
Холодний період року	Легка Іа	25	21
Теплий період року		28	22

У проектному відділі температура повітря становить 30℃ в теплий період року,що перевищує допустиму на 2 ℃. Забезпечили температуру приміщення 23 ℃,за допомогою механічної вентиляції з вентилятором VORTICE VARIO, повітрообмін якого становить 680 $м^3$ /год.

Недостатня освітленість. В приміщенні встановлені персональні комп’ютери, присутнє природне та штучне освітлення . За вимогами [35], величина коефіцієнта природної освітленості повинна бути не менше 1.5%. В проектному відділі порушенні

вимоги, освітленість робочої поверхні складає 370 лк , а коефіцієнт освітленості складає 1.2%. Природне світло проникає у приміщення через бічні світло прорізи. Вікна мають жалюзі. Штучне освітлення виконано у вигляді переривчастих ліній світлодіодних світильників, розташованих паралельно лінії зору інженера-проектувальника. Для місцевого освітлення використовувати галогенні лампи розжарювання

Виробничий шум. Шум на робочому місці створюється: комп'ютером та периферійним пристроєм. Допустимі рівні звукового тиску на робочому місці повинні відповідати вимогам [36]:

Таблиця 5.2

Санітарні норми виробничого шуму, ультразвуку та інфразвуку

Вид трудової діяльності, робоче місце	Рівні шуму та еквівалентні рівні шуму, ДБА, дБАекв
Конструювання та проектування.	50

Реальний рівень шуму в проектному відділі становить 54 дБ, що перевищує допустимий рівень.

Для зменшення рівня шуму рекомендується використовувати місцеву та загальну звукоізоляцію, шумопоглинаючі екрани, поглинаючі фільтри.

5.2. Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів

Нормалізація повітря робочої зони. Для створення й автоматичної підтримки в ІТ відділі незалежно від зовнішніх умов оптимальних значень температури, вологості, чистоти і швидкості руху повітря, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонування повітря [37].

Виробниче освітлення. Під час аналізу освітлення на робочому місті програміста було встановлено, що воно не відповідає встановленим нормам, тому для покращення умов праці рекомендуємо збільшити рівень загальної освітленості приміщення

шляхом встановлення 5 додаткових світильників, щоб загальна кількість лам відповідала розрахованому вище значенню, а саме 36 світлодіодних ламп. Також для підтримки запроектованого освітлення у чистому виді необхідно скласти графік, де передбачити очищення віконних блоків і світильників не менше 2 разів на рік [38].

Електробезпека. Електробезпечність у приміщенні ІТ відділу пропоную забезпечити наступними технічними способами і засобами захисту:

– для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;

– забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЭ) для електроустановок з напругою до 1000 В. А також організаційними заходами:

– своєчасне проведення інструктажів з техніки безпеки [39].

Ергономіка та організація робочого місця. Після проведення аналізу робочого місця програміста в ІТ Відділі було з'ясовано, що воно відповідає встановленим вимогам.

Виходячи з результатів аналізу важкості та напруженості праці пропоную скоротити час роботи за комп'ютером, робити перерви сумарний час яких повинен складати 50 хвилин при 8-ми годинному робочому дні [40].

5.2.1. Розрахунок повітрообміну за надлишком тепла у проектному відділі

Приміщення має розміри 4×8×4, яке розміщується на другому поверсі п’ятиповерхового будинку з південного боку. Площа вікон F = 2,88 м^2. На вікнах розміщенні жалюзі. У приміщенні 5 інженерів-проектувальників, розташовано $N_{пк} = 5$ персональних комп’ютерів та принтер. Для штучного освітлення використовується 4 офісних світлодіодних світильника потужністю 125 Вт.

1. Розраховуємо загальну кількість тепла:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад,}\ \text{Вт} \qquad (5.1)$$

$Q_{над}$ – загальна кількість тепла

$Q_{осв}$ - кількість тепла від джерел штучного освітлення

$Q_{облад}$ - кількість тепла від обладнання

$Q_{ін\text{-}пр.}$- кількість тепла від інженерів-проектувальників

$Q_{рад,}$- кількість тепла від сонячної радіації

2. Розраховуємо кількість тепла від джерел штучного освітлення:

$$Q_{осв} = N \cdot \eta \,, \tag{5.2}$$

де N - сумарна потужність джерел освітлення, Вт; η - коефіцієнт теплових витрат (η = 0,55 – для світлодіодних ламп).

$$Q_{осв.} = 125 \cdot 4 \cdot 0{,}55 = 275 \text{ Вт}$$

2. Розраховуємо кількість тепла при роботі обладнання: 5 комп'ютерів і принтера (в режимі друку):

$$Q_{облад} = n \cdot P_{комп.} + P_{пр.}, \tag{5.3}$$

де n – кількість комп'ютерів (обладнання);

$P_{комп}$ – встановлена потужність комп'ютерів, $P_{комп} = 400$ Вт

$P_{пр.}$ – потужність принтера в режимі друку, $P_{пр} = 465$ Вт

$$Q_{облад} = 5 \cdot 400 + 465 = 2.5 \text{ кВт}$$

3. Розраховуємо кількість тепла від інженерів-проектувальників:

$$Q_{ін\text{-}пр.} = n \cdot q \text{ , Вт} \tag{5.4}$$

n – кількість інженерів-проектувальників

q – кількість тепла, що виділяється одним інженером-проектувальником

Кількість тепла, що виділяється одним інженером-проектувальником, який виконує легку фізичну роботу дорівнює 99 Вт.

$$Q_{ін\text{-}пр} = 5 \cdot 99 = 495 \text{ Вт}$$

4. Розраховуємо кількість тепла від сонячної радіації:

$$Q_{рад} = m \cdot S \cdot k \cdot q_{скл} \tag{5.5}$$

де m – число вікон; $S_{вікна}$ – площа одного вікна, $S_{вікна}$ =2,88 $м^2$;

k – коефіцієнт, віконного переплетення: k = 0,6 матові;

