Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

ПРИХОВУВАННЯ ДАНИХ В ПРОСТОРОВІЙ ОБЛАСТІ НЕРУХОМИХ ЗОБРАЖЕНЬ НА ОСНОВІ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА

Методичні рекомендації
до лабораторної роботи з дисципліни «Стеганографія»
для студентів спеціальності 125 «Кібербезпека»

Харків – 2019

УДК 004.415.24 (075.8)
К 89

Рецензенти:

В. А. Краснобаєв – доктор технічних наук, професор, професор кафедри електроніки і управляючих систем Харківського національного університету імені В. Н. Каразіна;

О. Г. Толстолузька – доктор технічних наук, старший науковий співробітник, професор кафедри теоретичної та прикладної системотехніки Харківського національного університету імені В. Н. Каразіна.

Затверджено до друку рішенням Науково-методичної ради
Харківського національного університету імені В. Н. Каразіна
(протокол № 1 від 30.10.2019 р.)

К 89 **Приховування** даних в просторовій області нерухомих зображень на основі прямого розширення спектра. Методичні рекомендації до лабораторної роботи з дисципліни «Стеганографія» для студентів спеціальності 125 «Кібербезпека» / уклад. О. О. Кузнецов, М. О. Полуяненко, Т. Ю. Кузнецова – Харків : ХНУ імені В. Н. Каразіна, 2019. – 68 с.

Методичні рекомендації розроблено для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека». Матеріали методичних рекомендацій мають допомогти студентам усвідомити специфіку безпеки інформаційних і комунікаційних систем та особливості професійної наукової діяльності у галузі захисту інформації. Передбачається, що в результаті навчання студенти оволодіють початковими навичками роботи з дисципліни «Стеганографія», вироблять ставлення до використання методів та принципів приховування даних, набудуть практичних вмінь та навичок щодо розробки стеганографічних систем.

УДК 004.415.24 (075.8)

ЗМІСТ

1. МЕТА ТА ЗАВДАННЯ ЛАБОРАТОРНОЇ РОБОТИ

Мета роботи: закріпити теоретичні знання за темою «Приховування даних у просторовій області нерухомих зображень на основі прямого розширення спектру», набути практичних вмінь та навичок щодо розробки стеганографічних систем, дослідити властивості стеганографічних методів, що засновані на низькорівневих властивостях зорової системи людини (ЗСЛ).

Лабораторна робота № 3 виконується у середовищі символьної математики MathCAD версії 12 або вище.

Завдання лабораторної роботи

1. Реалізувати у середовищі символьної математики MathCAD алгоритми формування ансамблів ортогональних дискретних сигналів Уолша–Адамара. Реалізувати алгоритм кодування інформаційних бітів даних складними дискретними сигналами.

2. Реалізувати у середовищі символьної математики MathCAD алгоритми приховування даних у просторовій області зображень шляхом прямого розширення спектрів із використанням ортогональних дискретних сигналів. Виконати зорове порівняння порожнього та заповненого контейнера та зробити відповідні висновки. Реалізувати алгоритми кореляційного прийому дискретних сигналів. Реалізувати алгоритми вилучення даних з просторової області зображень на основі прямого розширення спектра.

3. Провести експериментальні дослідження ймовірнісних властивостей реалізованого методу, отримати емпіричні залежності ймовірності правильного вилучення даних та частки внесених при цьому похибок у контейнер-зображення.

4. Реалізувати у середовищі символьної математики MathCAD алгоритми формування ансамблів квазіортогональних дискретних сигналів. Реалізувати алгоритми приховування та вилучення даних в просторовій області зображень із використанням квазіортогональних дискретних сигналів.

5. (Додаткове завдання). Реалізувати у середовищі символьної математики MathCAD адаптивний алгоритм формування квазіортогональних дискретних сигналів. Реалізувати алгоритми приховування та вилучення даних із адаптовано сформованих квазіортогональних дискретних сигналів, отримати емпіричні залежності ймовірності правильного вилучення даних та частки внесених при цьому похибок у контейнер-зображення.

2. МЕТОДИЧНІ ВКАЗІВКИ З ОРГАНІЗАЦІЇ САМОСТІЙНОЇ РОБОТИ

1. Вивчити теоретичний матеріал лекції «Приховування даних у просторовій області нерухомих зображень на основі прямого розширення спектра».

2. Вивчити матеріал основного джерела літератури (Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография): метод розширення спектра (ст. 180–189).

3. Вивчити матеріал додаткових джерел:

а) основи використання складних сигналів у системах зв'язку (Стасєв Ю. В. Основи теорії побудови сигналів, ст. 5–13);

б) дискретні сигнали (Стасєв Ю. В. Основи теорії побудови сигналів, ст. 14–22).

4. Вивчити основні команди у середовищі символьної математики MathCAD щодо роботи із зображеннями.

5. Підготувати відповіді на контрольні запитання.

6. Підготувати бланк звіту з лабораторної роботи.

Допуск до виконання лабораторної роботи здійснюється за результатами письмового опитування.

3. ЗАГАЛЬНОТЕОРЕТИЧНІ ПОЛОЖЕННЯ ЗА ТЕМОЮ ЛАБОРАТОРНОЇ РОБОТИ

Завадозахисні системи зв'язку та управління

Прагнення забезпечити високу завадозахищеність, множинний безконфліктний доступ до каналу, а також енергетичний і інформаційний захист повідомлень, що передаються, привело до створення широкосмугових завадозахисних адресних систем зв'язку, що працюють в режимі вільного доступу з кодовим ущільненням каналів. Вільний доступ забезпечується тим, що загальний широкосмуговий радіотракт може використовуватися абонентами за необхідністю, коли з'являються повідомлення, що підлягають передачі.

Теоретичною основою завадозахищеного зв'язку є відома теорема Шеннона щодо пропускної здатності каналу зв'язку, яка стверджує, що за швидкості передачі інформації R, що менша від пропускної здатності каналу зв'язку C, існують такі засоби кодування інформації, що дозволяють передавати цю інформацію із заданою якістю за будь-якого, як завгодно малого відношення потужності сигналу P_c до потужності завади $P_п$.

Ця теорема не вказує на конкретні методи кодування, однак чітко формулює шлях досягнення заданої якості передачі.

Згідно із теоремою Шеннона пропускна здатність каналу зв'язку дорівнює

$$C = \Delta F_k \log_2\left(1 + \frac{P_c}{P_п}\right), \qquad (1)$$

де ΔF_k – ширина смуги пропускання каналу.

Поділивши обидві частини рівності (1) на ΔF_k і змінивши основу логарифма, отримаємо

$$\frac{C}{\Delta F_k} = 1,44 \cdot \ln\left(1 + \frac{P_c}{P_n}\right). \qquad (2)$$

За $\frac{P_c}{P_п} < 1$, що є корисним для завадозахищених радіоканалів, вираз (2) буде мати такий вигляд

$$\frac{C}{\Delta F_k} = 1,44 \cdot \left[\frac{P_c}{P_n} - \frac{1}{2}\left(\frac{P_c}{P_n}\right)^2 + \frac{1}{3}\left(\frac{P_c}{P_n}\right)^3 k\right]. \qquad (3)$$

Враховуючи, що $\frac{P_c}{P_п} < 1$ і нехтуючи членами ряду вищих порядків, можна записати

$$\frac{C}{\Delta F_k} = 1,44 \cdot \frac{P_c}{P_n}. \qquad (4)$$

Вираз (4) вказує на шлях досягнення заданої якості передачі за якого завгодно малого відношення $\frac{P_c}{P_п}$. Вважаючи, що ширина смуги пропускання каналу дорівнює ширині спектра використовуваних сигналів $\Delta F_k = \Delta F_c$, з (4) витікає, що зі зменшенням відношення потужності сигналу до потужності завади необхідно застосовувати методи кодування, що призводять до розширення спектра сигналів.

Для C = R неважко помітити, що зберігання рівняння (4) зі зменшенням відношення $\frac{P_c}{P_п}$ досягається пропорційним збільшенням відношення $\frac{\Delta F_c}{R}$.

Метод передачі інформації, за якого сигнал займає смугу частот, що набагато переважає смугу частот повідомлення називається широкосмуговим.

Ортогональні, субортогональні та квазіортогональні дискретні сигнали, їх кореляційні та ансамблеві властивості

Як уже було відмічено для побудови сучасних завадозахисних систем цифрового зв'язку використовуються методи теорії дискретних сигналів, кореляційного і спектрального аналізу. З позиції ефективного використання частотно-часових і енергетичних ресурсів каналів зв'язку найбільш перспективними вважаються широкосмугові системи з шумоподібними дискретними сигналами і прямим розширенням спектра.

Залежно від способу формування і статистичних властивостей кодові послідовності, що використовуються в системах зв'язку з кодовим розділенням каналів, розподіляються на ортогональні, субортогональні (інша назва трансортогональні) і квазіортогональні.

Нехай $S_i = \left(\varphi_{i_0}, \varphi, ..., \varphi_{i_{n-1}}\right)$ – двійкова послідовність псевдовипадкових чисел ППВЧ (кодовий сигнал) з множини $\Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\}$ потужності $|S| = M$.

Елементи двійкової ППВЧ набувають одного зі значень

$$\Phi_{i_z} = \begin{cases} +1 \\ -1 \end{cases}, \; z = 0, ..., n-1.$$

Нормована періодична функція взаємної кореляції (ПФВК) характеризує відгук обладнання на періодичну послідовність сигналів, що відрізняється від очікуваного сигналу, і визначається з виразом

$$R_{i,j}^{\text{ПФВК}}(\ell) = \frac{1}{n}\left(\Phi_{i_0}\Phi_{j_{(\ell)\bmod(n)}} + \Phi_{i_1}\Phi_{j_{(\ell+1)\bmod(n)}} + \cdots + \Phi_{i_{n-1}}\Phi_{j_{(\ell+n-1)\bmod(n)}}\right) =$$

$$= \frac{1}{n}\sum_{z=0}^{n-1}\Phi_{i_z}\Phi_{j_{(\ell+z)\bmod(n)}}.$$

Нормована періодична функція автокореляції (ПФАК) характеризує відгук обладнання на періодичну послідовність очікуваних сигналів і визначається за виразом

$$R_{i,i}^{\text{ПФАК}}(\ell) = \frac{1}{n}\left(\Phi_{i_0}\Phi_{i_{(\ell)\bmod(n)}} + \Phi_{i_1}\Phi_{i_{(\ell+1)\bmod(n)}} + \cdots + \Phi_{i_{n-1}}\Phi_{i_{(\ell+n-1)\bmod(n)}}\right) =$$

$$= \frac{1}{n}\sum_{z=0}^{n-1}\Phi_{i_z}\Phi_{i_{(\ell+z)\bmod(n)}}.$$

Значення функцій кореляції за фіксованого $\ell = 0$ називають коефіцієнтом кореляції $\rho_{ij} = R_{i,j}^{\text{ПФВК}}(0)$, що загалом змінюється від –1 до +1.

Коефіцієнт взаємної кореляції ортогональних послідовностей за визначенням дорівнює нулю, тобто

$$\rho_{ij} = 0.$$

Невелике значення коефіцієнта взаємно кореляційної функції (ВКФ) забезпечують субортогональні (трансортогональні) коди, для яких

$$\rho_{ij} = \begin{cases} -1/N, \text{ де N непарне,} \\ -1/(\mathrm{N}-1), \text{ де N парне.} \end{cases} \quad (5)$$

За великих значень N різніцею між коефіцієнтами кореляції ортогональних і трансортогональних кодів можна практично з нехтувати.

Існує декілька способів генерації ортогональних кодів. Найбільш поширений – за допомогою послідовностей Уолша довжини 2^i. Вони утворюються на основі рядків матриці Адамара $\mathrm{H_i}$, що зі свого боку будуються за рекурентним правилом

$$\mathrm{H_i} = \begin{bmatrix} \mathrm{H_{i-1}} & \mathrm{H_{i-1}} \\ \mathrm{H_{i-1}} & -\mathrm{H_{i-1}} \end{bmatrix}, \ \mathrm{H_0} = [1].$$

Використовуючи наведене правило, отримаємо

$$\mathrm{H_1} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \ \mathrm{H_2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

$$\mathrm{H_3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Багаторазове повторення процедури дозволяє сформувати матрицю розміру 2^i, для якої характерна взаємна ортогональность всіх рядків і стовпців.

Такий спосіб формування сигналів реалізований в стандарті IS-95, де довжина послідовностей Уолша дорівнює 64. Відзнавали, що різниця між рядками матриці Адамара і послідовностями Уолша полягає лише в тому, що в останніх використовуються уніполярні сигнали вигляду $\{1,0\}$.

На прикладі матриці Адамара легко проілюструвати й принцип побудови трансортогональних кодів. Так, можна переконатися, що якщо з матриці викреслити перший стовпець, що складається з одних одиниць, то ортогональні коди Уолша трансформуються в трансортогональні, у яких для будь-яких двох послідовностей кількість несподівань символів перевищує кількість збігів рівно на одиницю. Отже, виконується рівняння (5).

Інший важливий різновид кодів – біортогональний код, що формується з ортогонального коду і його інверсії. Головна позитивна якість біортогональних кодів порівняно з ортогональними – можливість передачі сигналу в удвічі меншій смузі частот. Скажімо, біортогональний блоковий код, що використовується в WCDMA, дозволяє передавати сигнал транспортного формату TFI.

Відзначимо, що ортогональним кодам властиві два принципові недоліки.

1. Максимальна кількість можливих кодів обмежена їх довжиною (у стандарті IS-95 кількість кодів дорівнює 64), а відповідно, вони мають обмежений адресний простір.

2. Ще один недолік ортогональних кодів полягає в тому, що функція взаємної кореляції дорівнює нулю лише «в точці», тобто за браком тимчасового зсуву між кодами. Тому такі сигнали використовуються лише в синхронних системах і переважно в прямих каналах (від базової станції до абонента).

Прагнення підвищити абонентську місткість систем зв'язку з кодовим розділенням каналів неминуче призводить до використання великих ансамблів т. з. квазіортогональних сигналів, тобто великої множини таких псевдовипадкових послідовностей, коефіцієнт кореляції між якими дуже близький до нуля (майже ортогональні сигнали). Так, в проекті стандарту cdma2000 запропонований метод генерації квазіортогональних кодів шляхом множення послідовностей Уолша на спеціальну маскуючу функцію. Цей метод дозволяє за допомогою однієї такої функції отримати набір квазіортогональних послідовностей Quasi-Orthogonal Function Set (QOFS). За допомогою m маскуючих функцій і ансамблю кодів Уолша завдовжки 2n можна створити (m + 1) 2n QOF – послідовностей.

Псевдовипадкова послідовність (ПВП) – послідовність чисел, що була обчислена за деяким певним арифметичним правилом, але має всі властивості випадкової послідовності чисел в межах вирішуваного завдання.

Хоча псевдовипадкова послідовність в цьому розумінні частіше, ніж може здатися позбавлена закономірностей, проте будь-який псевдовипадковий генератор з кінцевою кількістю внутрішніх станів повториться після дуже довгої послідовності чисел.

Псевдовипадкова двійкова послідовність – окремий випадок ПВП, у якій елементи набувають двох можливих значень 0 та 1 (або –1 та +1).

Одне з перших формулювань деяких основоположних правил для статистичних властивостей періодичних псевдовипадкових послідовностей було надано Соломоном Голомбом.

Три основні правила здобули популярність як постулати Голомба:

1. Кількість «1» в кожному періоді повинна відрізнятися від кількості «0» не більше, ніж на одиницю;

2. У кожному періоді половина серій (з однакових символів) повинна мати довжину один, одна чверть повинна мати довжину два, одна восьма повинна мати довжину три тощо. Більш того, для кожної з цих довжин повинна бути однакова кількість серій з «1» та «0».

3. Припустимо, у нас є дві копії однієї й тієї ж послідовності періоду p, зсунуті один щодо одного на деяке значення d. Тоді для кожного d

$$0 <= d <= p - 1,$$

ми можемо підрахувати кількість узгодженостей між цими двома послідовностями Ad і кількість неузгодженостей Dd. Коефіцієнт автокореляції для кожного d визначається співвідношенням (Ad – Dd)/p, і ця функція автокореляції набуває різних значень у міру того, як d проходить всі допустимі значення.

Тоді для будь-якої послідовності, що задовольняє правилу 3, автокореляційна функція (АКФ) повинна набувати лише двох значень.

Правило 3 – це технічний вираз того, що Голомб описав як поняття незалежних випробувань: знання деякого попереднього значення послідовності в принципі не допомагає припущенням про поточне значення. Ще одна точка зору на АКФ: це певна міра здатності, що дозволяє розрізняти послідовність та її копію, але ту, що починається в деякій іншій точці циклу.