$q_{скл.}$ – надходження тепла через 1 $м^2$ вікна при різній орієнтації вікон: $q_{скл.}$ = 150 – південь;

$$Q_{рад} = 1 \cdot 2{,}88 \cdot 0{,}6 \cdot 150 = 259{,}2 \text{ Вт}$$

5. Загальна кількість тепла в проектному відділі:

$Q_{над}= Q_{осв}+ Q_{облад}+ Q_{ін\text{-}пр.} + Q_{рад}=275+2500+495+259{,}2 = 3{,}529$ кВт

6. Потрібний повітрообмін за надлишком тепла:

$$L = \frac{Q}{c \cdot \rho \cdot (t_{\text{вид}} - t_{\text{зовн}})}, \text{м}^3/\text{год} \quad (5.6)$$

Q - кількість тепла, яке виділяється в приміщення за годину, Дж:

$Q=3600 \cdot Q_{надл}$=3600·3529=12704 Вт = 5328 кДж;

c – теплоємність повітря, Дж/кг (в інтервалі температур від 0ºС до 100ºС приймається рівною $1{,}01 \cdot 10^3$Дж/кг);

ρ – густина повітря, кг/м^3(дорівнює $\rho_{внт}$=1,2 кг/м^3);

$t_{вид}$– температура повітря, що видаляється, $t_{вид}=30$℃

$t_{зовн.}$- температура повітря, що подається до робочої зони, $t_{зовн.}$=23℃

$$L = \frac{5328}{1{,}01 \cdot 10^3 \cdot 1{,}2 \cdot (30 - 23)} = 628 \text{ м}^3/\text{год}$$

Оскільки, в проектному відділі підвищена температура повітря на 2 ℃ від допустимого значення 28℃, встановили механічну вентиляцію з вентилятором VORTICE VARIO , яка забезпечила надходження до приміщення температури повітря 23 ℃, дане значення є оптимальним.

5.3. Пожежна безпека

Відповідно до [39-40] дане приміщення відноситься до категорії В по вибухово-пожежній та пожежній небезпеці із-за використання у ньому твердих горючих матеріалів з температурою спалаху понад 61℃.

Проектний відділ оснащено:

- Двома безпровідними датчиками детектування диму SD-02 (оповіщає при задимленні приміщення; площа обслуговування: до 20 м^2);
- двома порошковими вогнегасниками ВП-5 (для приміщення категорії В за відсутності горючих газів і рідин, площею до 50 м^2 і масою вогнегасної речовини – 5 кг, мінімальна кількість порошкових вогнегасників 2).

- LifeSOS LS-30LR бездротова пожежно-охоронна система (при детектуванні вторгнення, датчики передають на центральний блок сигнал тривоги по радіоканалу без проводів. Централь приймає сигнал від датчиків, включає сирену, відправляє інформацію на пульт централізованого нагляду, дзвонить на зазначені телефонні номери та відправляє SMS повідомлення з повідомленнями про тривогу.)

Для попередження виникнення пожеж проводяться організаційно-технічні заходи пожежної безпеки, які включають:

- включення питань пожежної безпеки у всі інструкції по техніці безпеки;
- виконання встановленого режиму експлуатації електричних мереж та обладнання;
- заборона куріння в недозволеному місці;
- видання необхідних інструктажів, планів евакуації

План евакуації складається з графічної і текстової частин. Графічна частина являє собою схематичний план поверху (рис. 5.1), в якому зеленими суцільними стрілками вказують шляхи евакуації, що ведуть до основних евакуаційних виходів, а пунктирними зеленими стрілками - до аварійних виходів. Двері на шляху евакуації відчиняються назовні у напрямку виходу з будівлі. На плані евакуації умовними знаками показано розміщення вогнегасників, пожежних гідрантів, телефонів, аптечок медичної допомоги, електрощитів, датчиків диму, системи охоронно-пожежної сигналізації.