Послідовність, що задовольняє правилам 1–3 часто називають «псевдошумовою-послідовністю». До аналізованої послідовності застосовується широкий спектр різних статистичних тестів для дослідження того, наскільки добре вона узгоджується з допущенням, що для генерації використовувалося абсолютно випадкове джерело.

Методи розширення спектра для підвищення ефективності передачі дискретних повідомлень

В існуючих на сьогоднішній день системах передачі дискретних повідомлень використовуються два методи розширення спектру:

– *псевдовипадкова перебудова робочої частоти* (ППРЧ) (англ. FHSS – Frequency Hopping Spread Spectrum). Суть методу полягає в періодичній стрибкоподібній зміні частоти, що несе за деяким алгоритмом, відомим приймачу і передавачу. Перевага методу – простота реалізації. Метод використовується в Bluetooth;

– *розширення спектра методом прямої послідовності* (ПРС) (англ. DSSS – Direct Sequence Spread Spectrum). Метод за ефективністю перевищує ППРЧ, але складніший в реалізації. Суть методу полягає в підвищенні тактової частоти модуляції, водночас кожному символу переданого повідомлення відповідає деяка достатньо довга псевдовипадкова послідовність (ПВП). Метод використовується в таких системах, як CDMA і системах стандарту IEEE 802.11.

Розширення спектра псевдовипадковою перебудовою робочої частоти. Для того, щоб радіообмін не можна було перехопити або заглушити вузькосмуговим шумом, було запропоновано вести передачу з постійною зміною несучої частоти в межах широкого діапазону. В результаті потужність сигналу розподілялася по всьому діапазону, і прослуховування якоїсь певної частоти давало тільки невеликий шум. Послідовність несучих частот була псевдовипадковою, відомою тільки передавачу і приймачу. Спроба заглушення сигналу в якомусь вузькому діапазоні також не дуже погіршувала сигнал, оскільки заглушувалася тільки невелика частина інформації. Ідею цього методу ілюструє рис. 1.

Протягом фіксованого часу передача відбувається на незмінній несучій частоті. На кожній несучій частоті для передачі дискретної інформації застосовуються стандартні методи модуляції, такі як FSK або PSK. Для того, щоб приймач синхронізувався з передавачем для позначення початку кожного періоду передачі протягом деякого часу передаються синхробіти. Отже, корисна швидкість цього методу кодування виявляється меншою через постійні накладні витрати на синхронізацію.

Рис. 1. Розширення спектра стрибкоподібною перебудовою частоти

Несуча частота змінюється відповідно до номерів частотних підканалів, що виробляються алгоритмом псевдовипадкових чисел. Псевдо-

випадкова послідовність залежить від деякого параметра, що називають початковим числом. Якщо приймачу і передавачу відомі алгоритм і значення початкового числа, то вони змінюють частоти за однаковою послідовністю, що зветься послідовністю псевдовипадкової перебудови частоти.

Методи FHSS використовуються в бездротових технологіях IEEE 802.11 та Bluetooth. В FHSS підхід до використання частотного діапазону не такий як в інших методах кодування – замість економного витрачання вузької смуги робиться спроба зайняти весь доступний діапазон. На перший погляд це здається не дуже ефективним, адже в кожен момент часу в діапазоні працює тільки один канал. Проте останнє твердження не завжди справедливо – коди розширеного спектра можна використовувати і для мультиплексування декількох каналів в широкому діапазоні. Зокрема методи FHSS дозволяють організувати одночасну роботу декількох каналів шляхом вибору для кожного каналу таких псевдовипадкових послідовностей, щоб в кожен момент часу кожен канал працював на своїй частоті (звичайно, це можна зробити, якщо кількість каналів не перевищує кількості частотних підканалів).

Розширення спектра методом прямої послідовності

В методі прямого послідовного розширення спектра також використовується весь частотний діапазон, виділений для однієї лінії зв'язку. На відміну від методу FHSS весь частотний діапазон займається не за рахунок постійних перемикань з частоти на частоту, а за рахунок того, що кожен біт інформації замінюється N-бітами, так що тактова швидкість передачі сигналів збільшується в N разів. А це означає, що спектр сигналу також розширюється в N разів. Достатньо відповідним чином вибрати швидкість передачі даних і значення N, щоб спектр сигналу заповнив весь діапазон (рис. 2).

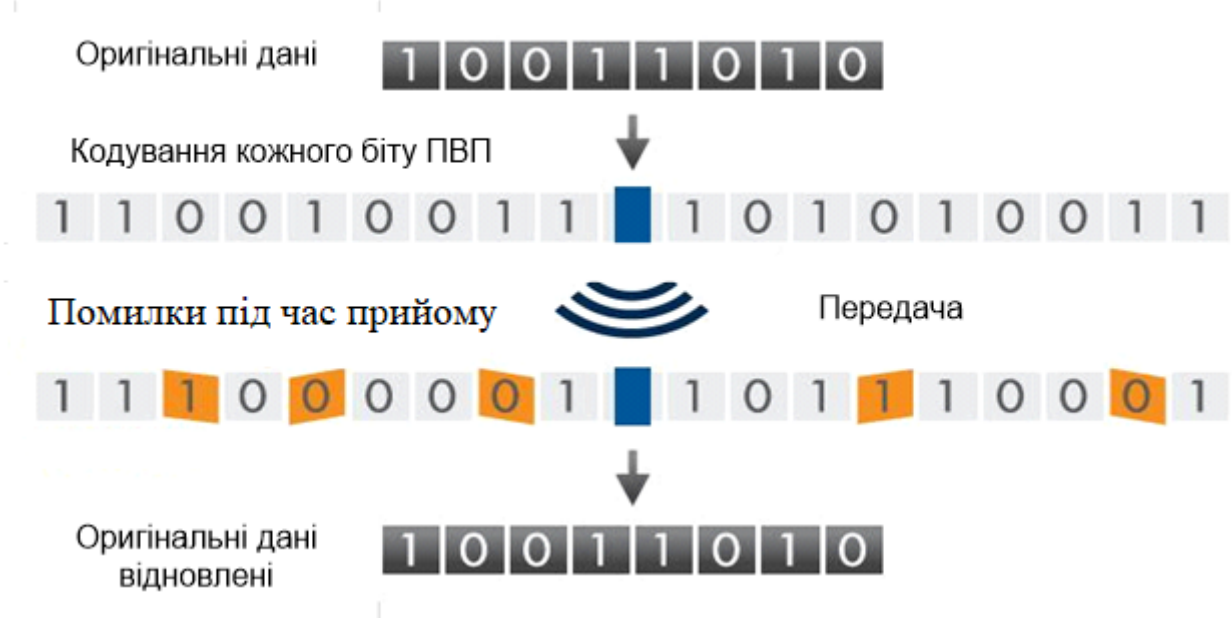


Рис. 2. Технологія кодового розподілення каналів CDMA

Для передачі даних в широкосмуговій системі зв'язку інформаційний сигнал $x(t)=\begin{cases}+1\\-1\end{cases}$ модулюється за допомогою його множення на розширюючий кодовий сигнал $g(t)=\Phi_i\in\Phi$ – псевдовипадкову послідовність з розглянутих вище ансамблів дискретних сигналів. Оскільки кодовий сигнал за своїми статистичними властивостями подібний до шуму, то отриманий розширений сигнал

$$y'(t)=y(t)+e(t) \tag{6}$$

не дуже відрізняться від шумів в каналі зв'язку, що і дозволяє здійснити приховану передачу.

Під час прийому в демодуляторі отриманий сигнал $y'(t)=y(t)+e(t)$ як суміш переданої послідовності $y(t)$ і подій в каналі зв'язку помилок $e(t)$ помножується на синхронізовану копію розширювального сигналу $g(t)$. Інакше кажучи, на приймальному боці здійснюється обчислення коефіцієнта кореляції, значення якого визначає правило ухвалення рішення

$$\rho\left(y'(t),g(t)\right)=\frac{1}{n}\sum_{z=0}^{n-1}x(t)\Phi_{i_z}\Phi_{i_z}+\frac{1}{n}\sum_{z=0}^{n-1}e(t)\Phi_{i_z}. \tag{7}$$

Враховуючи псевдовипадковість Φ_i, що використовується в якості $g(t)$, другим доданком в правій частині рівності можна знехтувати (кількість «+1» приблизно дорівнює кількості « -1»)

$$\rho\left(y'(t),g(t)\right)\approx\rho\left(y(t),g(t)\right)=x(t)\frac{1}{n}\sum_{z=0}^{n-1}\left(\Phi_{i_z}\right)^2=x(t), \tag{8}$$

тобто значення інформаційного сигналу на приймальному боці визначається згідно із виразом

$$x(t)=\begin{cases}+1, \text{ за } \rho\left(y'(t),g(t)\right)\approx+1;\\-1, \text{ за } \rho\left(y'(t),g(t)\right)\approx-1;\end{cases} \tag{9}$$

де знак «≈» припускає наявність помилок, що викликані природними або навмисними завадами в каналі зв'язку.

Структурна схема тракту прийому-передачі інформації з використанням прямого розширення спектра наведена на рис. 3.

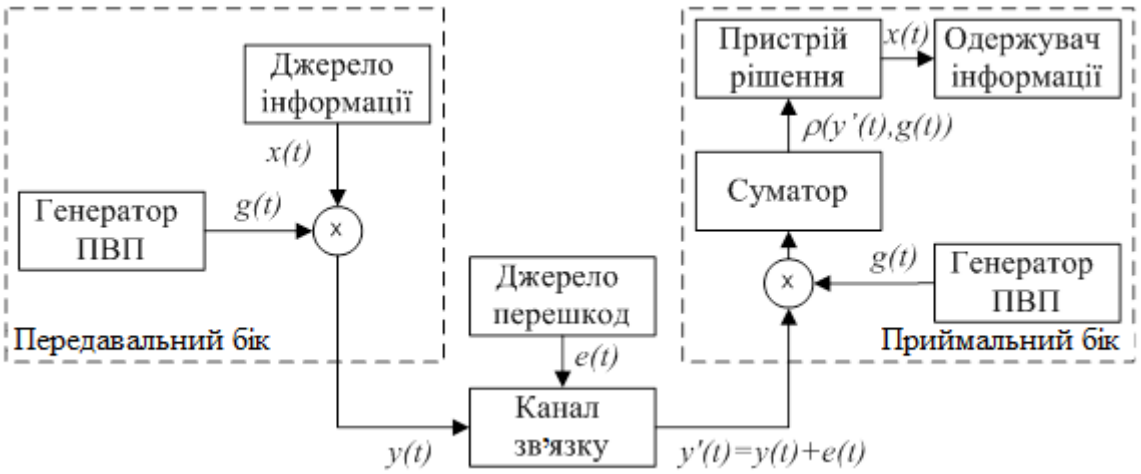


Рис. 3. Структурна схема тракту прийому-передачі інформації з використанням прямого розширення спектра

Припустимо, що часова тривалість немодульованого сигналу $x(t)$ дорівнює T, а його частота відповідно дорівнює $F(x(t)) = \frac{1}{T}$. Передача модульованого сигналу $y(t)$ за тієї ж часової тривалості T приведе до розширення частотного спектра переданого сигналу пропорційно кількості елементів псевдовипадкової послідовності, тобто пропорційно довжині n: $F(y(t)) = n\frac{1}{T} = nF(x(t))$. Проте використання прямого розширення спектра переданого сигналу забезпечує одночасну передачу багатьох інших інформаційних сигналів в тій же смузі частот. Це витікає із взаємної ортогональності (квазіортогональності) вживаних ансамблів дискретних сигналів. Дійсно, якщо на приймальному боці прийнята адитивна суміш $\sum_{\ell} y_1(t)$ декількох модульованих сигналів, тоді обчисленням коефіцієнта кореляції буде вираз

$$\rho\left(\sum_{\ell} y_{\ell}(t), g(t)\right) = \frac{1}{n}\sum_{\ell}\sum_{z=0}^{n-1} x_{\ell}(t)\Phi_{\ell_z}\Phi_{i_z}. \qquad (10)$$

Але всі послідовності з множини мають низьке значення взаємної кореляції, тобто за $\ell \neq i$ маємо $\rho(\Phi_{\ell}, \Phi_i) = 0$ (для ортогональних сигналів маємо рівність $\rho(\Phi_{\ell}, \Phi_i) = 0$. Отже, всіма доданками за $\ell \neq i$ в правій частині рівності (10) можна знехтувати. Звідси, за наявністю в адитивній суміші $\sum_{\ell} y_{\ell}(t)$ дискретного сигналу $\Phi_{\ell=i}$ маємо вираз (8) і відповідне правило ухвалення рішення (9).

Мета кодування методом DSSS та ж, що і методом FHSS – підвищення стійкості до завад. Вузькосмугова завада спотворюватиме тільки певні частоти спектру сигналу, тому приймач з великим ступенем імовірності зможе правильно розпізнати передану інформацію.

Код, яким замінюється двійкова одиниця початкової інформації, називається розширюючою послідовністю, а кожен біт такої послідовності – чіпом (елементарним сигналом). Відповідно, швидкість передачі результуючого коду називають чіповою швидкістю. Двійковий нуль кодується інверсним значенням розширюючої послідовності. Приймачі повинні знати розширюючу послідовність, яку використовує передавач, щоб зрозуміти передану інформацію.

Кількість бітів в розширюючій послідовності визначає коефіцієнт розширення початкового коду. Як і у разі FHSS для кодування бітів результуючого коду може використовуватися будь-який вид модуляції, наприклад BFSK.

Чим більшим є коефіцієнт розширення, тим ширшим спектр результуючого сигналу і вищим ступінь заглушення завад. Але водночас зростає займаний каналом діапазон спектра. Зазвичай коефіцієнт розширення має значення від 10 до 100.

Приклад. Дуже часто як значення розширюючої послідовності беруть послідовність Баркера (Barker), що складається з 11 бітів: 10110111000. Якщо передавач використовує цю послідовність, то передача трьох бітів 110 є причиною до передачі наступних бітів: 10110111000 10110111000 01001000111.

Послідовність Баркера дозволяє приймачу швидко синхронізуватися з передавачем, тобто надійно виявляти початок послідовності. Приймач визначає таку подію, по черзі порівнюючи отримувані біти зі зразком послідовності. Дійсно, якщо порівняти послідовність Баркера з такою ж послідовністю, але зсуненою на один біт вліво або вправо, ми отримаємо менше половини збігів значень бітів. Навіть під час спотворення декількох бітів з великою часткою імовірності приймач правильно визначить початок послідовності, а отже, зможе правильно інтерпретувати отримувану інформацію.

Перерахуємо деякі властивості сигналів з прямим розширенням спектра, що є найбільш важливими з погляду організації множинного доступу в системах зв’язку з пересувними об’єктами.

1. *Множинний доступ.* Якщо одночасно декілька абонентів використовують канал передачі, то в каналі одночасно є декілька сигналів з прямим розширенням спектра. У приймачі сигналу конкретного абонента здійснюється зворотна операція – згортання сигналу цього абонента шляхом використання того ж псевдовипадкового сигналу, що був використаний в передавачі цього абонента. Ця операція концентрує потужність широкосму-

гового сигналу, що приймається у вузькій смузі частот, яка дорівнює ширині спектра інформаційних символів. Якщо взаємна кореляційна функція між псевдовипадковими сигналами цього абонента і інших абонентів є достатньо малою, то під час когерентного прийому в інформаційну смугу приймача абонента потрапить лише незначна частина потужності сигналів решти абонентів. Сигнал конкретного абонента буде прийнятий правильно.

2. *Багатопроменева інтерференція.* Якщо псевдовипадковий сигнал, що використовується для розширення спектру має ідеальну автокореляційну функцію, значення якої поза інтервалом $[-t_0, +t_0]$ дорівнює нулю, і якщо сигнал, що приймається, і копія цього сигналу в іншому промені зміщені в часі на величину, велику $2t_0$, то під час згортання сигналу його копія може розглядатися як заважаюча інтерференція, що додає лише малу частину потужності до інформаційної смуги.

3. *Вузькосмугова завада*. У разі когерентного прийому в приймачі здійснюється множення прийнятого сигналу на копію псевдовипадкового сигналу, що використовується для розширення спектра в передавачі. Отже, в приймачі здійснюватиметься операція розширення спектра вузькосмугової завади, аналогічної тій, що виконувалася з інформаційним сигналом в передавачі. Отже, спектр вузькосмугової завади в приймачі буде розширений у B раз, де B – коефіцієнт розширення, тому в інформаційну смугу частот потрапить лише мала частка потужності завади, що у B раз менше початкової потужності завади.

4. *Імовірність перехоплення.* Оскільки сигнал з прямим розширенням спектра займає всю смугу частот системи протягом усього часу передачі, то його випромінювана потужність, що доводиться на 1 Гц смуги, матиме дуже малі значення. Отже, виявлення такого сигналу є дуже важким завданням.

Отже, перспективним напрямом в розвитку сучасних систем широкосмугового зв’язку з прямим розширенням спектра є розробка і дослідження методів синтезу великих ансамблів квазіортогональних дискретних сигналів з покращуваними ансамблевими, структурними і кореляційними властивостями.

Розглянутий підхід до організації цифрових завадозахисних каналів зв’язку застосовується під час побудови стеганографічних методів захисту інформації. Так, наприклад, розширення спектра прямою послідовністю використовується для створення стеганографічного методу вбудовування даних в нерухомі зображення. Розглянемо один з варіантів реалізації цього методу, авторами якого є Сміт (J. R. Smith) і Коміські (B. O. Comiskey), проведемо дослідження його ефективності з погляду забезпечуваної пропускної спроможності стеганографічного каналу зв’язку і стійкості, що досягається, до несанкціонованого вилучення інформаційних повідомлень.

Пряме розширення спектра в стеганографії

В методі Сміта-Коміські, як і в розглянутих вище системах зв'язку з прямим розширенням спектра, інформаційне повідомлення побітно модулюється шляхом множення на ансамбль ортогональних сигналів. Потім промодульоване повідомлення вбудовується в контейнер – нерухоме зображення.

Введемо деякі умовні позначення і математичні співвідношення, що за аналогією з розглянутими вище системами широкосмугового цифрового зв'язку дозволять досліджувати особливості побудови і інформаційного обміну даних в стеганосистемі.

Уявімо інформаційне повідомлення m, що підлягає вбудовуванню в цифровий контейнер-зображення, у вигляді блоків $\mathrm{m_i}$ рівної довжини, тобто $\mathrm{m} = (\mathrm{m}_0, \mathrm{m}_1, ..., \mathrm{m}_{\mathrm{N}-1})$, де кожен блок $\mathrm{m_i}$ – послідовність (вектор) з n біт

$$\mathrm{m_i} = (\mathrm{m}_{\mathrm{i}_0}, \mathrm{m}_{\mathrm{i}_1}, ..., \mathrm{m}_{\mathrm{i}_{n-1}}).$$

Контейнер-зображення розглядатимемо як масив даних C розмірністю $\mathrm{K} \cdot \mathrm{L}$, розбитий на підблоки розміром $k \cdot l = n$. Елементами масиву C можуть бути, наприклад, растрові дані використовуваного зображення.

Секретними ключовими даними є набір базисних функцій $\mathrm{Key} = \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{\mathrm{M}-1}\}$, де всі базисні функції $\Phi_\mathrm{i} = (\varphi_{\mathrm{i}_0}, \varphi_{\mathrm{i}_1}, ..., \varphi_{\mathrm{i}_{n-1}})$ – що взаємно ортогональні дискретні сигнали з довжиною, що дорівнює розміру блоку n повідомлення $\mathrm{m_i}$, тобто для будь-яких $\mathrm{i, j} \in [0, ..., \mathrm{M}-1]$ виконується рівність

$$\rho(\Phi_i, \Phi_j) = \frac{1}{n}\sum_{z=0}^{n-1} \Phi_{i_z} \Phi_{jz} = \begin{cases} +1, \text{за i = j;} \\ -1, \text{за } i \neq \text{j.} \end{cases}$$

Формальне графічне подання інформаційного повідомлення, контейнера-зображення і ключових даних наведене на рис. 6.

Метою стеганографічного перетворення інформації є вбудовування кожного окремого блоку повідомлення $\mathrm{m_i}$ у відповідний блок контейнера-зображення. В блок даних цифрового зображення розміром $\mathrm{K} \cdot \mathrm{L}$ елементів може бути вбудовано $K \cdot \frac{L}{n}$ блоків інформаційного повідомлення, тобто до $\mathrm{K} \cdot \mathrm{L}$ бітів.

Розбиття контейнера на блоки може бути довільним, проте, як показує практика, найбільш доцільним (менший на відміну від одновимірного уявлення чисельний розкид значень в блоці) є двовимірне розбиття, наведене на рис. 4. Як ключові дані (масиву базисних функцій $Key = \Phi$)

використаємо розглянуті вище ансамблі ортогональних дискретних сигналів Уолша–Адамара.

$$m = \begin{array}{|c|c|c|c|c|c|} \hline m_0 & m_1 & \dots & m_i & \dots & m_{N-1} \\ \hline \end{array}$$

$$\forall i:\ m_i = \begin{array}{|c|c|c|c|} \hline m_{i0} & m_{i1} & \dots & m_{in-1} \\ \hline \end{array}$$

$$N = K \cdot L / n$$

$$Key = \begin{array}{|c|c|c|c|c|c|} \hline \varphi_{00} & \varphi_{01} & \dots & \varphi_{0z} & \dots & \varphi_{0n-1} \\ \hline \varphi_{10} & \varphi_{11} & \dots & \varphi_{1z} & \dots & \varphi_{1n-1} \\ \hline \dots & \dots & \dots & \dots & \dots & \dots \\ \hline \varphi_{i0} & \varphi_{i1} & \dots & \varphi_{iz} & \dots & \varphi_{in-1} \\ \hline \dots & \dots & \dots & \dots & \dots & \dots \\ \hline \varphi_{n0} & \varphi_{n1} & \dots & \varphi_{nz} & \dots & \varphi_{nn-1} \\ \hline \end{array}$$

$$C = \begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline c_{0,0} & c_{0,1} & \dots & c_{0,k-1} & c_{0,k} & c_{0,k+1} & \dots & c_{0,2k-1} & \dots & c_{0,K-1} \\ \hline c_{1,0} & c_{1,1} & \dots & c_{1,k-1} & c_{1,k} & c_{1,k+1} & \dots & c_{1,2k-1} & \dots & c_{1,K-1} \\ \hline \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \hline c_{l-1,0} & c_{l-1,1} & \dots & c_{l-1,k-1} & c_{l-1,k} & c_{l-1,k+1} & \dots & c_{l-1,2k-1} & \dots & c_{l-1,K-1} \\ \hline c_{l,0} & c_{l,1} & \dots & c_{l,K-1} & c_{l,K} & c_{l,K+1} & \dots & c_{l,2k-1} & \dots & c_{l,K-1} \\ \hline c_{l,0} & c_{l,1} & \dots & c_{l,K-1} & c_{l,K} & c_{l,K+1} & \dots & c_{l+1,2k-1} & \dots & c_{l+1,K-1} \\ \hline \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \hline c_{2l-1,0} & c_{2l-1,1} & \dots & c_{2l-1,k-1} & c_{2l-1,k} & c_{2l-1,k+1} & \dots & c_{2l-1,2k-1} & \dots & c_{2l-1,K-1} \\ \hline \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \hline c_{L-1,0} & c_{L-1,1} & \dots & c_{L-1,k-1} & c_{L-1,k} & c_{L-1,k+1} & \dots & c_{L-1,2k-1} & \dots & c_{L-1,K-1} \\ \hline \end{array}$$

Рис. 4. Формальне подання інформаційного повідомлення, контейнера-зображення і ключових даних

Вбудовування інформаційного повідомлення здійснюється так. Кожен блок повідомлення $m_{i_j}, j = 0,...,n-1$ зіставляється з окремим блоком контейнера-зображення. Кожен інформаційний біт блоку $m_{i_j}, j = 0,...,n-1$ подається у вигляді інформаційного сигналу $\mathrm{m_{i_j}(t)} = \begin{cases} +1, \mathrm{m_{i_j}} = 1; \\ -1, \mathrm{m_{i_j}} = 0; \end{cases}$ і за аналогією з (6) модулюється розширюючим кодовим сигналом (базисними функціями), тобто ПВП $\Phi_j \in \Phi$.

В результаті, для кожного інформаційного блоку формується модульований інформаційний сигнал

$$E_i(t) = \sum_{j=0}^{n-1} \sum_{z=0}^{n-1} m_{i_j}(t) \Phi_{j_z}. \tag{11}$$

Отриманий блок повідомлення $\mathrm{E_i}$ попіксельно підсумовується з підблоком контейнера.

Позначимо блоки контейнера у такий спосіб (див. рис. 4)

$$\mathrm{C_0} = \begin{pmatrix} \mathrm{c_{0,0}} & \mathrm{c_{0,1}} & \dots & \mathrm{c_{0,k-1}} \\ \mathrm{c_{1,0}} & \mathrm{c_{1,1}} & \dots & \mathrm{c_{1,k-1}} \\ \dots & \dots & \dots & \dots \\ \mathrm{c_{\ell-1,0}} & \mathrm{c_{\ell-1,1}} & \dots & \mathrm{c_{\ell-1,k-1}} \end{pmatrix}, \mathrm{C_1} = \begin{pmatrix} \mathrm{c_{0,k}} & \mathrm{c_{0,k+1}} & \dots & \mathrm{c_{0,2k-1}} \\ \mathrm{c_{1,k}} & \mathrm{c_{1,k+1}} & \dots & \mathrm{c_{1,2k-1}} \\ \dots & \dots & \dots & \dots \\ \mathrm{c_{\ell-1,k}} & \mathrm{c_{\ell-1,k+1}} & \dots & \mathrm{c_{\ell-1,2k-1}} \end{pmatrix}, \dots,$$

$$\mathrm{C_{N-1}} = \begin{pmatrix} \mathrm{c_{L-l-1,K-k-1}} & \mathrm{c_{L-l-1,K-k}} & \dots & \mathrm{c_{L-l-1,K-1}} \\ \mathrm{c_{L-l,K-k-1}} & \mathrm{c_{L-l,K-k}} & \dots & \mathrm{c_{L-l,K-1}} \\ \dots & \dots & \dots & \dots \\ \mathrm{c_{L-1,K-k-1}} & \mathrm{c_{l-1,k+1}} & \dots & \mathrm{c_{L-1,K-1}} \end{pmatrix}.$$

Відповідні модульовані інформаційні сигнали $\mathrm{E_i(t)}$ подамо у вигляді двовимірного масиву даних

$$\mathrm{E_i} = \begin{pmatrix} \mathrm{E_{i_0}} & \mathrm{E_{i_1}} & \dots & \mathrm{E_{i_{k-1}}} \\ \mathrm{E_{i_k}} & \mathrm{E_{i_{k+1}}} & \dots & \mathrm{E_{i_{2k-1}}} \\ \dots & \dots & \dots & \dots \\ \mathrm{E_{i_{(\ell-1)(k-1)-k+1=n-k+1}}} & \mathrm{E_{i_{(\ell-1)(k-1)-k+2=n-k+2}}} & \dots & \mathrm{E_{i_{(\ell-1)(k-1)=n-1}}} \end{pmatrix}, \mathrm{i} = 0,..., \mathrm{N}-1.$$

Тоді стеганограма (заповнений контейнер) формується за допомогою об'єднання масивів даних $\mathrm{S_i}$, $\mathrm{i} = 0,..., \mathrm{N}-1$

$$S_i = C_i + E_i \cdot G, \tag{12}$$

де $\mathrm{G} > 0$ – коефіцієнт посилення розширюючого сигналу, що задає «енергію» вбудованих біт інформаційної послідовності.

Отже, заповнений контейнер S утворюється зі сформованих блоків S_i, $i = 0,..., N-1$ за допомогою їх об'єднання як це показано на рис. 4 для початкового (порожнього) контейнера *C*.

На етапі вибудовування даних немає необхідності володіти інформацією про первинний контейнер *C*. Операція декодування полягає у відновленні прихованого повідомлення шляхом проектування кожного блоку S_i, отриманого стеганозображення S на всі базисні функції $\Phi_j \in \Phi$, $i = 0,..., N-1$. Для цього кожен блок S_i подається у формі вектора $S_i = (S_{i_0}, S_{i_1}, ..., S_{i_{n-1}}),\ i = 0,..., N-1.$

Щоб витягнути j-й біт повідомлення з i-го блоку стеганозображення, необхідно обчислити коефіцієнт кореляції між Φ_j і прийнятим блоком S_i (поданим у вигляді вектора)

$$\rho(S_i, \Phi_j) = \frac{1}{n}\sum_{z=0}^{n-1} S_{i_z}\Phi_{j_z} = G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{i_z}\Phi_{j_z} + \frac{1}{n}\sum_{z=0}^{n-1} C_{i_z}\Phi_{j_z}, \qquad (13)$$

де під C_i розуміється одновимірний масив, тобто відповідний блок контейнера, поданий у формі вектора.

Припустимо, що масив C_i має випадкову статистичну структуру, тобто другий доданок в правій частині виразу (13) прямує до нуля, і ним можна знехтувати. Тоді маємо

$$\rho(S_i, \Phi_j) \approx G \cdot E_i \cdot \Phi_j = G \cdot \sum_{l=0}^{n-1}\sum_{z=0}^{n-1} m_{i_x}(t) \cdot \Phi_{l_z}\Phi_{j_z}. \qquad (14)$$

За аналогією з (10) відзначимо, що всі послідовності з множини Φ взаємно ортогональні, тобто за $l \neq j$ маємо $\rho(\Phi_i, \Phi_j) = 0$. Отже, всіма доданками в правій частині рівності (14) за $l \neq j$ можна знехтувати. Звідси маємо

$$\rho(S_i, \Phi_j) \approx G \cdot m_{i_j}(t) \cdot \frac{1}{n}\sum_{z=0}^{n-1}(\Phi_{j_z})^2 = G \cdot m_{i_j}(t). \qquad (15)$$

Згідно з правилом виділення корисного сигналу

$$x(t) = \begin{cases} \text{«1», за } polarity > 0; \\ \text{«0», за } polarity < 0; \\ \text{сторонній сигнал, за } polarity = 0, \end{cases} \qquad (16)$$

значення $m_{i_j}(t)$ можуть бути легко відновлені за допомогою знакової функції (polarity – полярність піка кореляційної функції).

Оскільки $G > 0$ і $n > 0$ знак $\rho(S_i, \Phi_j)$ в (15) залежить тільки від $m_{i_j}(t)$, звідки маємо

$$m_{i_j}(t) = sign\left(\rho\left(S_i, \Phi_j\right)\right) = \begin{cases} -1, \text{за } \rho\left(S_i, \Phi_j\right) < 0; \\ +1, \text{за } \rho\left(S_i, \Phi_j\right) > 0; \\ ?, \text{за } \rho\left(S_i, \Phi_j\right) = 0; \end{cases} \quad (17)$$

Якщо $\rho(S_i, \Phi_j) = 0$ в (17) вважатимемо, що вбудована інформація була втрачена.

Структурна схема вбудовування інформації в контейнер-зображення з використанням прямого розширення спектра для прихованої передачі повідомлень подається на рис. 5.

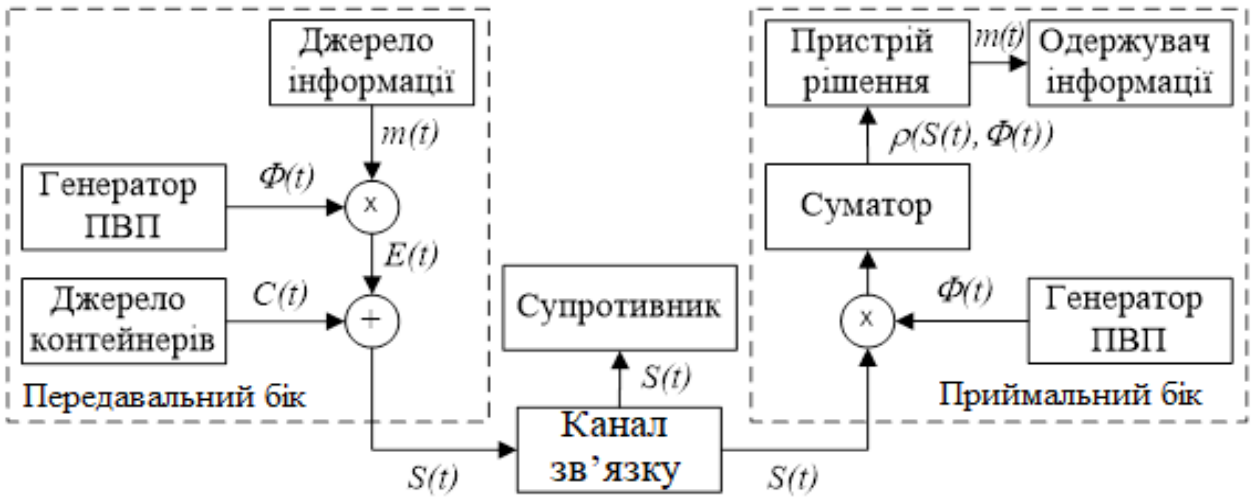


Рис. 5. Структурна схема вбудовування інформації в контейнер-зображення для прихованої передачі повідомлень

Рис. 5. показує, що процес вбудовування інформаційних повідомлень для прихованої передачі дуже схожий на процес розширення спектра дискретних сигналів в системах зв'язку (див. рис. 3). Поелементне складання модульованого повідомлення $E(t)$ з контейнером-зображенням $C(t)$ (див. вираз (12)) слід інтерпретувати як накладання помилок $e(t)$ на корисний сигнал в каналі зв'язку $y(t)$. Завдання вибудовування повідомлення $m(t)$ з $S(t)$ на приймальному боці стеганосистеми еквівалентно завданню детектування $x(t)$ з суміші корисного сигналу і завади $y'(t) = y(t) + e(t)$ в широкосмуговій системі зв'язку. Інакше кажучи, розглянута стеганосистема успадковує всі переваги широкосмугових систем зв'язку: стійкість до несанкціонованого добування вбудованих повідомлень (аналог прихованості в системі зв'язку), стійкість до руйнування або модифікації вбудованих повідомлень (аналог завадозахисту), стійкість до нав'язування помилкових повідомлень (аналог імітостійкості в системі зв'язку).