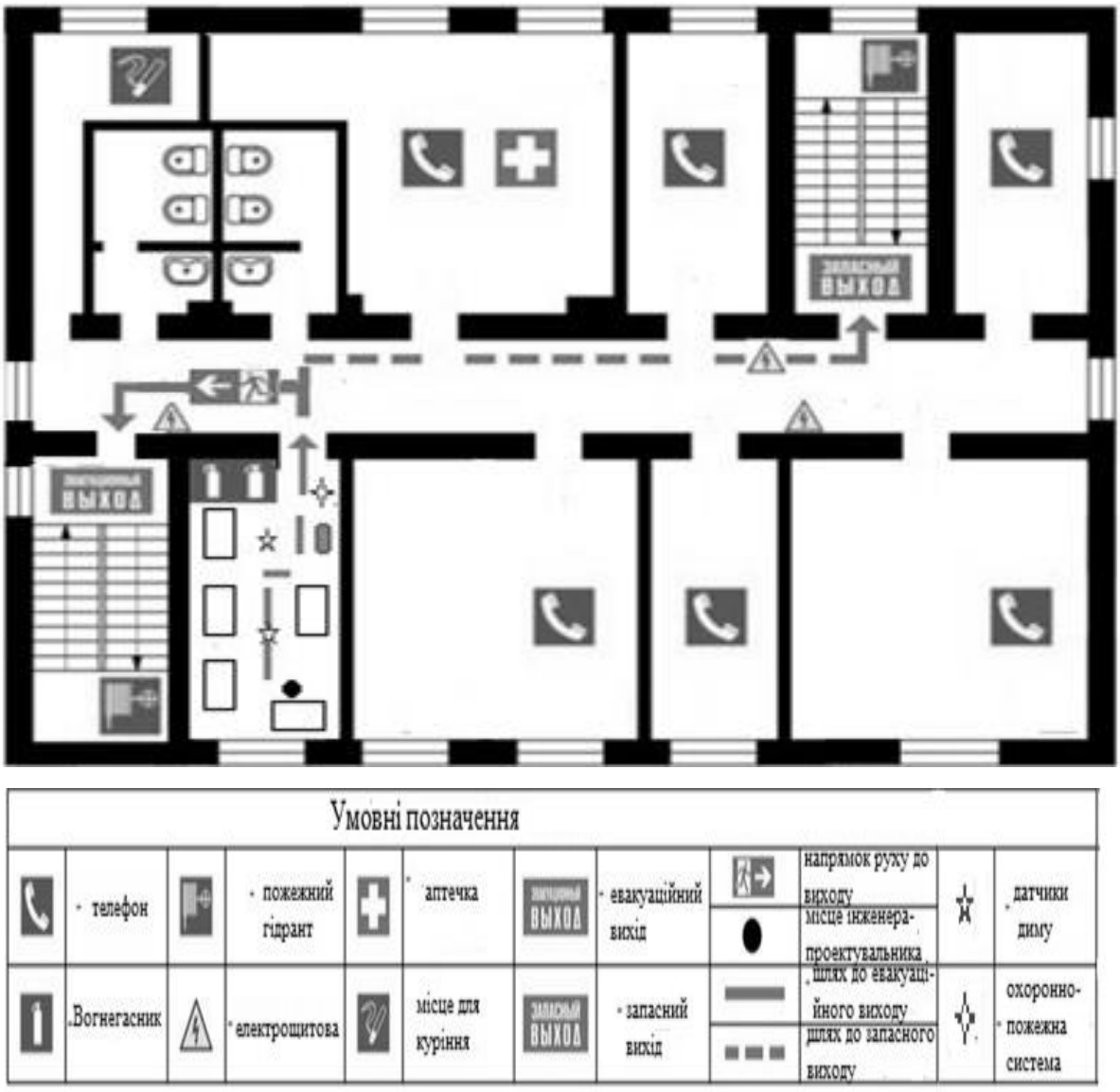

Рис 5.1. План евакуації 2 поверх

5.4. Інструкція з охорони праці при роботі з персональним комп'ютером

Вимоги безпеки перед початком роботи.

- Перед початком роботи працівник повинен зовнішнім оглядом перевірити цілісність корпусів системного блоку, відео монітора, принтера, клавіатури.
- Перевірити цілісність кабелів живлення, місць їх підключення (розеток електромережі, продовжувачів електромережі, розгалужувальних коробок, штепсельних вилок).

- Підготувати своє робоче місце, прибравши речі, які можуть заважати при виконанні роботи.
- Ввімкнути живлення ПК.
- У випадку, якщо після ввімкнення ПК не проходить загрузка або комп'ютер не виходить на робочий режим, працівник повинен повідомити керівника чи спеціаліста відділу інформаційних технологій.
- При виявленні ушкодження або яких-небудь інших недоліків повідомити безпосереднього керівника. Не приступати до роботи без його вказівки.

Вимоги безпеки під час роботи

- Необхідно стійко розташувати всі складові пристрої на столі, в тому числі і клавіатуру. Разом з тим повинна бути передбачена можливість переміщення клавіатури. ЇЇ розташування і кут нахилу повинні відповідати побажанням користувача ПК. Якщо в конструкції клавіатури не передбачений простір для опору долонь, то її слід розташовувати на відстані не менше 100 мм від краю столу в оптимальній зоні моніторного поля. При роботі на клавіатурі слід сидіти прямо, не напружуватись.
- Для зменшення несприятливого впливу на користувача пристроїв типу "миша" (вимушена поза, необхідність постійного контролю за якістю дій) слід забезпечити вільною більшу площу поверхні столу для переміщення "миші" і зручного упору ліктьового суглоба.
- Не припустимі сторонні розмови, роздратовуючи шуми тощо.
- Періодично при вимкнутому ПК слід видаляти злегка зволоженою мильним розчином хлопко-паперовою салфеткою пил з поверхонь апаратури. Екран і захисний екран протирають ватою, зволоженою спиртом.
- Не дозволяється використовувати рідинні або аерозольні засоби чистки поверхонь ПК.

Забороняється:

- самостійно ремонтувати апаратуру, в яких кінескоп та інші елементи можуть знаходитись під високою напругою (до 25 кВ0.)

- класти будь-які речі на апаратуру ПК, бутерброди та напої на клавіатуру або поруч з нею. Це може вивести її з ладу;
- затуляти вентиляційні отвори в апаратурі, це може призвести до її перегріву і виходу з ладу.

- Для зменшення негативного впливу на стан здоров'я працівників різних факторів ризику, пов'язаних з роботою на ПК, передбачаються додаткові регламентовані перерви для відпочинку користувачів ПК:
  - через кожний час безперервної роботи – 10 хвилин;
  - через кожні 2 години – 15 хвилин.
- При можливості слід чергувати зміну діяльності з іншою, не пов'язаною з роботою на ПК.
- З метою зменшення негативного впливу монотонності доцільно застосовувати чергування операцій введення тексту і введення даних (зміна змісту і темпу роботи) і т.п.
- При роботі на лазерних принтерах:
- Розташовувати принтер необхідно поряд з системним блоком так, щоб з'єднувальні шнури не були натягнуті. Забороняється ставити принтер на системний блок.
- Перш, ніж програмувати роботу принтера, впевніться, що він знаходиться в режимі зв'язку з системним блоком.
- Для досягнення високоякісного, чистого, з високою роздільною здатністю зображення щоб не зіпсувати апарат, потрібно використовувати папір, марка якого вказана в інструкції до принтера (найчастіше папір вагою 60-135 г/м^2, типу Canon або Xerox 4024).
- Обрізання країв паперу повинно бути виконаним гострим лезом ножа, без зазусенців – це зменшить вірогідність загинання паперу.
- При виконанні роботи (більше 20 хвилин), коли втручання користувача в роботу програми не потрібне, бажано вимикати живлення відео монітора.
- Для підтримки загального тонусу м'язів, профілактики кістково-м'язових порушень, зорового дискомфорту та інших несприятливих суб'єктивних почуттів під час

регламентованих перерв необхідно виконувати комплекси рекомендованих вправ для очей, для хребта, для рук.

- Кількість мікро пауз до 1-2 хвилин слід визначити індивідуально. Форма та зміст перерв можуть бути різними виконання допоміжних робіт, не пов'язаних з роботою ПК , приймання їжі, виконання рекомендованих вправ.
- Виконання фізичних вправ протягом дня рекомендується індивідуально, залежно від почуття втоми. Гімнастика повинна біти на корекцію вимушеної пози покращення кровообігу, часткову компенсацію, дефіциту рухової активності.
- Про виявлені несправності (іскріння, пробоїв, запаху гару, ознак горіння тощо) негайно припинити роботу, відключити все обладнання від електромережі і терміново повідомити безпосереднього керівника або спеціаліста по ремонту ПК.

Вимоги безпеки при закінчення роботи на ПК.

- Закінчити і зберегти в пам'яті ПК файли, які знаходились у роботі. Виконати всі дії для коректного завершення роботи в оперативній системі.
- Вимкнути принтер та інші периферійні пристрої, вимкнути системний блок. При наявності пристрою безперебійного живлення (ПБЖ) вимкнути його живлення.
- Вимкнути ПК кнопкою «POWER" (ЖИВЛЕННЯ) та вийняти штепсельну вилку кабелю живлення з розетки
- Накрити клавіатуру кришкою для попередження попадання в неї пилу.
- Навести порядок на робочому місці.

Вимоги безпеки в аварійних ситуаціях.

- Якщо після ввімкнення ПК відчувається запах горілого або при доторканні до металевих частин ПК відчувається дія електричного струму, потрібно негайно відключити ПК від електромережі та повідомити про це своєму керівникові.
- У випадку виникнення пожежі негайно розпочати гасіння наявними засобами пожежогасіння і повідомити за телефоном 101 (міська пожежна охорона) та на-

чальнику ДПД підприємства. Пам`ятайте, що загашувати електроустановки слід вуглекислотними вогнегасниками, сухим піском, щоб уникнути ураження електричним струмом.

У разі виникнення інших аварійних ситуацій слід припинити роботу і повідомити про це керівника робіт.

ВИСНОВОК ДО РОЗДІЛУ 5

На підставі виконаного розрахунку повітрообміну за надлишком тепла, значення якого 628 м^3/год, встановили механічну вентиляцію з вентилятором VORTICE VARIO, оскільки використання природної вентиляції є малоефективним. Механічна вентиляція здатна забезпечити виведення з проектного відділу температури 30℃ і підтримувати температуру повітря допустимого та навіть оптимального значення.

РОЗДІЛ 6
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

На сьогоднішній день радіотехнічне та електронне виробництво є досить розвинутим і без нього суспільство не уявляє свого життя. Електронна і радіотехнічна промисловість грає провідну роль в науково-технічній революції. Впровадження електронних приладів в різні сфери людської діяльності значною мірою сприяє успішній розробці складних науково-технічних проблем, підвищенню продуктивності фізичної і розумової праці, поліпшенню економічних показників виробництва.

В кваліфікаційній роботі розроблена система захисту з використанням серверного обладнання, що може здійснювати негативний вплив на навколишнє середовище.

6.1. Аналіз впливу техногенних чинників

Широке використання електричного та електронного обладнання дозволило не тільки підвищити якість життя людей, але й призвело до негативних наслідків для навколишнього середовища та здоров'я людини. Можна виділити основні шкідливі та небезпечні чинники, які впливають на навколишнє середовище [42]:

- шумове забруднення;
- вібраційне забруднення;
- електромагнітне забруднення
- теплове забруднення
- радіаційне забруднення

Шумове забруднення. У сучасному світі в умовах науково-технічного прогресу шум став однією з форм фізичного (хвильового) забруднення природного середовища. Шумом прийнято вважати усі неприємні та небажані звуки або їх сукупність, які заважають нормально працювати, сприймати потрібну звукову інформацію та відпочивати.

Адаптація до нього практично неможлива. Фоновий рівень шуму навколишнього середовища становить 30-60 децибел. До цього природного фону за сучасних умов додаються виробничі й транспортні шуми, рівень яких нерідко перевищує 100 децибел. Джерелами шуму є: промислові об'єкти, транспорт, гучномовні пристрої, телевізори, радіоприймачі, музичні інструменти, юрби людей тощо. Шум у виробничих умовах негативно впливає на працівника: послаблює увагу, посилює розвиток втоми, сповільнює реакцію на небезпеку. Внаслідок цього знижується працездатність та підвищується ймовірність нещасних випадків. Допустимі рівні звукового тиску в октавних смугах частот на робочих місцях у виробничих приміщеннях наведені в таблиці 5.1 [42]:

Таблиця 6.1

Допустимі рівні звукового тиску в октавних смугах частот

Рівні звукового тиску в дБ, в октавних смугах частот, Гц								
31,5	63	125	250	500	1000	2000	4000	8000
107	95	87	82	78	75	73	71	69

Встановлено, що рослини під впливом шуму знижують енергію до зростання, у них спостерігається надмірне (навіть повне, що призводить до загибелі) виділення вологи через листя, можливі порушення у клітинах. Гинуть листя і квіти рослин, які розташовані близько до джерела інтенсивного шуму (звуку). Відсутність шуму особливо необхідний для тварин, які обмінюються звуковою інформацією, а також аналізуючи звуки навколишнього середовища з метою покращання отримання інформації, в тому числі сигналів тривоги. Аналогічно діє шум на тварин. Від шуму реактивного літака гинуть личинки бджіл, самі

вони втрачають здатність орієнтуватися, у пташиних гніздах дає тріщини шкаралупа яєць. Від коливань повітря, які утворюються звуками переносної радіоапаратури, не можуть піднятися у повітря жуки, джмелі та інші комахи.