Отже, використання прямого розширення спектра дискретних сигналів дозволяє здійснити вбудовування інформаційних даних в нерухомі

зображення для прихованої передачі і реалізувати у такий спосіб, стеганографічний захист інформації.

Оцінка ефективності стеганосистеми

Під ефективністю технічної системи в широкому сенсі розуміють відповідність результату виконання деякої операції потрібному параметру. Водночас технічна система є засобом реалізації досліджуваної операції.

Стосовно цього процесу стеганографічна система є технічним засобом реалізації операції, метою якої є приховання від супротивника факту здійснення приховоної передачі інформації. отже, з урахуванням функціонального призначення стеганосистеми, введемо такі показники ефективності.

1. Пропускна спроможність – відношення об'єму V вбудованої в контейнер інформації до загального об'єму D контейнера

$$Q = \frac{V}{D}. \tag{18}$$

2. Об'єм ключових даних (у бітах)

$$\ell_{Key} = \log_2(|Key|), \tag{19}$$

де $|Key|$ – потужність множини ключових даних.

3. Стійкість стеганографічного методу оцінюватимемо як величину, зворотну потужності множини секретних ключових даних. Її можна тлумачити як імовірнісний показник підбору секретного ключа

$$W = \frac{1}{|Key|} = 2^{-l_{Key}}. \tag{20}$$

4. Величина спотворень, що вносяться, – як процентне співвідношення середньоарифметичного всіх абсолютних значень Δ – змін даних контейнера до максимально можливого значення Δ_{max}

$$I = \frac{\Delta_{ср}}{\Delta_{max}} \cdot 100 = \frac{100}{\Delta_{max} \cdot D} \cdot \sum_{i=1}^{D} |\Delta_i|, \tag{21}$$

де Δ_i – Δ-зміни i-го елемента контейнера.

5. Імовірність помилкового вибудовування інформаційних даних повідомлення

$$P_{ош} = \lim_{D\to\infty} \frac{V_{ош}}{D} = 1 - \lim_{D\to\infty} \frac{V - V_{ош}}{D}, \tag{22}$$

де $V_{ош}$ – об'єм помилково вибудованих даних.

Використовуючи (18) – (22), оцінимо ефективність розглянутого стеганографічного методу захисту інформації.

1. *Пропускна спроможність.* На кожен n-елементний блок S_i заповненого контейнера (стеганограми) припадає n-бітовий вектор вбудованого повідомлення m_i (див. вирази (11) (12)). Отже, $Q = \frac{1}{B}$, де B – об'єм даних, що припадає на один елемент контейнера. Для випадку вбудовування в растрові дані зображення (колірна модель R, G, B) з 8-бітовим кодуванням кожного кольору маємо $B = 8$ і $Q = \frac{1}{8}$.

2. *Об'єм ключових даних.* Ключовими даними є ансамбль дискретних сигналів, утворений рядками матриці Адамара порядку *n.* Отже, під множиною ключових даних слід розуміти множину різних (неізоморфних) матриць Адамара, кожна з матриць задає ансамбль дискретних сигналів. В таблиці 1 наведені деякі оцінки потужності M_A цієї множини.

Таблиця 1

Кількість ансамблів дискретних сигналів Уолша–Адамара

n	M_A
64	19
100	1
256	54
512	102
1024	162
2000	9
4000	16
10000	10

Наведені оцінки потужності M_A дають оцінку кількості ансамблів дискретних сигналів Уолша–Адамара, тобто оцінку потужності нееквівалентних ключів стеганосистеми. Отже, об'єм ключових даних оцінюється як $l_{key} = \log_2(M_A)$.

3. *Імовірність підбору секретного ключа* $W = (M_A)^{-1}$.

4. Для оцінки *величини спотворень, що вносяться,* скористаємось виразом (12). Другий доданок в правій частині (12) визначає величину Δ-змін елементів даних контейнера. Співмножник E_i формується в результаті підсумовування n дискретних сигналів (що набувають значення ± 1) з відповідними полярностями (що задаються $m_{i_j}(t)$). Отже, всі елементи E_i набуватимуть значень в діапазоні $[-n,...,+n]$, а відповідні Δ-зміни елементів контейнера не перевищуватимуть $|\Delta_i| \le n \cdot G.$ Звідки маємо верхню оцінку величини спотворень, що вносяться: $I = \frac{\Delta_{cp}}{\Delta_{max}} \cdot 100 \le \frac{n \cdot G}{\Delta_{max}} \cdot 100$. (23)

Для випадку вбудовування в растрові ці зображення (колірна модель R, G, B) з 8-бітовим кодуванням кожного кольору і використанням дискретних сигналів з $n = 256$ навіть за $G = 1$ спотворення, що вносяться, можуть досягати 100 %. Знизити спотворення, що вносяться, можна за рахунок скорочення кількості вбудованих біт даних m_{i_j} (зменшивши число доданків в (11)), що неминуче призведе до зниження пропускної спроможності стеганографічного каналу зв'язку.

5. *Імовірність помилкового добування.* Добування інформаційного повідомлення, також як і під час організації завадозахисного зв'язку (див. (6) – (9)), здійснюється кореляційним способом (див. (12) – (15)). Отже, помилка добування відбудеться під час зміни знака коефіцієнта кореляції $\rho(S_i, \Phi_j)$ у виразі (17).

Подамо коефіцієнт $\rho(S_i, \Phi_j)$ у вигляді

$$\rho(S_i, \Phi_j) = \rho(C_i + E_i \cdot G, \Phi_j) = \rho(C_i, \Phi_j) + \rho(E_i \cdot G, \Phi_j).$$

Останній доданок не змінює знак $\rho(S_i, \Phi_j)$, подія $\rho(S_i, \Phi_j) = \rho(E_i \cdot G, \Phi_j)$ відповідає безпомилковому добуванню повідомлення (див. (16) і (17)).

Отже, помилка добування інформаційного біту m_{i_j} повідомлення відбудеться у разі події

$$\left|\rho(C_i, \Phi_j)\right| > \rho\left|E_i \cdot G, \Phi_j\right| = \left|G \cdot m_{i_j}\right| = G, \qquad (24)$$

тобто якщо абсолютне значення коефіцієнта кореляції, що був використаний для вбудовування біту m_{i_j} дискретного сигналу Φ_j з блоком контейнеру C_i, в який цей біт вбудовується, перевершить коефіцієнт посилення G.

Отже, напишемо

$$P_{ош} = P\left(\left|\rho(C_i, \Phi_j)\right| > G\right)$$

де $P(x)$ – імовірність випадкової події x.

Інакше кажучи, правильне добування вбудованого повідомлення є випадковою подією, імовірність $P_{б.ош}$ якої безпосередньо пов'язана із статистичними властивостями використовуваного контейнера-зображення. Для безпомилкового добування повідомлення

$$P_{ош} = 0, P_{б.ош} = 1 - P_{ош} = 1, \qquad (25)$$

слід прагнути до взаємної ортогональності окремих фрагментів зображення C_i і використовуваних як секретні ключі дискретних сигналів Φ_j.

В цьому випадку подія

$$\left|\rho(C_i, \Phi_j)\right| = 0 < G$$

для всіх $i = 0, ..., N-1$ є достовірним і виконується (25).

В той же час, як показали експериментальні дослідження, коефіцієнт кореляції зазвичай значно більше за нуль $\left|\rho(C_i, \Phi_j)\right| >> 0$, і дуже часто виникає подія (24). Річ у тому, що елементи дискретних сигналів $\Phi_j \in \Phi$ набувають значення $\begin{cases} +1 \\ -1 \end{cases}$, а відповідний нормований коефіцієнт кореляції $\rho(\Phi_i, \Phi_j)$ за абсолютним значенням не перевищує довжини n послідовності і перебуває в діапазоні $[0,...,1]$, звідки власне і маємо умову (24).

Проте елементи контейнера C_i набувають значення з числового поля $[0,..., Y]$, розмірність якого задається способом кодування даних зображення. Наприклад, під час вбудовування інформації в растрові ці зображення (колірна модель R, G, B) з 8-бітовим кодуванням кожного кольору відповідні C_i набувають значення з діапазону цілих чисел $[0,...,255]$. Інакше кажучи, значення нормованого щодо n коефіцієнту кореляції $\left|\rho(C_i, \Phi_j)\right|$ перебуватиме в діапазоні $\left[0,...,Y\right]$, і для безпомилкового добування всіх біт повідомлення (24) необхідно буде виконати умову $G > Y$.

Як показали дослідження підвищення G веде до неминучого зростання обсягу спотворень (23), що вносяться. У разі $I > 2...3\ \%$ (поріг зорової чутливості людини) вони стають помітні сторонньому спостерігачу, що компрометує стеганоканал і робить неможливим використання розглянутої стеганосистеми.

Отже, під час досліджень виявлені суперечності, які є основою розробки і використання стеганографічних систем з розширенням спектра дискретних сигналів:

– імовірність правильного добування вбудованих даних $P_{б.ош}$ залежить від величини спотворень I, що вносяться;

– обсяг спотворень I, що вносяться, залежить від об'єму вбудованих біт даних, тобто від пропускної спроможності стеганоканалу Q;

– імовірність правильного добування вбудованих даних $P_{б.ош}$ безпосередньо залежить від статистичних властивостей використовуваного контейнера-зображення.

В результаті проведених експериментів отримано емпіричні оцінки:

– залежності величини спотворень I, що вносяться, від пропускної спроможності Q стеганоканалу;

– залежності величини спотворень I, що вносяться, і частоти помилок добування $P^{*}_{ош} \approx P_{ош}$ від коефіцієнта посилення G;

– залежності величини спотворень I, що вносяться, від частоти помилок добування $P^{*}_{ош} \approx P_{ош}$.

Дослідження проводилися під час вбудовування інформаційних даних в растрові дані зображення (колірна модель R, G, B) з 8-бітовим кодуванням кожного кольору. Отримані емпіричні залежності наведені на рис. 6–9.

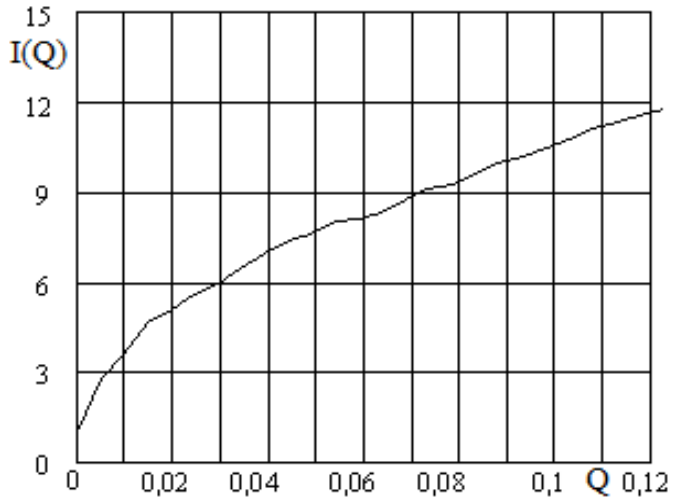


Рис. 6. Залежність I(Q)

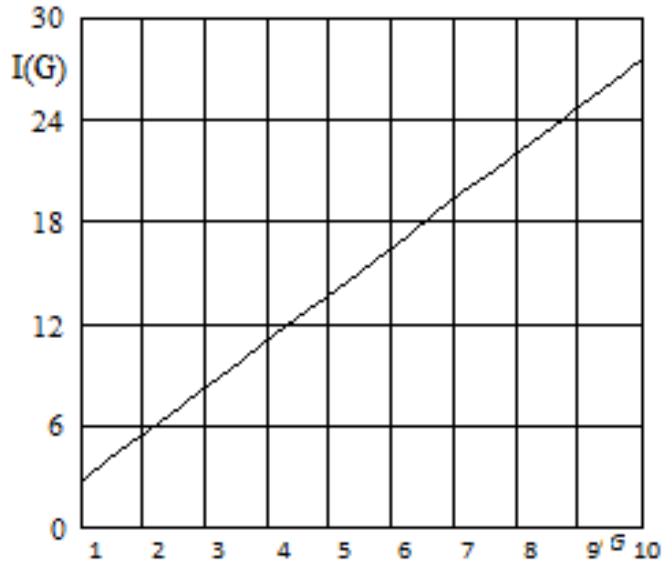


Рис. 7. Залежність $I(G)$ за $Q = 0{,}005$

Аналіз експериментально отриманих залежностей підтверджує зроблені раніше висновки. Якщо результати експерименту збігаються з теоретичними міркуваннями, це свідчить про достовірність отриманих результатів.

З наведеної на рис. 6 залежності виходить, що підвищення пропускної спроможності стеганоканалу веде до різкого збільшення спотворень, що вносяться до контейнера-зображення. Непомітні для стороннього спостерігача спотворення (що перебувають нижче порогу чутливості зорової системи людини) вносяться лише за $Q \le 0{,}005$. Це відповідає вбудовуванню не більше 10 бітів в один блок зображення, тобто модуляції до десяти інформаційних сигналів $m_{i_j}(t)$, $j = 0, ..., 9$ у виразі (6.11).

Залежності, наведені на рис. 7, 8 свідчать, що коефіцієнт посилення, що був використаний у виразах (12) – (14) дозволяє істотно знизити ймовірність помилкового добування інформацій них даних. На жаль, це досягається за рахунок різкого підвищення спотворень, що вносяться до контейнера-зображення. Залежності отримано за $Q = 0{,}005$. Очевидно, що для такої величини пропускної спроможності коефіцієнт посилення не може перевишувати 1 .. 1,5 (див. рис. 7). Проте навіть для таких значень ймовірність помилкового добування велика і знаходиться в діапазоні 0,1 .. 0,5.

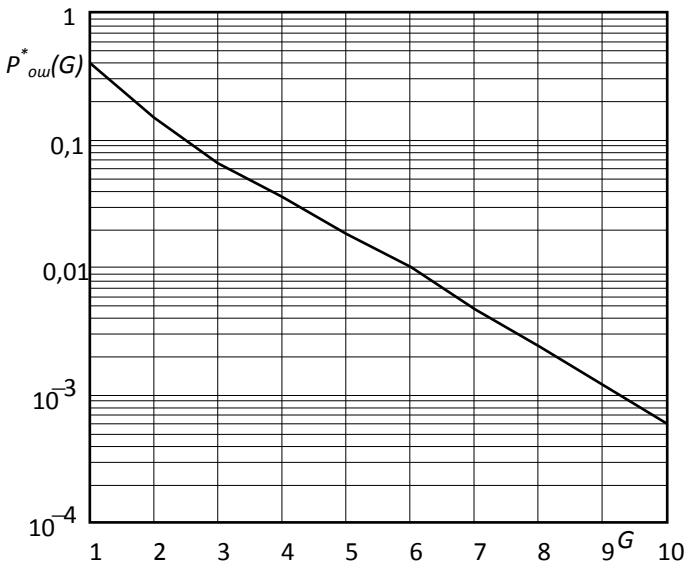


Рис. 8. Залежність $P^*_{ош}(G)$ за $Q = 0{,}005$

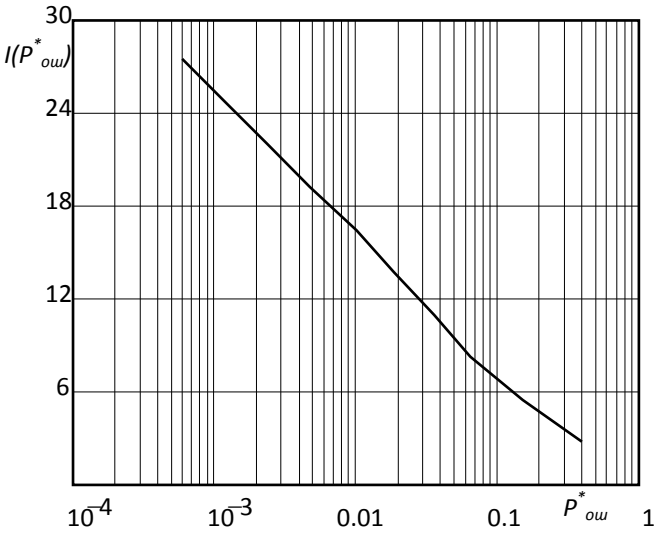


Рис. 9. Залежність $I(P^*_{ош})$ за $Q = 0{,}005$

Інтегральна залежність $I(P^*_{ош})$, що наведена на рис. 9, узагальнює приведені на рис. 7, 8 дані. Для фіксованої пропускної спроможності $Q = 0{,}005$ отримано емпіричну криву, яка характеризує залежність величини спотворень, що вносяться до контейнера-зображення та ймовірність помилкового добування інформаційних даних. Для $Q = 0{,}005$ домогтися низьких спотворень, які знаходяться нижче порогу зорової чутливості людини ($I \le 2\ldots3\,\%$), можна тільки за дуже високої імовірності помилкового добування інформаційних даних ($P_{ош} \ge 0{,}1$). Очевидно, що практичне застосування подібних стеганосистем необхідно поєднувати з завадостійким кодуванням інформаційних даних, що дозволить істотно знизити $P_{ош}$.

В результаті проведених досліджень показано, що використання в стеганографічних цілях прямого розширення спектру дискретних сигналів дозволяє здійснити приховане вбудовування інформаційних повідомлень в нерухомі зображення. Завдання добування повідомлення на приймальному боці стеганосистеми еквівалентне завданню виявлення інформації з суміші корисного сигналу і завади в широкосмуговій системі зв'язку.

Під час дослідження виявлені такі недоліки стеганографічних систем з розширенням спектра дискретних сигналів: імовірність правильного добування вбудованих даних залежить від обсягу спотворень, що вносяться, яка зі свого боку залежить від забезпечуваної пропускної спроможності стеганоканалу. Інакше кажучи, практична побудова стеганосистеми пов'язана з пошуком компромісу між обсягом спотворень, що вносяться, ймовірністю правильного добування повідомлення на приймальному боці і забезпечуваною пропускною спроможністю. Крім того, під час досліджень встановлено, що імовірність правильного добування вбудованих

даних безпосередньо залежить від статистичних властивостей контейнера-зображення, що використовується.

4. ПИТАННЯ ДЛЯ ПОТОЧНОГО КОНТРОЛЮ ПІДГОТОВЛЕНОСТІ СТУДЕНТІВ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ

1. Методи розширення спектра, які застосовуються для завадозахищеної передачі повідомлень. Переваги систем зв'язку з розширеним спектром.

2. Пряме розширення спектра в системах зв'язку. Кодовий розподіл каналів. Використання ортогональних дискретних сигналів в системах CDMA.

3. Матриці Адамара. Формування ортогональних дискретних сигналів Уолша–Адамара. Ансамблеві та кореляційні властивості сигналів Уолша–Адамара.

4. Кореляційний прийом дискретних сигналів. Структурна схема та математична модель системи зв'язку з кореляційним прийомом дискретних сигналів.

5. Метод приховування даних у просторовій сфері нерухомих зображень на основі прямого розширення спектра. Використання ансамблів ортогональних дискретних сигналів Уолша–Адамара в якості таємного ключа для приховування даних.

6. Структурна схема та математична модель стеганографічної системи з приховуванням даних у просторовій сфері нерухомих зображень на основі прямого розширення спектру. Вилучення вбудованих даних за допомогою кореляційного приймача дискретних сигналів.

7. Квазіортогональні дискретні сигнали. Похідні ортогональні сигнали. Застосування квазіортогональних дискретних сигналів для побудови ефективних стеганографічних систем.

8. Ймовірнісні властивості методу приховування даних у просторовій сфері нерухомих зображень на основі прямого розширення спектра, залежності ймовірності правильного вилучення даних та частки внесених при цьому похибок до контейнера-зображення. Додаткові вимоги до ансамблів дискретних сигналів, що застосовуються в стеганографічному перетворенні.

9. Адаптоване до властивостей контейнера формування квазіортогональних дискретних сигналів. Приховування та вилучення даних із адаптовано сформованих квазіортогональних дискретних сигналів, їх вплив на ймовірність правильного вилучення даних та частку внесених при цьому похибок до контейнера-зображення.

5. ІНСТРУКЦІЯ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ

Завдання 1. Реалізація алгоритмів формування ансамблів ортогональних дискретних сигналів Уолша–Адамара та алгоритмів кодування інформаційних бітів даних складними дискретними сигналами

1.1. Завантажуємо вихідні дані: контейнер – нерухоме зображення (в форматі *.bmp24); інформаційне повідомлення – текстовий документ (у форматі *.txt). Для цього в середовищі MathCAD виконуємо дії, аналогічні п. 1.1. інструкції до лабораторної роботи № 1.

1.2. Перетворюємо масив інформаційних даних. Для цього в середовищі MathCAD виконуємо дії, аналогічні п. 1.2. інструкції до лабораторної роботи.

1.3. Реалізуємо алгоритм формування матриць Адамара. Для цього скористаємося такою процедурою

$H_0 := (1)$

```
H := for i ∈ 1..8
       F ← H_(i-1)
       for j ∈ 0..rows(F) - 1
         for jj ∈ 0..cols(F) - 1
           a ← F_(jj,j)
           F1_(jj,j) ← a
       for j ∈ 0..rows(F) - 1
         for jj ∈ 0..cols(F) - 1
           a ← F_(jj,j)
           F1_(jj+cols(F),j) ← a
       for j ∈ 0..rows(F) - 1
         for jj ∈ 0..cols(F) - 1
           a ← F_(jj,j)
           F1_(jj,j+rows(F)) ← a
       for j ∈ 0..rows(F) - 1
         for jj ∈ 0..cols(F) - 1
           a ← F_(jj,j)
           F1_(jj+cols(F),j+rows(F)) ← -a
       H_i ← F1
     H
```

Процедура ітеративно формує матриці Адамара H_1, H_2, …, H_8. Матриця H_0, що складається з одного елемента, задається в якості початкового значення ітеративної процедури. Решта матриць формуються згідно із рекурентним правилом

$$H_i = \begin{pmatrix} H_{i-1} & H_{i-1} \\ H_{i-1} & -H_{i-1} \end{pmatrix}.$$

Результатом виконання процедури є масив матриць H, кожний елемент якого є матрицею Адамара

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

$H_8 =$

	0	1	2	3	4	5	6	7	8	9
0	1	1	1	1	1	1	1	1	1	1
1	1	-1	1	-1	1	-1	1	-1	1	-1
2	1	1	-1	-1	1	1	-1	-1	1	1
3	1	-1	-1	1	1	-1	-1	1	1	-1
4	1	1	1	1	-1	-1	-1	-1	1	1
5	1	-1	1	-1	-1	1	-1	1	1	-1
6	1	1	-1	-1	-1	-1	1	1	1	1
7	1	-1	-1	1	-1	1	1	-1	1	-1
8	1	1	1	1	1	1	1	1	-1	-1
9	1	-1	1	-1	1	-1	1	-1	-1	1
10	1	1	-1	-1	1	1	-1	-1	-1	-1
11	1	-1	-1	1	1	-1	-1	1	-1	1
12	1	1	1	1	-1	-1	-1	-1	-1	-1
13	1	-1	1	-1	-1	1	-1	1	-1	1
14	1	1	-1	-1	-1	-1	1	1	-1	-1
15	1	-1	-1	1	-1	1	1	-1	-1	...

1.4. Реалізуємо алгоритм формування ансамблів ортогональних дискретних сигналів Уолша–Адамара. Для цього сформуємо масив рядків матриці Адамара, де кожен елемент сформованого у такий спосіб масиву є дискретним сигналом Уолша–Адамара

$$\text{ArrayFunction} := \left| \begin{array}{l} \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} \text{for } j \in 0..255 \\ \quad a_j \leftarrow \left(H_8\right)_{i,j} \\ \quad \text{ArrayFunction}_i \leftarrow a \end{array} \right. \\ \text{ArrayFunction} \end{array} \right.$$

Розглянемо, як приклад, кілька дискретних сигналів

$\text{ArrayFunction}_5 =$

	0
0	1
1	-1
2	1
3	-1
4	-1
5	1
6	-1
7	1
8	1
9	...

$\text{ArrayFunction}_{45} =$

	0
0	1
1	-1
2	1
3	-1
4	-1
5	1
6	-1
7	1
8	-1
9	...

1.5. Реалізуємо алгоритм кодування інформаційних бітів даних складними дискретними сигналами. Для цього сформуємо модульоване інформаційне повідомлення, для чого перетворимо масив інформаційних бітів в масив, що складається з «1» і «–1» за такою процедурою

```
m := | for i ∈ 0.. rows(M_b) − 1
     |     m_i ← 1  if M_b_i = 1
     |     m_i ← −1  if M_b_i = 0
     | m
```

В результаті отримаємо масив m, порівняємо його з вихідним масивом даних

m =

	0
0	-1
1	-1
2	-1
3	1
4	-1
5	-1
6	1
7	1
8	1
9	-1
10	1
11	1
12	-1
13	1
14	1
15	...

M_b =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

Вбудовувати повідомлення в контейнер будемо по рядках (кілька бітів в один рядок контейнера). Кодування складними дискретними сигналами зробимо у такий спосіб

k := 4 g:=1

```
Sum := | for i ∈ 0.. rows (R) − 1
       |     a ← Σ_{j=0}^{k−1} [ g · ( m_{k·i+j} · ArrayFunction_{j+1} ) ]
       |     Sum_i ← a
       | Sum
```

Значення «k» обумовлює кількість інформаційних бітів, вбудованих в один фрагмент (в один рядок) контейнера. Значення «g» обумовлює «енергію» вбудованих бітів повідомлення, тобто фактично є коефіцієнтом посилення вбудованого повідомлення. У цьому разі кодування складними сигналами проводиться без посилення (g = 1). Саме кодування полягає в множенні модульованого повідомлення на сформовані вище дискретні сигнали Уолша–Адамара. Результатом виконання процедури кодування є масив «Sum»

$Sum_0 =$

	0
0	-2
1	2
2	2
3	2
4	-4
5	0
6	0
7	0
8	-2
9	2
10	2
11	2
12	-4
13	0
14	0
15	...

$Sum_{57} =$

	0
0	2
1	2
2	-2
3	2
4	0
5	0
6	-4
7	0
8	2
9	2
10	-2
11	2
12	0
13	0
14	-4
15	...

Кожен елемент масиву являє собою суму добутків k модульованих повідомлень і дискретних сигналів Уолша–Адамара. Всього масив «Sum» містить «Rows (R)» елементів за кількістю рядків контейнера. Кожен елемент масиву «Sum» призначений для вбудовування в окремий рядок контейнера-зображення. Максимальне абсолютне значення елементів масиву «Sum» задає максимальну величину внесених спотворень під час вбудовування повідомлення. Ця величина не буде перевершувати $g \cdot k$, тобто величина внесених спотворень безпосередньо визначається коефіцієнтом посилення інформаційного повідомлення і кількістю вбудованих бітів даних в один фрагмент зображення.

Завдання 2. Реалізація алгоритмів приховування та вилучення даних шляхом прямого розширення спектрів із використанням ортогональних дискретних сигналів

2.1. Реалізуємо алгоритм вбудовування інформаційних даних в просторову сферу зображення на основі прямого розширення спектра з використанням ортогональних дискретних сигналів Уолша–Адамара.

$$
\begin{aligned}
S := \;& \text{for } i \in 0..\text{rows}(R) - 1 \\
& \quad \text{for } j \in 0..\text{cols}(R) - 1 \\
& \quad\quad S_{i,j} \leftarrow R_{i,j} + \left(\text{Sum}_i\right)_j \\
& \quad\quad S_{i,j} \leftarrow 255 \text{ if } S_{i,j} > 255 \\
& \quad\quad S_{i,j} \leftarrow 0 \text{ if } S_{i,j} < 0 \\
& S
\end{aligned}
$$

Процедура вбудовування полягає в підсумовуванні даних контейнера (цифрового зображення) з модульованими складними дискретними сигналами інформаційного повідомлення.

Використовувані обмеження призначені для обліку можливостей виходу значень окремих елементів заповненого контейнера за діапазон допустимих значень яскравості окремих пікселів зображення. В результаті виконання процедури вбудовування даних отримуємо масив заповненого контейнера (стеганограмму). Порівняємо масив даних порожнього і заповненого контейнера.

Результат порівняння показує, що максимальні зміни, які вносяться до контейнера-зображення, не перевищують величини $g \cdot k = 4$. Так, наприклад, значення яскравості червоного кольору окремого пікселя $R_{1,3} = 86$ під час вбудовування інформації змінилося на значення $S_{1,3} = 90$, тобто абсолютна зміна яскравості червоного кольору в цьому пікселі дорівнює максимальному значенню. Здебільшого зміни яскравості окремих пікселів зображення знаходяться нижче за це порогове значення.

S =

	0	1	2	3	4	5
0	84	81	74	74	68	69
1	110	97	90	90	76	69
2	134	118	114	107	96	84
3	124	118	103	106	103	102
4	129	124	115	116	118	120
5	151	147	148	148	152	151
6	169	160	167	170	175	173
7	191	197	191	191	183	172
8	187	192	194	199	192	189
9	190	188	194	198	194	185
10	195	192	199	200	203	188
11	187	191	200	205	203	199
12	190	194	200	197	204	202
13	181	185	187	186	182	176
14	169	176	174	166	163	167
15	158	164	156	151	156	...

R =

	0	1	2	3	4	5
0	86	79	72	72	72	69
1	110	97	90	86	78	71
2	132	120	112	105	96	88
3	122	116	105	104	103	102
4	131	122	117	118	118	116
5	147	147	148	148	150	153
6	169	164	167	170	173	175
7	189	195	193	189	183	172
8	191	192	194	199	194	187
9	186	188	194	198	192	187
10	195	196	199	200	201	190
11	185	189	202	203	203	199
12	192	196	198	199	204	202
13	177	185	187	186	180	178
14	173	176	174	166	165	165
15	160	162	158	153	156	...

Переглянемо результат вбудовування:

S

R

Зрозуміло, що в результаті вбудовування даних з обраними параметрами (коефіцієнт посилення g і кількість бітів k, вбудованих в один елемент контейнера) внесені спотворення в контейнер-зображення, які знаходяться нижче порогу чутливості зорової системи людини і не можуть бути візуально виявлені.

Отриманий заповнений масив S записуємо в канал червоного кольору заповненого контейнера-стеганограми. Виконуємо команду

"WRITERGB("Stego_Adamar_1_4.bmp"):=augment(S, G, B)".

В результаті виконання команди система MathCAD формує на фізичному носії новий файл з ім'ям "Stego_Adamar_1_4.bmp".

Для графічного відображення вихідного (порожнього) і заповненого контейнера виконуємо вставку відповідних зображень:

"Stego_Adamar_1_4.bmp"

"1.bmp"

Переконуємося, що немає помітних спотворень.

2.2. Реалізуємо алгоритм кореляційного прийому дискретних сигналів. Для цього скористаємося функцією, що призначена для розрахунку коефіцієнта кореляції

$$\text{MultString}(A,B) := \left| \begin{array}{l} X \leftarrow 0 \\ \text{for } i \in 0..255 \\ \quad X \leftarrow X + A_i \cdot B_i \\ X \end{array} \right.$$

Наведена функція "MultString(A, B)" обчислює скалярний добуток векторів «A» і «B», результатом є коефіцієнт кореляції аргументів функції.

Для перевірки правильності обчислень виконуємо розрахунок коефіцієнта кореляції двох ортогональних векторів. Для цього запишемо

$$\text{MultString}\left(\text{ArrayFunction}_2, \text{ArrayFunction}_3\right) = 0$$

Зрозуміло, що використання в якості аргументів функції скалярного добутку двох ортогональних сигналів Уолша–Адамара призводить до нульового результату, що підтверджує правильність роботи реалізованої функції.

Розглянемо тепер масив модульованих інформаційних даних «m», масив даних – результат кодування інформаційних даних складними сигналами "Sum", а також складні сигнали, що використовуються під час встановлення інформації "ArrayFunction1", "ArrayFunction2", "ArrayFunction3", "ArrayFunction4"

m =

	0
0	-1
1	-1
2	-1
3	1
4	-1
5	-1
6	1
7	…

Sum_0 =

	0
0	-2
1	2
2	2
3	2
4	-4
5	0
6	0
7	…

ArrayFunction_1 =

	0
0	1
1	-1
2	1
3	-1
4	1
5	-1
6	1
7	…

ArrayFunction_2 =

	0
0	1
1	1
2	-1
3	-1
4	1
5	1
6	-1
7	…

ArrayFunction_3 =

	0
0	1
1	-1
2	-1
3	1
4	1
5	-1
6	-1
7	…

ArrayFunction_4 =

	0
0	1
1	1
2	1
3	1
4	-1
5	-1
6	-1
7	…

Обчислимо коефіцієнт кореляції масиву «Sum_0» з усіма чотирма ортогональними сигналами, що використовуються під час встановлення інформаційних даних. Отримаємо

$$\text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_1\right) = -256$$
$$\text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_2\right) = -256$$

$$\text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_3\right) = -256$$
$$\text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_4\right) = 256$$

Зрозуміло, що знак коефіцієнта кореляції збігається з першими чотирма елементами модульованого інформаційного повідомлення "m."