Вібраційне забруднення. Вібрація – це механічні коливання твердого тіла. Вібрацію поділяють на природну та штучну. Джерелами природної вібрації є землетруси, що викликаються природними чинниками. Джерелами штучної вібрації є промисло-

вість, транспорт. Тривалі вібрації завдають великої шкоди здоров'ю людини – від сильної втоми до змін багатьох функцій організму: порушення серцевої діяльності, нервової системи, спазмів судин, деформації м'язів, струсу головного мозку тощо. Особливо небезпечна вібрація з частотою, яка є резонансною з частотою коливання окремих органів чи частин тіла людини, що може призвести до їх пошкодження. Тривала дія вібрації може спричинити професійне захворювання – вібраційну хворобу [42].

Електромагнітне забруднення. У процесі еволюції біосфера постійно знаходилася і знаходиться під впливом електромагнітного поля (ЕМП) природного походження (природний фон): електричного й магнітного поля Землі, космічного електромагнітного випромінювання, насамперед того, що генерується Сонцем. У період науково-технічного прогресу людство створювало і дедалі ширше використовувало штучні (антропогенні) джерела ЕМП. У наш час ЕМП антропогенного походження значно перевищують природний фон і є тим несприятливим чинником, вплив якого на людину та довкілля рік за роком зростає. Ступінь впливу ЕМП на організм людини залежить від діапазону частот, інтенсивності та тривалості дії, характеру випромінювання (неперервного чи модульованого), режиму опромінювання, розміру поверхні тіла, що зазнає опромінювання, індивідуальних особливостей організму. Електромагнітні поля можуть викликати біологічні та функціональні порушення у функціонуванні організму. Функціональні ефекти проявляються у передчасній втомлюваності, частих болях голови, погіршенні сну, порушенні функцій серцево-судинної та центральної нервової систем. Тривалий та інтенсивний вплив ЕМП призводить до стійких порушень та захворювань. Біологічні негативні ефекти впливу ЕМП проявляються у тепловій та нетепловій діях. Теплова дія призводить до підвищення температури тіла та місцевого вибіркового нагрівання органів і тканин організму внаслідок переходу електромагнітної енергії в теплову. Таке нагрівання особливо небезпечне для органів із слабкою терморегуляцією (головний мозок, очі, нирки, шлунок тощо). Наприклад, випромінювання сантиметрового діапазону призводить до появи катаракти, тобто до поступової втрати зору [42].

Теплове забруднення. Теплове забруднення – це результат розсіювання в навколишнє середовище теплоти, яка виділяється у багаточисельних теплових процесах,

насамперед пов’язаних зі згоранням палива. Під час згорання палива щорічно витрачається до 23% кисню, що утворюється в процесі фотосинтезу на Землі за рік. За підрахунками під час спалювання вугілля в навколишнє середовище викидається радіоактивних компонентів більше, ніж за той самий час на всіх атомних електростанціях у разі безаварійної роботи. Теплове забруднення гідросфери відбувається переважно внаслідок скидання у водойми підігрітих вод від ТЕС, АЕС та інших енергетичних об’єктів. Тепла вода змінює термічні та біологічні режими водойм і шкідливо впливає на їхніх мешканців [42].

6.2. Вплив приймальних пристроїв на навколишнє середовище

Абонентський приймач – телевізійний приймач (приставка), пристрій, що приймає сигнал цифрового телебачення, декодує його і перетворює в аналоговий сигнал для виведення через роз'єми RCA або SCART або перетворює в цифровий сигнал для виведення через роз'єм HDMI , і передає його далі на телевізор.

Перехід до цифрового телебачення призвів до зростання виробництва цифрових абонентських приймачів, що в свою чергу може негативно впливати на навколишнє середовище. Приймач продукує слабкі електричні і магнітні змінні поля в широкому діапазоні частот. Проте проблема впливу електромагнітних випромінювань, що продукуються заслуговує на особливу увагу. Наукові дослідження показали, що ЕМВ мають у своєму складі чинник, котрий впливає на користувачів при наявності сучасних екранів від ЕМВ. Вчені України ідентифікували цей чинник як торсіонові поля, котрі супроводжують будь-яке електромагнітне випромінювання та являються його інформаційною компонентою [45]. Робоча група Всесвітньої організації охорони здоров’я з гігієнічних аспектів користування моніторами та радіо терміналами виявили порушення стану здоров’я при користуванні пристроями, які мають електромагнітне випромінювання, найсерйозніші з яких:

- погіршення зору;
- порушення імунної системи;
- порушення психоемоційної сфери (стресовий синдром, агресивність)

Для забезпечення безпеки здоров'я користувачів в Україні діють Державні санітарні норми і правила при роботі з джерелами електромагнітних полів «ДСанПіН 3.3.6.096-2002». Значення ГДР напруженості електричної ($E_{гд}$) і магнітної ($H_{гд}$) складових залежно від тривалості їх дії наведені в таблиці 5.2.