Наступний елемент інформаційних даних після модуляції відповідає масиву «Sum_1» та ортогональному сигналу "ArrayFunction1". Перевіримо правильність роботи алгоритму

$$\text{MultString}\left(\text{Sum}_1, \text{ArrayFunction}_1\right) = -256.$$

Знак коефіцієнта кореляції в цьому разі також співпадає з вбудовуваним елементом даних «m_4».

2.3. Реалізуємо алгоритм вилучення інформаційних даних з просторової області зображення на основі прямого розширення спектра з використанням ортогональних дискретних сигналів Уолша–Адамара. Для цього в тому ж вікні середовища MathCAD виконуємо команди читання растрових даних нерухомого зображення з заданого файлу (файлу заповненого контейнера) у вигляді двовимірного масиву цілих чисел. Для розглянутого прикладу виконуємо команди

"C1:=READRGB(“Stego_Adamar_1_4.bmp")",
"R1:=READ_RED(“Stego_Adamar_1_4.bmp”)",
"G1:=READ_GREEN(“Stego_Adamar_1_4.bmp”)",
"B1:=READ_BLUE(“Stego_Adamar_1_4.bmp”)."

Отримуємо такий результат

R1 =

	0	1	2	3	4
0	84	81	74	74	68
1	110	97	90	90	76
2	134	118	114	107	96
3	124	118	103	106	103
4	129	124	115	116	118
5	151	147	148	148	152
6	169	160	167	170	175
7	191	197	191	191	...

R1

Далі формуємо масив рядків заповненого контейнера за такою процедурою

```
ArrayString := | for i ∈ 0.. rows(R1) − 1
               |     for j ∈ 0.. cols(R1) − 1
               |       a_j ← R1_{i,j}
               |     ArrayString_i ← a
               | ArrayString
```

В результаті отримуємо масив рядків, в кожний з яких за допомогою k ортогональних дискретних сигналів Уолша–Адамара вбудовано k інформаційних бітів повідомлення

$\text{ArrayString}_0 =$

	0
0	84
1	81
2	74
3	74
4	68
5	69
6	71
7	...

$\text{ArrayString}_1 =$

	0
0	110
1	97
2	90
3	90
4	76
5	69
6	68
7	...

$\text{ArrayString}_2 =$

	0
0	134
1	118
2	114
3	107
4	96
5	84
6	81
7	...

Для вилучення вбудованого повідомлення скористаємося процедурою, що заснована на розглянутій вище функції обчислення коефіцієнта кореляції "MultString":

$$
\begin{aligned}
m1 := \;& \text{for } i \in 0..\text{rows}(R1) - 1 \\
& \quad \text{for } j \in 0..k - 1 \\
& \qquad m1_{k\cdot i+j} \leftarrow 1 \text{ if } \text{MultString}\left(\text{ArrayString}_i, \text{ArrayFunction}_{j+1}\right) > 0 \\
& \qquad m1_{k\cdot i+j} \leftarrow -1 \text{ if } \text{MultString}\left(\text{ArrayString}_i, \text{ArrayFunction}_{j+1}\right) \le 0 \\
& m1
\end{aligned}
$$

Правило вилучення окремих елементів повідомлення полягає в зіставленні результату обчислення коефіцієнта кореляції з граничним значенням «0». У кожному рядку контейнера вбудовано k елементів повідомлення, тобто для кожного рядка k раз виконуємо обчислення коефіцієнта кореляції.

В результаті маємо масив даних "m1", в якому містяться вилучені дані. Порівняємо вбудовані дані з вилученими

m1 =

	0
0	-1
1	-1
2	-1
3	1
4	-1
5	-1
6	1
7	1
8	1
9	-1
10	1
11	1
12	-1
13	1
14	1
15	...

m =

	0
0	-1
1	-1
2	-1
3	1
4	-1
5	-1
6	1
7	1
8	1
9	-1
10	1
11	1
12	-1
13	1
14	1
15	...

2.4. Для перетворення витягнутих даних на бітову форму використовуємо процедуру

$$M\_b1 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(m1) - 1 \\ \quad \left| \begin{array}{l} M\_b1_i \leftarrow 1 \text{ if } m1_i = 1 \\ M\_b1_i \leftarrow 0 \text{ if } m1_i = -1 \end{array} \right. \\ M\_b1 \end{array} \right.$$

В результаті отримаємо бітовий масив даних. Порівняємо його з вбудованим бітовим масивом:

M_b1 =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

M_b =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

Порівняння масивів вбудованих і витягнутих даних підтверджує правильність роботи алгоритмів вбудовування-вилучення.

Завдання 3. Проведення експериментальних досліджень ймовірносних властивостей реалізованого методу, отримання емпіричних залежностей ймовірності правильного вилучення даних та частки внесених при цьому похибок до контейнера-зображення

3.1. Проведемо оцінку ймовірності правильного вилучення повідомлення і обсягу внесених спотворень як від пропускної здатності стеганоканалу (задається величиною k), так і від коефіцієнта посилення g.

Першу емпіричну залежність побудуємо у такий спосіб. Зафіксуємо g = 1, і за цього значення будемо послідовно збільшувати величину k. Для кожного значення k розрахуємо частоту Posh помилково вилучених інформаційних бітів. Одночасно будемо розраховувати усереднену величину w внесених спотворень, виражену у відсотковому співвідношенні до максимального значення яскравості. Використаємо для цього такі процедури

$$\text{Posh} := \left| \begin{array}{l} a \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(M\_b1) - 1 \\ \quad a \leftarrow a + 1 \text{ if } M\_b1_i \neq M\_b_i \\ \text{Posh} \leftarrow \dfrac{a}{\text{rows}(M\_b1)} \\ \text{Posh} \end{array} \right. \qquad w := \left| \begin{array}{l} w \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(R1) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R1) - 1 \\ \quad\quad w \leftarrow w + \left| R1_{i,j} - R_{i,j} \right| \\ w \leftarrow \dfrac{w \cdot 100}{\text{rows}(R1) \cdot \text{cols}(R1) \cdot 256} \\ w \end{array} \right.$$

Для розглянутого прикладу у разі g = 1 и k = 4 отримуємо такі значення

$$\text{Posh} = 0,093 \qquad w = 0,586$$

Отримані емпіричні дані заносимо у відповідні таблиці

$$\text{Posh\_k} := \begin{pmatrix} 0 & 0 \\ 1 & 0,006 \\ 2 & 0,053 \\ 4 & 0,093 \\ 8 & 0,121 \\ 16 & 0,126 \\ 32 & 0,145 \\ 64 & 0,148 \\ 128 & 0,148 \\ 255 & 0,15 \end{pmatrix} \qquad \text{W\_k} := \begin{pmatrix} 0 & 0 \\ 1 & 0,39 \\ 2 & 0,39 \\ 4 & 0,586 \\ 8 & 0,871 \\ 16 & 1,244 \\ 32 & 1,723 \\ 64 & 2,385 \\ 128 & 3,286 \\ 256 & 4,5 \end{pmatrix}$$

Для побудови другої емпіричної залежності зафіксуємо величину k = 4 і, послідовно збільшуючи коефіцієнт g, будемо розраховувати

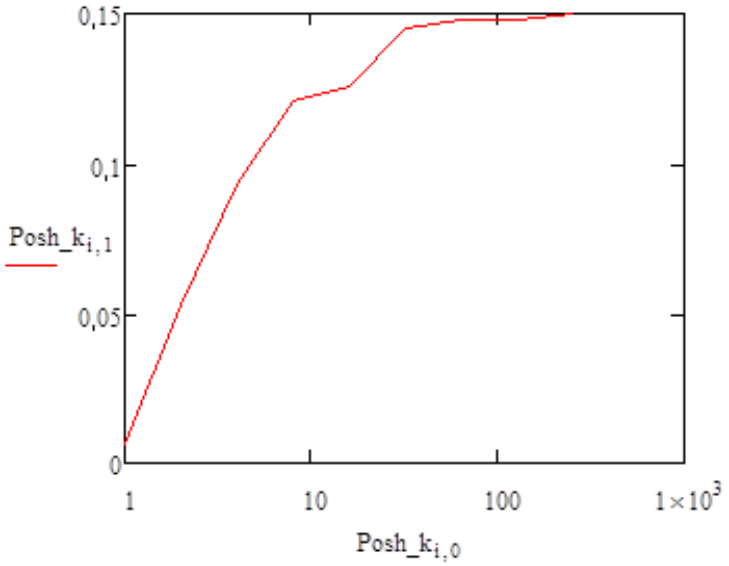
частоту Posh помилково витягнутих інформаційних бітів та усереднений обсяг w внесених спотворень.

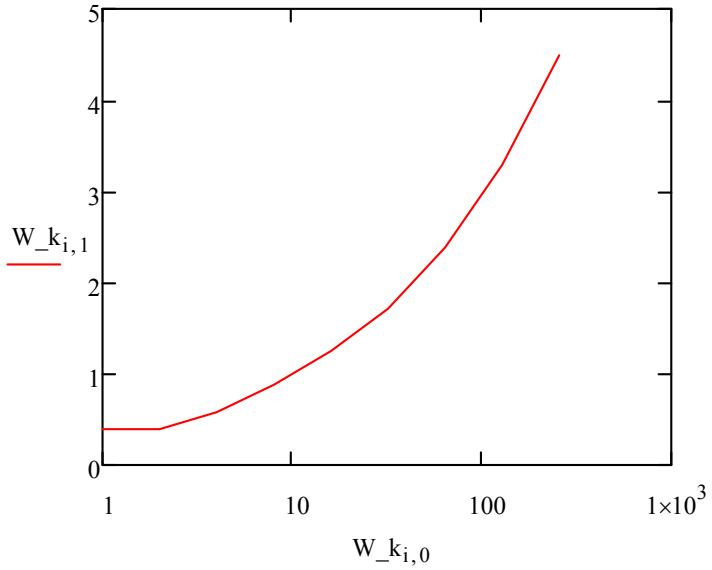
Отримані емпіричні дані заносимо у відповідні таблиці

$$Posh\_g := \begin{pmatrix} 1 & 0,093 \\ 2 & 0,018 \\ 3 & 0,003 \\ 4 & 0 \end{pmatrix} \qquad W\_g := \begin{pmatrix} 1 & 0,586 \\ 2 & 1,17 \\ 3 & 1,754 \\ 4 & 2,338 \end{pmatrix}$$

3.2. Побудуємо графіки отриманих емпіричних залежностей (для фіксованого g = 1 зі змінним k)

$$i := 0 .. 9$$

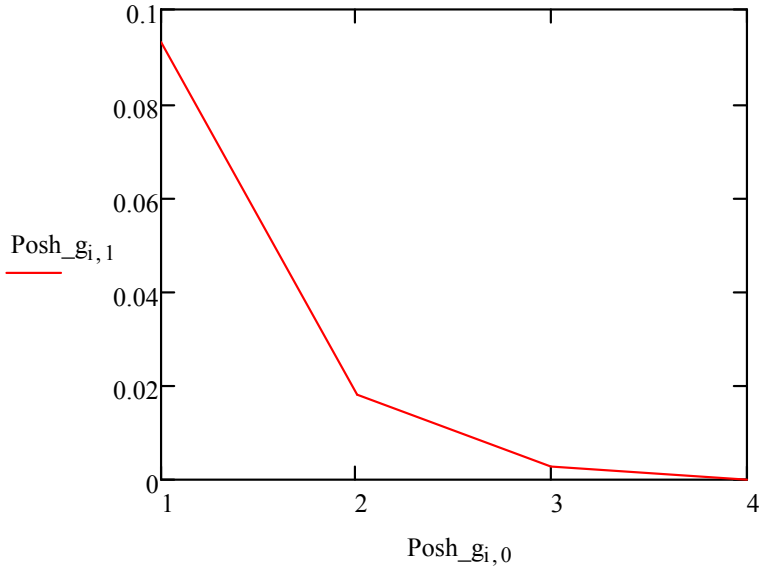


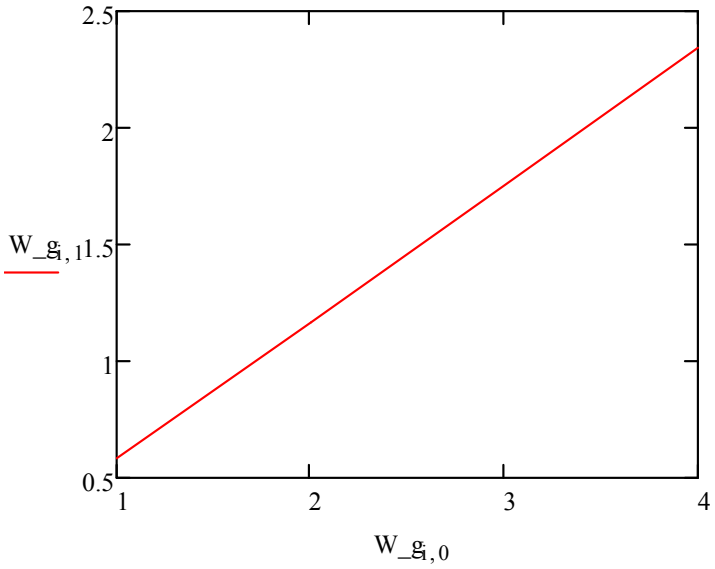


зрозуміло, що підвищення кількості вбудованих бітів даних призводить до збільшення як ймовірності помилкового вилучення даних, так і до підвищення частки внесених спотворень в контейнер-зображення. Слід зазначити, що збільшення кількості вбудованих бітів на один порядок (з 10 до

100 і вище) призводить до незначного (менше 0,05) збільшення ймовірності помилкового вилучення, в той час як частка внесених спотворень збільшується при цьому в 4–5 разів.

3.3. Побудуємо графіки отриманих емпіричних залежностей (для фіксованого k = 4 зі змінним g)

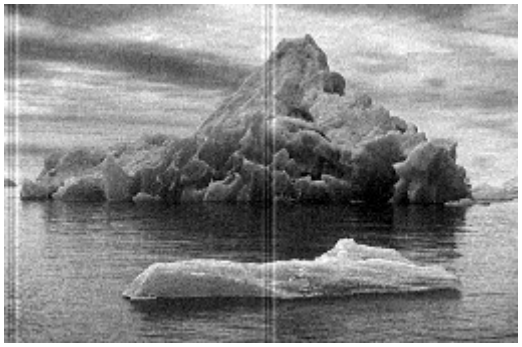




Наведені залежності свідчать, що збільшення коефіцієнта посилення g призводить до різкого зниження ймовірності помилкового вилучення інформаційних бітів даних і водночас до підвищення обсягу внесених спотворень. З наведених графіків видно, що у разі g = 4 забезпечується безпомилкове вилучення інформаційних даних, частка внесених спотворень в середньому знаходиться нижче порогу зорової чутливості людини.

У той же час слід зазначити, що розраховане значення w є усередненою величиною, що характеризує частку внесених спотворень в середньому за всіма пікселями контейнера-зображення. Окремі пікселі або група пікселів можуть бути перекручені дуже сильно, частка внесених

спотворень для цих фрагментів зображення може істотно перевищувати розраховане середнє значення w. Для прикладу наведемо контейнер-зображення, що заповнено з показниками: k = 128, g = 1,



S

R

Як випливає з наведених вище графіків, вбудовування з такими параметрами дає усереднене значення частки внесених спотворень в межах порогу зорової чутливості людини. Однак, як видно з наведених зображень, для деяких фрагментів спотворення дуже істотні. Позбутися подібних негативних факторів можливо за допомогою адаптивного формування дискретних сигналів, що враховує особливості використовуваного контейнера-зображення. Крім того, використання під час встановлення даних ортогональних дискретних сигналів Уолша–Адамара не завжди виправдано в стеганографії. Подібні сигнали на окремих ділянках мають вигляд детермінованих послідовностей. Наприклад, сигнал "ArrayFunction_0" зовсім не використовувався нами під час встановлення інформації, оскільки він складається з послідовності одних одиничних символів. Альтернативою використання ортогональних сигналів Уолша–Адамара є квазіортогональні дискретні послідовності, що мають псевдовипадкову структуру і не містять (в ідеальному випадку) детерміновані ділянки.

Завдання 4. Реалізація алгоритмів формування ансамблів квазіортогональних дискретних сигналів та алгоритмів приховування та вилучення даних

4.1. Реалізуємо алгоритм формування квазіортогональних дискретних сигналів так

```
ArrayFunction1 := | for i ∈ 0..1023
                  |   for j ∈ 0..255
                  |     b ← ceil(rnd(2)) − 1
                  |     a_j ← 1  if b = 1
                  |     a_j ← −1  if b = 0
                  |   ArrayFunction1_i ← a
                  | ArrayFunction1
```

Для формування окремих елементів послідовностей використаємо вбудовану функцію генерації псевдовипадкових чисел «rnd()», що формує раціональне число, що знаходиться в заданому діапазоні.

Функція «ceil()» округляє отриманий результат до найближчого цілого числа.

Після перетворення «0» в «–1» отримаємо масив "ArrayFunction1", елементами якого є псевдовипадкові послідовності – сформовані дискретні сигнали. Значення коефіцієнта взаємної кореляції сформованих сигналів (через псевдовипадковість їх формування) значно не відрізняються від нуля, тобто вважатимемо сформовану множину послідовностей ансамблем квазіортогональних дискретних сигналів.

Так, наприклад, для першого і сьомого дискретного сигналу

ArrayFunction1 $_1$ =

	0
0	1
1	1
2	-1
3	1
4	1
5	1
6	-1
7	-1
8	1
9	-1
10	1
11	-1
12	1
13	1
14	-1
15	...

ArrayFunction1 $_7$ =

	0
0	-1
1	1
2	1
3	-1
4	-1
5	1
6	1
7	1
8	1
9	-1
10	-1
11	-1
12	-1
13	-1
14	-1
15	...

коефіцієнт взаємної кореляції дорівнює

$$\text{MultString}\left(\text{ArrayFunction1}_2, \text{ArrayFunction1}_7\right) = 26$$

4.2. Для вбудовування інформаційних повідомлень з використанням сформованого ансамблю квазіортогональних дискретних сигналів розіб'ємо бітовий масив "M_b" на підблоки і сформуємо масив десяткових чисел

```
M_d := | for i ∈ 0.. rows(R) − 1
       |     a ← 0
       |     for j ∈ 0.. 9
       |       a ← a + M_b[10·i+j] · 2^j
       |     M_d[i] ← a
       | M_d
```

M_d =

	0
0	456
1	187
2	607
3	963
4	485
5	60
6	674
7	131
8	...

Елементами сформованого масиву "M_d" є десяткові числа, кожне з яких в двійковому поданні відповідає підблоку з десяти бітів масиву "M_b".

4.3. Реалізуємо алгоритм кодування квазіортогональними дискретними сигналами

$g := 40$

$Sum1 :=$ for $i \in 0..\text{rows}(R) - 1$

$Sum1_i \leftarrow g \cdot \text{ArrayFunction1}\left(M\_d_i\right)$

$Sum1$

$Sum1_0 =$

	0
0	-40
1	-40
2	40
3	40
4	-40
5	-40
6	-40
7	-40
8	...

В результаті виконання наведеної процедури формуємо масив "Sum1", елементами якого є дискретні сигнали з масиву "ArrayFunction1", посилені коефіцієнтами "g". Номери використовуваних сигналів відповідають десятковим поданням інформаційних блоків вбудованого повідомлення.

4.4. Реалізуємо алгоритм вбудовування інформаційного повідомлення в контейнер-зображення за допомогою накладення модульованого повідомлення на масив яскравостей каналу червоного кольору.

$S1 :=$ for $i \in 0..\text{rows}(R) - 1$

for $j \in 0..\text{cols}(R) - 1$

$S1_{i,j} \leftarrow R_{i,j} + \left(Sum1_i\right)_j$

$S1_{i,j} \leftarrow 255$ if $S1_{i,j} > 255$

$S1_{i,j} \leftarrow 0$ if $S1_{i,j} < 0$

$S1$

В результаті виконання наведеної процедури формуємо масив «S1». Порівняємо канали червоного кольору порожнього і заповненого контейнера

$S1 =$

	0	1	2	3
0	46	39	112	112
1	70	137	50	126
2	172	80	152	145
3	162	76	145	144
4	171	82	157	158
5	107	187	188	108
6	129	124	127	210
7	229	235	153	229
8	151	232	234	239
9	226	148	154	...

$R =$

	0	1	2	3
0	86	79	72	72
1	110	97	90	86
2	132	120	112	105
3	122	116	105	104
4	131	122	117	118
5	147	147	148	148
6	169	164	167	170
7	189	195	193	189
8	191	192	194	199
9	186	188	194	...

S1

R

Після виконання командного запису

WRITERGB("Stego_Kvasi.bmp") := augment(S1, G, B)

отримуємо контейнер-повідомлення

"Stego_Kvasi.bmp"

"1.bmp"

Зрозуміло, що вбудовування з таким високим значенням коефіцієнта посилення (g = 40) призводить до появи суттєвих перекручень, наочно поданих на зображеннях.

4.5. Реалізуємо алгоритм вилучення повідомлень з використанням квазіортогональних дискретних сигналів. Для цього зробимо зчитування растрових даних з контейнера-зображення

C2 := READRGB("Stego_Kvasi.bmp")

R2 := READ_RED("Stego_Kvasi.bmp")

G2 := READ_GREEN("Stego_Kvasi.bmp")

B2 := READ_BLUE("Stego_Kvasi.bmp")

В результаті отримуємо

R2 =

	0	1	2	3	4
0	46	39	112	112	32
1	70	137	50	126	38
2	172	80	152	145	136
3	162	76	145	144	63
4	171	82	157	158	78
5	107	187	188	108	190
6	129	124	127	210	133
7	229	235	153	229	...

R2

Сформуємо зі зчитаного масиву червоного кольору "R2" масив рядків контейнера

```
ArrayString1 := | for i ∈ 0.. rows(R2) − 1
                |   for j ∈ 0.. cols(R2) − 1
                |     a_j ← R2_{i,j}
                |   ArrayString1_i ← a
                | ArrayString1
```

ArrayString1 =

	0
0	46
1	39
2	112
3	112
4	32
5	29
6	31
7	34
8	...

Після чого сформуємо масив десяткових чисел "M_d1", елементами якого будуть номери квазіотрогональних сигналів з масиву "ArrayFunction1", які дають найбільше значення коефіцієнта кореляції з рядками контейнера-зображення

```
M_d1 := | for i ∈ 0.. rows(R1) − 1
        |   a ← 0
        |   for j ∈ 0.. 1023
        |     if MultString(ArrayString1_i, ArrayFunction1_j) > a
        |       a ← MultString(ArrayString1_i, ArrayFunction1_j)
        |       M_d1_i ← j
        | M_d1
```

Фактично наведена процедура реалізує кореляційний прийом (в термінах статистичної теорії зв'язку).

Порівняємо витягнутий масив «M_d1» з тим масивом, що був вбудований в контейнер-зображення

M_d =

	0
0	456
1	187
2	607
3	963
4	485
5	60
6	674
7	131
8	753
9	380
10	574
11	899
12	749
13	251
14	782
15	...

M_d1 =

	0
0	456
1	561
2	607
3	561
4	561
5	60
6	674
7	561
8	561
9	561
10	574
11	561
12	561
13	561
14	561
15	...

Зрозуміло, що отриманий масив десяткових чисел відрізняється від вбудованого масиву, що пояснюється, вочевидь, сильною кореляцією використовуваних квазіортогональних дискретних сигналів з окремими елементами контейнера-зображення.

4.6. Надамо отриманому масиву "M_d1" двійкового вигляду

```
M_b2 := | for i ∈ 0.. rows(M_d1) − 1
        |   x ← M_d1_i
        |   for j ∈ 0..9
        |     M_b2_(i·10+j) ← mod(x, 2)
        |     x ← floor(x/2)
        | M_b2
```

Отримаємо масив "M_d1". Порівняємо його з вбудованим двійковим масивом "Md"

M_b2 =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	...

M_b =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	...

4.7. Проведемо оцінку ймовірності правильного вилучення повідомлення обсягу внесених спотворень від коефіцієнта посилення g. Для цього розрахуємо частоту помилково отриманих інформаційних бітів і оцінку внесених спотворень в контейнер-зображення

```
Posh := | a ← 0
        | for i ∈ 0.. rows(M_b2) − 1
        |   a ← a + 1 if M_b2_i ≠ M_b_i
        | Posh ← a / rows(M_b2)
        | Posh
```

Posh = 0,104

```
w := | w ← 0
     | for i ∈ 0.. rows(R2) − 1
     |   for j ∈ 0.. cols(R2) − 1
     |     w ← w + |R2_(i,j) − R_(i,j)|
     | w ← w·100 / (rows(R2)·cols(R2)·256)
     | w
```

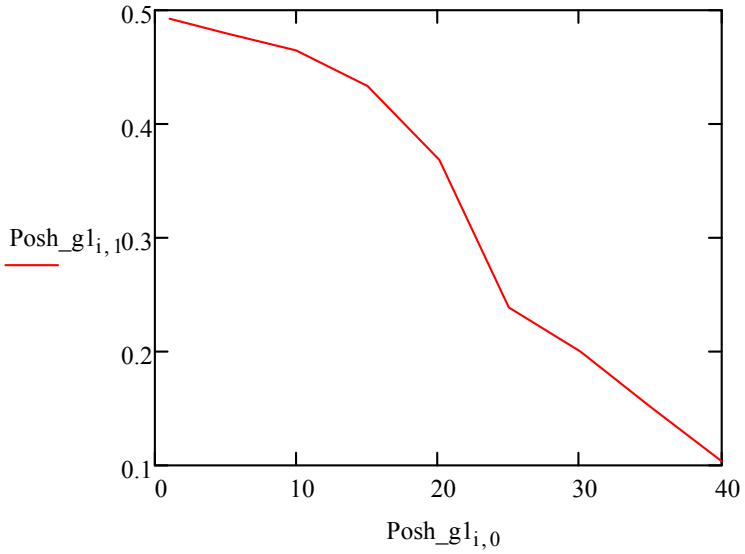
w = 15,311

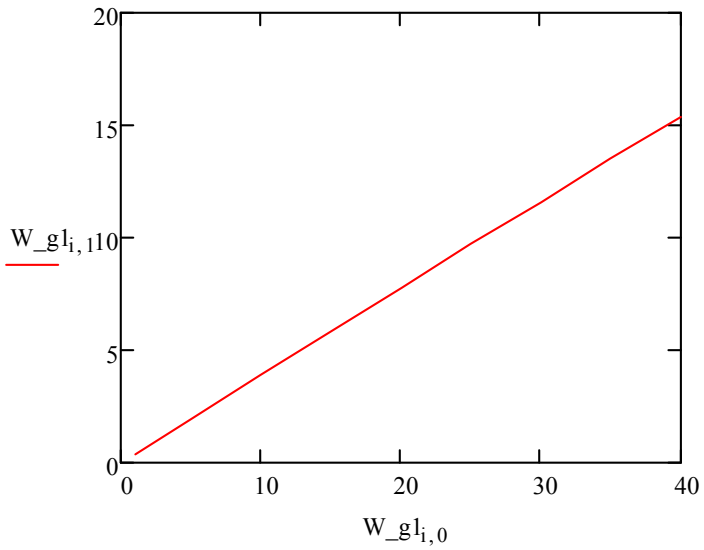
Послідовно змінюючи коефіцієнт посилення g і виконуючи процедури вбудовування та вилучення повідомлення, отримаємо відповідні емпіричні оцінки, які занесемо в таблиці

$$Posh\_g1 := \begin{pmatrix} 1 & 0{,}493 \\ 5 & 0{,}479 \\ 10 & 0{,}464 \\ 15 & 0{,}434 \\ 20 & 0{,}368 \\ 25 & 0{,}238 \\ 30 & 0{,}2 \\ 35 & 0{,}151 \\ 40 & 0{,}104 \end{pmatrix} \qquad W\_g1 := \begin{pmatrix} 1 & 0{,}39 \\ 5 & 1{,}951 \\ 10 & 3{,}897 \\ 15 & 5{,}838 \\ 20 & 7{,}771 \\ 25 & 9{,}692 \\ 30 & 11{,}596 \\ 35 & 13{,}473 \\ 40 & 15{,}331 \end{pmatrix}$$

4.8. Побудуємо графіки отриманих емпіричних оцінок

$$i := 0 .. 9$$





Отримані емпіричні залежності показують, що підвищення коефіцієнта посилення призводить до різкого зниження ймовірності помилкового вилучення інформаційних бітів повідомлення. Це також веде до збільшення внесених спотворень в контейнер-зображення. Однак порівняно із використанням ортогональних дискретних сигналів (див. рисунки п. 3.3.)

застосування квазіортогональних сигналів призводить до меншого спотворення контейнера. Так, наприклад, під час встановлення k = 4 біт повідомлення в один рядок контейнера з використанням ортогональних дискретних сигналів за коефіцієнта посилення g = 4 обсяг внесених спотворень становить понад 2,33 %. За більшої кількості внесених бітів даних (10 бітів в один рядок контейнера), а отже і за більшої пропускної здатності стеганографічного каналу передачі даних застосування квазіортогональних дискретних сигналів навіть з великим значенням коефіцієнта посилення (g = 5) призводить до менших спотворень контейнера, обсяг внесених спотворень не перевищує 2 %.

Отже, застосування квазіортогональних дискретних сигналів дозволяє істотно підвищити пропускну здатність стеганоканалів за меншого обсягу внесених спотворень. У той же час, використання квазіортогональних дискретних сигналів істотно підвищує ймовірність помилкового вилучення бітів повідомлення (за рахунок сильної кореляції з окремими фрагментами контейнера-зображення). Позбутися цього негативного фактора можливо за рахунок адаптивного формування квазіортогональних дискретних сигналів з урахуванням особливостей використовуваного контейнера-зображення.

Завдання 5. (Додаткове завдання). Реалізація адаптивного алгоритму формування квазіортогональних дискретних сигналів. Реалізація алгоритмів приховування та вилучення даних із адаптовано сформованих квазіортогональних дискретних сигналів, отримання емпіричних залежностей ймовірності правильного вилучення даних та частки внесених при цьому похибок у контейнер-зображення

5.1. Реалізуємо адаптивний алгоритм формування квазіортогональних дискретних сигналів з урахуванням особливостей використовуваного контейнера-зображення. Для цього розіб’ємо масив яскравостей червоного кольору на рядки у такий спосіб формований масив "R_Arr" в якості елементів містить рядки масиву яскравостей червоного кольору контейнера-зображення.

$$
\begin{array}{l}
\text{R\_Arr} := \left| \begin{array}{l}
\text{for } i \in 0..\text{rows}(R) - 1 \\
\quad \left| \begin{array}{l}
\text{for } j \in 0..255 \\
\quad a_j \leftarrow R_{i,j} \\
\quad \text{R\_Arr}_i \leftarrow a
\end{array} \right. \\
\text{R\_Arr}
\end{array} \right.
\end{array}
$$

Алгоритм адаптивного формування квазіортогональних дискретних сигналів подано за такою процедурою

```
ArrayFunction2 := | i ← 0
                  | while i < 1024
                  |     for j ∈ 0..255
                  |         b ← ceil(rnd(2)) − 1
                  |         a_j ← 1  if b = 1
                  |         a_j ← −1  if b = 0
                  |     ArrayFunction2_i ← a
                  |     b ← 0
                  |     jj ← 0
                  |     while jj < rows(R_Arr) ∧ b = 0
                  |         a ← MultString(R_Arr_jj, ArrayFunction2_i)
                  |         b ← b + 1  if |a| > 1000
                  |         jj ← jj + 1
                  |     i ← i + 1  if b = 0
                  | ArrayFunction2
```

ArrayFunction2 $_{777}$ =

	0
0	1
1	1
2	1
3	1
4	1
5	1
6	-1
7	-1
8	-1
9	1
10	1
11	-1
12	-1
13	-1
14	1
15	...