Таблиця 6.2

Значення ГДР напруженості електричної ($E_{гд}$) і магнітної ($H_{гд}$) складових

Час перебування персоналу, год	$E_{гд}$, В/м					$H_{гд}$, А/м			
	1-10 кГц	10-60 кГц	0,063 МГц	3-30 МГц	30-300 МГц	1-10 кГц	10-60 кГц	0,06-3 МГц	30-50 МГц
8	120	70	50	30	10	9	7	5	0,3
7	130	75	53	32	11	9,8	7,5	5,3	0,32
6	140	82	58	34	12	10,6	8,1	5,8	0,34
5	155	90	63	37	13	11,6	8,8	6,3	0,38
4	175	110	71	42	14	13	9,9	7,1	0,42
3	200	115	82	48	16	15	11,4	8,2	0,49
2	250	140	100	59	20	18,4	14	10	0,6
1	350	200	141	84	28	26	19,7	14,2	0,85
0,5	500	280	200	118	40	37,6	27,9	20	1,2

У результаті дії на організм людини електромагнітних випромінювань в діапазоні 30 кГц - 300 МГц (НЧ) спостерігається: загальна слабкість, підвищена втома, сонливість, порушення сну, головний біль та біль в ділянці серця. З'являється роздратованість, втрачається увага, сповільнюються рухово-мовні реакції. Виникає ряд симптомів, які свідчать про порушення роботи окремих органів - шлунку, печінки, підшлункової залози.

Для того, щоб зменшити рівень електромагнітного випромінювання потрібно обмежити безперервний час роботи абонентського приймача [43-46].

В Україні норми електромагнітної безпеки регламентуються Державними санітарними нормами і правилами захисту населення від впливу електромагнітного випромінювання, згідно з якими допустимі рівні інтенсивності електромагнітного випромінювання для цивільного населення становлять 2,5 мкВт/см^2.

Абонентський приймач під час роботи створює шум, рівень якого становить 54 дБ. Допустимий рівень звукового тиску повинний відповідати «ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку», а саме 50 дБ.

Велика кількість звукових сигналів, що поступають до кори головного мозку, викликають переживання, страх, передчасну втому. Дія шуму на людину виражається в широкому діапазоні - від суб'єктивного роздратування до об'єктивних змін в ЦНС, органах слуху, серцево-судинних та ендокринній системах, травному акті та інших органів і систем. Першим показником шкідливої дії шуму є скарги на роздратованість, переживання, порушення сну [45].

6.3. Засоби для захисту від електромагнітного випромінювання та шуму, проблема електронних відходів

Захист від електромагнітного випромінювання. Для зменшення впливу ЕМП на персонал та населення, яке знаходиться у зоні дії радіоелектронних засобів, потрібно вжити ряд захисних заходів. До їх числа можуть входити організаційні, інженерно-технічні та лікарсько-профілактичні.

До заходів щодо зменшення впливу на працівників ЕМП належать: організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи здійснюють органи санітарного нагляду. Вони проводять санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи передбачають таке розташування джерел ЕМП, яке б зводило до мінімуму їх вплив на працюючих, використання в умовах виробництва дистанційного керування апаратурою, що є джерелом випромінювання, екранування джерел випромінювання, застосування засобів індивідуального захисту (халатів, комбінезонів із металізованої тканини, з виводом на заземлюючий пристрій). Для захисту очей доцільно використовувати захисні окуляри ЗП5-90. Скло окулярів вкрито напівпровідниковим оловом, що послаблює інтенсивність електромагнітної енергії при світлопропусканні не нижче 75%.

Взагалі, засоби індивідуального захисту необхідно використовувати лише тоді, коли інші захисні засоби неможливі чи недостатньо ефективні: при проходженні через зони опромінення підвищеної інтенсивності, при ремонтних і налагоджувальних роботах в аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливість виконання трудових операцій, погіршують гігієнічні умови.

У радіочастотному діапазоні засоби індивідуального захисту працюють за принципом екранування людини з використанням відбиття і поглинання ЕМП. Для захисту тіла використовується одяг з металізованих тканин і рідіопоглинаючих матеріалів. Металізовану тканину роблять із бавовняних ниток з розміщеним всередині них тонким проводом, або з бавовняних чи капронових ниток, спірально обвитих металевим дротом. Така тканина, наче металева сітка, при відстані між нитками до 0,5 мм значно послаблює дію випромінювання. При зшиванні деталей захисного одягу треба забезпечити контакт ізольованих проводів. Тому електрогерметизацію швів здійснюють електропровідними масами чи клеями, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок безконтактних проводів.

Лікарсько-профілактичні заходи передбачають проведення систематичних медичних оглядів працівників, які перебувають у зоні дії ЕМП, обмеження в часі перебування людей в зоні підвищеної інтенсивності електромагнітних випромінювань, видачу працюючим безкоштовного лікарсько-профілактичного харчування, перерви санітарно-оздоровчого характеру.

Захист від шуму. Для зменшення і ліквідації шуму застосовується цілий комплекс заходів, що називається шумозахистом. Це застосування звукопоглинаючих матеріалів, раціональне розміщення будівельних об'єктів, створення вздовж вулиць екранів у вигляді земляних валів, стін різних конструкцій, шумовідбиваючих, як правило не житлових будівель - магазинів, складів, гаражів.

Проблема електронних відходів. Згідно Закону України «Про відходи» з метою запобігання або зменшення обсягів утворення відходів потрібно здійснювати системи збирання та утилізації електричного та електронного обладнання [30]. Вирішення проблеми електронних відходів в Україні мав би забезпечити «Технічний регламент з поводження з

відходами електричного та електронного обладнання», розробка якого в Україні здійснюється з 2008 року. Згідно з проектами цих законодавчих актів імпортери і виробники можуть як самостійно утилізувати електровідходи, так і підписувати договори на виконання робіт з організації збирання, заготівлі та утилізації відповідних видів техніки з уповноваженими підприємствами. Розроблено також проект Постанови Кабінету Міністрів України «Про затвердження Технічного регламенту з поводження з відходами електронного та електричного устаткування». Цим регламентом передбачається створення пунктів збору відходів електронного та електричного обладнання, які повинні розташовуватися у місцях, зручних для користувачів, та забезпечувати безоплатність послуг, що надаються цими пунктами для користувачів. Наразі обговорюється ще один варіант вирішення проблеми, а саме проект внесення змін до Податкового Кодексу, в якому передбачає централізоване стягнення коштів з імпортерів та виробників різних споживчих товарів з метою забезпечення за рахунок цих коштів належної організації збирання, заготівлі та утилізації відходів від зазначених товарів.

Однак, загалом проблему електронних відходів в Україні необхідно вирішити як в організаційно-правовому аспекті – створення фондів виробників, підтримка держави підприємств з утилізації відходів, так і в соціально-інформаційному: українців треба переконати в тому, що виносити на звичайний смітник поламаний електронний пристрій – не можна.

ВИСНОВОК ДО РОЗДІЛУ 6

Телекомунікаційні ресурси створюють негативний вплив на навколишнє середовище. Вони є джерелами електромагнітного випромінювання та шумового забруднення. Для мінімізації ризику виникнення захворювань, ефективними є інженерно-технічні заходи, які зменшать дію шкідливих чинників. Також були розглянута проблема електронних відходів, одним зі шляхом вирішення якої є створення пунктів збору відходів електронного та електричного обладнання.

ВИСНОВКИ

Ціль кваліфікаційної роботи полягає в визначенні характеристик цифрових зображень-контейнерів, що забезпечують найбільшу стійкість стеганографічної системи для подальшої передачі за допомогою транспортної мережі п’ятого покоління. Для досягнення вказаної мети було вирішено ряд теоретичних і практичних задач. У ході проведених досліджень отримані такі основні наукові результати.

1. Зроблено короткий огляд методів вбудовування інформації в просторові області цифрових зображень. Дана коротка характеристика існуючим методам.

2. Розглянуто принцип дії LSB методу для стеганографічної системи на основі цифрових зображень. Сформовано загальний список вимог та критеріїв вибору зображень-контейнерів для алгоритмів стеганографічного приховання інформації на основі методу LSB. На основі сформульованих вимог в якості досліджуваних зображень-контейнерів обрані зображення формату BMP.

3. Проведено дослідження статистичних характеристик цифрових зображень BMP формату, зображення отримані з допомогою цифрового фотоапарата шляхом конвертації з RAW формату. Конвертація з RAW формату, не призначеного для безпосередньої візуалізації, в формат BMP відбувається без втрати якості зображення. Як досліджувані характеристики були обрані монотонність, ентропія і дисперсія зображень. Дослідження зміни статистичних характеристик зображень проведено методами оцінки критерію Хі-квадрат і RS методом стегоаналізу. На основі отриманих даних можна зробити висновок, що найбільшою стеганографічною стійкістю володіють зображення з найбільшою ентропією та дисперсією молодшої бітової площини, з підвищенням монотонності зображення стійкість стеганографічної системи погіршується.

4. Аналіз дисперсії бітових площин показав, що молодші бітові площини тестованих зображення мають досить близькі показниками дисперсії порядку 16000. Мінімальне значення дисперсії молодших бітових площин становить близько 6000,

що відповідає ймовірності виявлення повідомлення методу RS аналізу в 60 %. З збільшенням біта вбудовування збільшується розкид значень дисперсії досліджуваних зображень. RS метод стегоаналізу показує, що при показниках дисперсії що прямують до 0, ймовірність виявлення прихованої інформації, що міститься у зображенні, прямує до 100 %. Таким чином, наведені дані о дисперсії підтверджують теорію випадковості молодших біт і показують їх перевагу найбільш старшим бітам при вбудовуванні інформації методом LSB. При виникненні необхідності залучення старших біт при LSB стеганографії, слід більше уважно відноситися до вибору зображення в силу великих розкидів показників дисперсії різних зображень та віддавати переваги зображенням, що володіють найбільшою дисперсією в цих бітах.

5. Аналіз даних про ентропії показує, що її відносна величина молодших бітових площин є більшою у порівнянні зі старшими бітами. Максимальне відносне значення молодших бітових площин становить близько 18, у свою чергу максимальне значення ентропії другої бітової площини поменшало більше чим в два рази. Максимальна ймовірність виявлення впровадження повідомлення в молодший біт зображення становить близько 60 % при значенні ентропії рівному 3. При задіянні найбільш старших біт зображень, ймовірність виявлення у 60 % досягається при відносному значенні ентропії близько 6. Необхідно відзначити, що з збільшенням біта вбудовування, відносне значення ентропії бітових площин тестованих зображень прямує до максимального значення. Підсумовуючи, можна дійти висновку, що, як і у випадку з дисперсією зображень, при виборі зображення в якості контейнера для стеганографічного приховування даних методом LSB, слід вибирати зображення з великими значеннями ентропії в бітових площинах.

Результати представлені для цифрових зображень формату BMP, однак можуть бути адаптовані та на інші формати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конахович р. Ф., Пузиренко А. Ю. Комп'ютерна стеганографія. Теорія та практика. - К.: "МК-Прес", 2006.
2. Ewan Fleischmann, Michael Gorski, Jan-Hendrik Hühne and Stefan Lucks, "Key Recovery Attack on Full GOST Block Cipher with Zero Time and Memory", Published as ISO/IEC JTC, 2019.
3. J. Daemen, R. Govaerts and J. Vandewalle, "A New Approach to Block Cipher Design" in ast Software Encryption (FSE), Springer-Verlag, pp. 18-32, 1993.
4. M. Juan and Gutierrez Cardenas, "Secret Key Steganography with Message Obfuscation by Pseudo-random Number Generators", IEEE 38th International Computer Software and Applications Conference Workshops, pp. 164-168, 2014.
5. Pavit Singh Sapra and Himanshu Mittal, "Secured LSB Modification using Dual Randomness", International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-4, 2016.
6. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich and Ton Kalker, Digital Watermarking and Steganography 2nd Ed. (The Morgan Kaufmann Series in Multimedia Information and Systems).
7. Mikhail Buinevich, Konstantin Izrailov and Andrei Vladyko, "Testing of utilities for finding vulnerabilities in the machine code of telecommunication devices", 19th International Conference on Advanced Communication Technology (ICACT), pp. 408-414, 2017.
8. F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding-A survey", special issue on protection of multimedia content IEEE, pp. 1062-1078, July 2019.
9. I. J. Cox, J. Killian, F. T. Leighton and T. Shannon, "Secure spread spectrum watermarking for multimedia", IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673-1687, Dec. 2017.

10. H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking", IEEE Trans. Signal Process., vol. 51, no. 4, pp. 898-905, Apr. 2013.

11. M. Gkizeli, D. A. Pados and M. J. Medley, "Optimal signature design for spread-spectrum steganography", IEEE Trans. Image Process., vol. 16, no. 2, pp. 391-405, Feb. 2017.

12. P. P. Markopoulos, G. N. Karystinos and D. A. Pados, "Optimal algorithms for L1-subspace signal processing", IEEE Trans. Signal Process., vol. 62, no. 19, pp. 5046-5068, Oct. 2019.

13. S. Kundu, P. P. Markopoulos and D. A. Pados, " Fast computation of the L 1 -principal component of real-valued data ", Proc. IEEE Int. Conf. Acoustic Speech Signal Process. (ICASSP), pp. 8028-8032, May 2019.

14. Jessica Fridrich, Steganography in digital media: principles algorithms and applications, Cambridge University Press, 2019.

15. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, Anthony TS Ho and Ki-Hyun Jung, "Image steganography in spatial domain: A survey", Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

16. Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial and Brendan Halloran, "Comprehensive survey of image steganography: Techniques evaluations and trends in future research", Neurocomputing, vol. 335, pp. 299-326, 2019.

17. Shumeet Baluja, "Hiding images within images", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 7, pp. 1685-1697, 2020.

18. Miroslav Goljan, Jessica Fridrich and Rémi Cogranne, "Rich model for steganalysis of color images", 2014 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 185-190, 2014.

19. Mehdi Boroumand, Mo Chen and Jessica Fridrich, "Deep residual network for steganalysis of digital images", IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1181-1193, 2021.

20. Jiaohua Qin, Yuanjing Luo, Xuyu Xiang, Yun Tan and Huajun Huang, "Coverless image steganography: a survey", IEEE Access, vol. 7, pp. 171372-171394, 2021.

21. K Wu and C Wang, "Steganography using reversible texture synthesis", IEEE Transactions on Image Processing, vol. 24, no. 1, pp. 130-139, 2021.

22. Sheng Li and Xinpeng Zhang, "Toward construction-based data hiding: from secrets to fingerprint images", IEEE Transactions on Image Processing, vol. 28, no. 3, pp. 1482-1497, 2018.

23. Zhuo Zhang, Guangyuan Fu, Rongrong Ni, Jia Liu and Xiaoyuan Yang, "A generative method for steganography by cover synthesis with auxiliary semantics", Tsinghua Science and Technology, vol. 25, no. 4, pp. 516-527, 2020.

24. Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng and Bin Li, "A novel image steganography method via deep convolutional generative adversarial networks", IEEE Access, vol. 6, pp. 38303-38314, 2018.

25. Diederik P Kingma and Prafulla Dhariwal, Glow: Generative flow with invertible 1×1 convolutions, 2018.

26. Kaiming He, Xiangyu Zhang, Shaoqing Ren and Jian Sun, "Deep residual learning for image recognition", Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 770-778, 2016.

27. Ziwei Liu, Ping Luo, Xiaogang Wang and Xiaoou Tang, "Deep learning face attributes in the wild", Proceedings of International Conference on Computer Vision (ICCV), December 2015.

28. Jian Ye, Jiangqun Ni and Yang Yi, "Deep learning hierarchical representations for image steganalysis", IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2545-2557, 2017.

29. Weike You, Hong Zhang and Xianfeng Zhao, "A siamese cnn for image steganalysis", IEEE Transactions on Information Forensics and Security, vol. 16, pp. 291-306, 2020.

30. Anish Mittal, Rajiv Soundararajan and Alan C Bovik, "Making a “completely blind” image quality analyzer", IEEE Signal processing letters, vol. 20, no. 3, pp. 209-212, 2012.

31. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації електронно-обчислювальних машин.

32. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

33. Державні санітарні норми та правила «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу».

34. «ДСН 3.3.6.042-99 Санітарних норми мікроклімату виробничих приміщень».

35. ДБН 13.2.5-28-2006 «Природне і штучне освітлення».

36. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

37. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони».

38. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення».

39. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».

40. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».

41. НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».

42. Прогнозування екологічних ризиків з використанням аналізу ієрархів та теорії нечітких множин: міжнародна науково-практична конференція «І-й всеукраїнський з'їзд екологів»: Тези доповідей. Україна, м. Вінниця, 4-7 жовтня 2016. – 2016. – С.25.

43. Клап Я. А., Яремкевич О. С., Червецова В. Г., Заярнюк Н. Л., Новіков В. П., Дослідження впливу електромагнітних, постійних магнітних та акустичних полів на організм людини // Вісник Нац. ун-ту "Львівська політехніка". – 2016 – № 812. – С. 365–372.

44. Сучасний стан досліджень впливу електромагнітних випромінювань на організм людини [Електронний ресурс]/[А. П. Чорний, В. В. Никифоров, Д. І. Родькін,

В. Ю. Ноженко] // Інженерні та освітні технології в електротехнічних та комп'ютерних системах: щоквартальний науково-практичний журнал. – Кременчук: КрНУ, 2013.

45. Екологія та охорона навколишнього природного середовища: навч. посібник для вузів / В. С. Джигирей. - 6-те вид., випр. і доп. - К. : Знання, 2017. - 422 с.

46. Боротьба з шумом на виробництві: Довідник / Під ред. О. Я. Юдіна. – М: Машинобудування, 2015. – 297 с.