Суть алгоритму полягає у формуванні псевдовипадкових послідовностей і обчисленні коефіцієнта кореляції з усіма елементами масиву "R_Arr", тобто з усіма рядками контейнера. Якщо коефіцієнт кореляції для всіх рядків контейнера не перевищує заздалегідь заданої величини (в цьому разі значення 1024) сформована послідовність використовується як квазіортогональний дискретний сигнал. Якщо коефіцієнт кореляції для будь-якого рядка контейнера перевищить задане значення, сформована послідовність бракується і формується інша послідовність. Зрозуміло, що час формування ансамблю дискретних сигналів залежить від граничної величини, з якою порівнюється значення коефіцієнта кореляції. Із її зменшенням різко зростають тимчасові витрати на формування ансамблю сигналу, проте мале граничне значення забезпечить слабку кореляцію сформованих квазі-

ортогональних дискретних сигналів з окремими фрагментами контейнера-зображення. Для прикладу наведемо один з дискретних сигналів і значення коефіцієнта кореляції з одним із рядків контейнера

$$\text{MultString}\left(\text{R\_Arr}_2, \text{ArrayFunction2}_{777}\right) = -562.$$

5.2. Для вбудовування повідомлення скористаємося такою процедурою

$$g := 9$$

$$\text{Sum2} := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R) - 1 \\ \quad \text{Sum2}_i \leftarrow g \cdot \text{ArrayFunction2}\left(\text{M\_d}_i\right) \\ \text{Sum2} \end{array} \right.$$

Сформований масив "Sum2" в якості елементів містить модульоване квазіортогональними сигналами повідомлення. Для його вбудовування виконаємо накладення масиву "Sum2" на контейнер-зображення

$$\text{S2} := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R) - 1 \\ \quad\quad \left| \begin{array}{l} \text{S2}_{i,j} \leftarrow \text{R}_{i,j} + \left(\text{Sum2}_i\right)_j \\ \text{S2}_{i,j} \leftarrow 255 \text{ if } \text{S2}_{i,j} > 255 \\ \text{S2}_{i,j} \leftarrow 0 \text{ if } \text{S2}_{i,j} < 0 \end{array} \right. \\ \text{S2} \end{array} \right.$$

Отримаємо заповнений контейнер, порівняємо його з початковим

S2 =

	0	1	2	3
0	77	70	81	81
1	119	106	99	77
2	141	129	121	114
3	113	125	96	95
4	122	131	126	109
5	156	138	157	139
6	178	173	158	179
7	198	204	184	...

R =

	0	1	2	3
0	86	79	72	72
1	110	97	90	86
2	132	120	112	105
3	122	116	105	104
4	131	122	117	118
5	147	147	148	148
6	169	164	167	170
7	189	195	193	...

S2

R

Запишемо сформований контейнер у файл і подивимося результат

WRITERGB("Stego_Kvasi_ad.bmp") := augment (S2, G, B)

"Stego_Kvast_.ad.bmp"

"1.bmp"

Як видно з наведених рисунків, сформований контейнер практично не відрізняється від початкового. Проте в нього вбудовано більш за 1600 бітів інформаційного повідомлення.

5.3. Для вилучення інформаційного повідомлення розрахуємо дані контейнера

C3 := READRGB("Stego_Kvasi_ad.bmp")

R3 := READ_RED("Stego_Kvasi_ad.bmp")

G3 := READ_GREEN("Stego_Kvasi_ad.bmp")

B3 := READ_BLUE("Stego_Kvasi_ad.bmp")

R3 =

	0	1	2	3	4
0	77	70	81	81	63
1	119	106	99	77	69
2	141	129	121	114	87
3	113	125	96	95	112
4	122	131	126	109	109
5	156	138	157	139	159
6	178	173	158	179	164
7	198	204	184	180	...

R3

Сформуємо масив рядків заповненого контейнера

ArrayString2 :=
for i ∈ 0.. rows(R3) − 1
  for j ∈ 0.. cols(R3) − 1
    $a_j \leftarrow R3_{i,j}$
  $ArrayString2_i \leftarrow a$
ArrayString2

і винесемо вбудоване повідомлення у вигляді десяткового масиву даних

```
M_d2 := | for i ∈ 0.. rows(R3) − 1
        |   a ← 0
        |   for j ∈ 0.. 1023
        |     if MultString(ArrayString2_i, ArrayFunction2_j) > a
        |       a ← MultString(ArrayString2_i, ArrayFunction2_j)
        |       M_d2_i ← j
        | M_d2
```

Отриманий результат можна порівняти з масивом вбудованих даних

M_d =

	0
0	456
1	187
2	607
3	963
4	485
5	60
6	674
7	131
8	753
9	380
10	574
11	899
12	749
13	251
14	782
15	...

M_d2 =

	0
0	456
1	187
2	607
3	963
4	485
5	60
6	674
7	131
8	753
9	380
10	574
11	899
12	749
13	251
14	782
15	...

Зрозуміло, що використання адаптивно формованих дискретних сигналів дозволило істотно підвищити ймовірність правильного вилучення повідомлень.

5.4. Надамо отриманому масиву даних двійковий вигляду і порівняємо отриманий результат з тими двійковими даними, які були вбудовані в контейнер

```
M_b3 := | for i ∈ 0.. rows(M_d2) − 1
        |   x ← M_d2_i
        |   for j ∈ 0.. 9
        |     M_b3_(i·10+j) ← mod(x, 2)
        |     x ← floor(x / 2)
        | M_b3
```

M_b3 =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

M_b =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

5.5. Проведемо оцінку ймовірності правильного вилучення повідомлення і обсягу внесених спотворень від коефіцієнта посилення g. Для цього розрахуємо частоту помилково витягнутих інформаційних бітів і оцінку внесених спотворень в контейнер-зображення

$$\text{Posh} := \left| \begin{array}{l} a \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(M\_b3) - 1 \\ \quad a \leftarrow a + 1 \text{ if } M\_b3_i \neq M\_b_i \\ \text{Posh} \leftarrow \dfrac{a}{\text{rows}(M\_b3)} \\ \text{Posh} \end{array} \right.$$

$$w := \left| \begin{array}{l} w \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(R3) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R3) - 1 \\ \quad\quad w \leftarrow w + \left| R3_{i,j} - R_{i,j} \right| \\ w \leftarrow \dfrac{w \cdot 100}{\text{rows}(R3) \cdot \text{cols}(R3) \cdot 256} \\ w \end{array} \right.$$

Posh = 0

w = 3,508

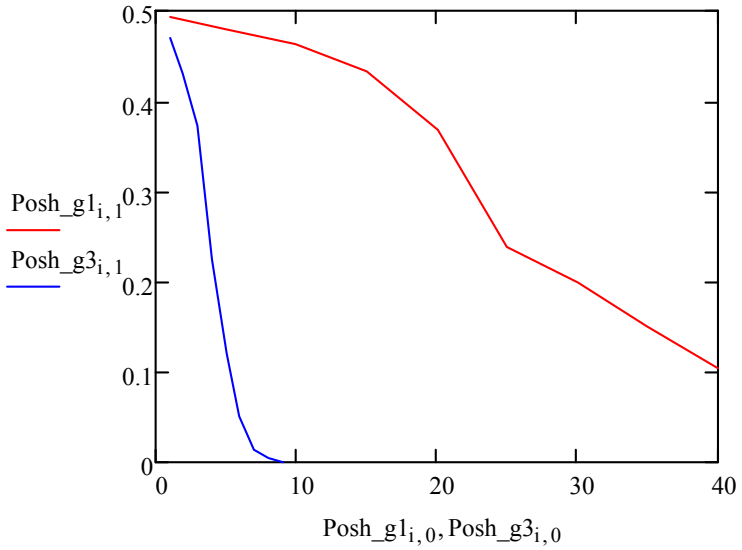
Послідовно змінюючи коефіцієнт посилення g і виконуючи процедури вбудовування та вилучення повідомлення, отримаємо відповідні емпіричні оцінки, які занесемо в таблиці

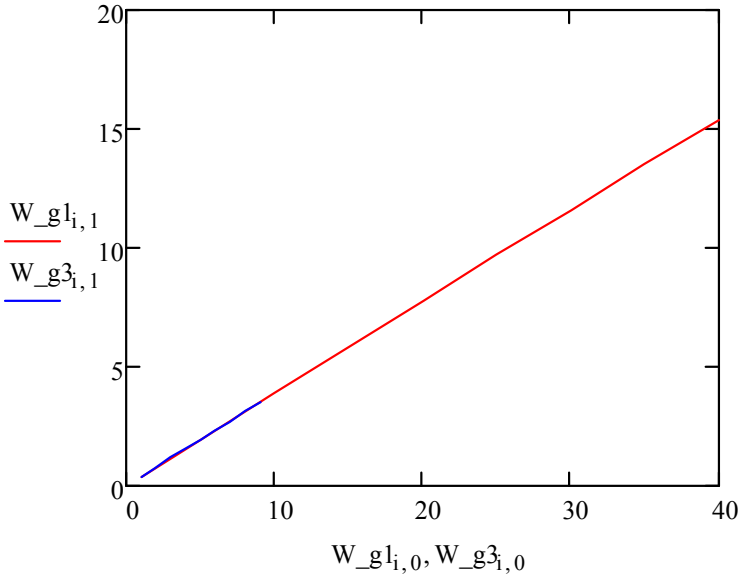
$$Posh\_g3 := \begin{pmatrix} 1 & 0,47 \\ 2 & 0,43 \\ 3 & 0,373 \\ 4 & 0,224 \\ 5 & 0,121 \\ 6 & 0,051 \\ 7 & 0,015 \\ 8 & 0,005 \\ 9 & 0 \end{pmatrix}$$

$$W\_g3 := \begin{pmatrix} 1 & 0,39 \\ 2 & 0,781 \\ 3 & 1,171 \\ 4 & 1,561 \\ 5 & 1,951 \\ 6 & 2,34 \\ 7 & 2,73 \\ 8 & 3,119 \\ 9 & 3,508 \end{pmatrix}$$

5.6. Побудуємо графіки отриманих емпіричних оцінок і порівняємо їх з отриманими раніше залежностями для випадку використання квазіортогональних дискретних сигналів без адаптації до використовуваного контейнера

$i := 0 .. 9$





Синім кольором на графіках відображені результати моделювання стеганосистем з адаптивним формуванням сигналів, червоним – без адаптації. Зрозуміло, що без збільшення обсягу внесених спотворень вдалося істотно знизити ймовірність помилкового вилучення інформаційних бітів повідомлень. Порівняно із використанням ортогональних дискретних сигналів вдалося істотно збільшити пропускну здатність стеганоканалу під час порівняння внесених викривлень. Як приклад на рисунках наведемо контейнери:

S

S2

R

Перший контейнер заповнено з використанням ортогональних дискретних сигналів з параметрами «k = 4» і «g = 4», тобто в кожен рядок контейнера вбудовано чотири біти, всього в контейнер вбудовано 676 бітів інформації. Ці параметри забезпечують практично безпомилкове отримання повідомлення, проте максимальний обсяг внесених спотворень в окремі пікселі зображення складає k * g = 16 рівнів яскравості.

Другий контейнер заповнений з використанням адаптивно сформованих (з урахуванням властивостей контейнера-зображення) квазіортогональних дискретних сигналів. При цьому використаний коефіцієнт посилення «g = 9» також забезпечує практично безпомилкове отримання інформаційного повідомлення, проте максимальний обсяг внесених спотворень в окремі пікселі зображення становить g = 9 рівнів яскравості. І хоча усереднене значення внесених спотворень для ортогональних сигналів трохи нижче, їх абсолютне значення істотно (майже в два рази) може перевищувати аналогічний показник для адаптивно сформованих квазіортогональних сигналів. Вплив зниження максимального рівня внесених викривлень на окремі пікселі зображення візуально помітний на наведених рисунках. Третій контейнер являє собою немодифікований (порожній) контейнер.

Отже, як бачимо з отриманих результатів застосування адаптивно сформованих квазіортогональних дискретних сигналів дозволяє істотно підвищити пропускну здатність стеганоканалу у разі порівняних викривлень, що вносяться до контейнера-зображення. Внесені спотворення можна ще значніше знизити, зменшивши чисельний поріг, що обмежує коефіцієнт взаємної кореляції в алгоритмі адаптивного формування дискретних сигналів.

6. ПРИКЛАД ОФОРМЛЕННЯ ЗВІТУ З ЛАБОРАТОРНОЇ РОБОТИ

Лабораторна робота № 3

Вбудовування даних у просторову сферу нерухомих зображень на основі прямого розширення спектра.

1.

"Picture.bmp"

C := READRGB("Picture.bmp")

R := READ_RED("Picture.bmp")

G := READ_GREEN("Picture.bmp")

B := READ_BLUE("Picture.bmp")

M := READBIN("Text.txt","byte")

Функція перетворення повідомлення з двійкового виду в на десятковий

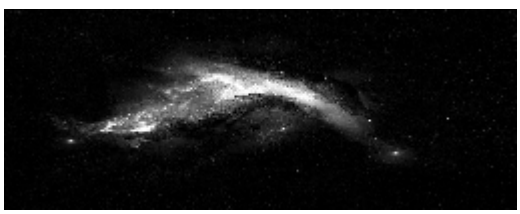
$$B2D(x) := \sum_{i=0}^{7} \left(x_i \cdot 2^i \right)$$

Функція перетворення повідомлення десяткового виду в двійковий

$$D\_B(x) := \left| \begin{array}{l} \text{for } i \in 0..7 \\ \quad \left| \begin{array}{l} V_i \leftarrow \text{mod}(x, 2) \\ x \leftarrow \text{floor}\left(\frac{x}{2}\right) \end{array} \right. \\ V \end{array} \right.$$

Функція перетворення з десяткового масива M на двійковий

$$M\_b := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(M) - 1 \\ \quad \left| \begin{array}{l} V \leftarrow D\_B\left(M_i\right) \\ \text{for } j \in 0..7 \\ \quad M\_b_{i \cdot 8 + j} \leftarrow V_j \end{array} \right. \\ M\_b \end{array} \right.$$



R

M =

	0
0	68
1	69
2	70
3	32
4	76
5	69
6	80
7	80
8	65
9	82
10	68
11	32
12	76
13	89
14	82
15	...

M_b =

	0
0	0
1	0
2	1
3	0
4	0
5	0
6	1
7	0
8	1
9	0
10	1
11	0
12	0
13	0
14	1
15	...

Формування матриць Адамара

$H_0 := (1)$

```
H := | for i ∈ 1..8
       | F ← H_(i−1)
       | for j ∈ 0..rows(F) − 1
       |   for jj ∈ 0..cols(F) − 1
       |     | a ← F_(jj,j)
       |     | F1_(jj,j) ← a
       | for j ∈ 0..rows(F) − 1
       |   for jj ∈ 0..cols(F) − 1
       |     | a ← F_(jj,j)
       |     | F1_(jj+cols(F),j) ← a
       | for j ∈ 0..rows(F) − 1
       |   for jj ∈ 0..cols(F) − 1
       |     | a ← F_(jj,j)
       |     | F1_(jj,j+rows(F)) ← a
       | for j ∈ 0..rows(F) − 1
       |   for jj ∈ 0..cols(F) − 1
       |     | a ← F_(jj,j)
       |     | F1_(jj+cols(F),j+rows(F)) ← −a
       | H_i ← F1
     | H
```

$H_8 =$

	0	1	2	3	4	5	6	7	8	9
0	1	1	1	1	1	1	1	1	1	1
1	1	-1	1	-1	1	-1	1	-1	1	-1
2	1	1	-1	-1	1	1	-1	-1	1	1
3	1	-1	-1	1	1	-1	-1	1	1	-1
4	1	1	1	1	-1	-1	-1	-1	1	1
5	1	-1	1	-1	-1	1	-1	1	1	-1
6	1	1	-1	-1	-1	-1	1	1	1	1
7	1	-1	-1	1	-1	1	1	-1	1	-1
8	1	1	1	1	1	1	1	1	-1	-1
9	1	-1	1	-1	1	-1	1	-1	-1	1
10	1	1	-1	-1	1	1	-1	-1	-1	-1
11	1	-1	-1	1	1	-1	-1	1	-1	1
12	1	1	1	1	-1	-1	-1	-1	-1	-1
13	1	-1	1	-1	-1	1	-1	1	-1	1
14	1	1	-1	-1	-1	-1	1	1	-1	-1
15	1	-1	-1	1	-1	1	1	-1	-1	...

Масив ортогональних функцій

```
ArrayFunction := | for i ∈ 0..255
                 |   for j ∈ 0..255
                 |     a_j ← (H_8)_(i,j)
                 |   ArrayFunction_i ← a
                 | ArrayFunction
```

$ArrayFunction_5 =$

	0
0	1
1	-1
2	1
3	-1
4	-1
5	1
6	-1
7	1
8	1
9	-1
10	1
11	...

Перетворимо бітове повідомлення

```
m := | for i ∈ 0..rows(M_b) − 1
     |   | m_i ← 1  if M_b_i = 1
     |   | m_i ← −1  if M_b_i = 0
     | m
```

```
m2b(m) := | for i ∈ 0..rows(m) − 1
          |   | m1_i ← 1  if m_i = 1
          |   | m1_i ← 0  if m_i = −1
          | m1
```

Модулюємо кожен інформаційний біт за допомогою ПВП довжиною 256 бітів

$$k := 4 \qquad g := 4$$

$$\text{Sum} := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R) - 1 \\ \quad \left| \begin{array}{l} a \leftarrow \sum_{j=0}^{k-1} \left[g \cdot \left(m_{k \cdot i + j} \cdot \text{ArrayFunction}_{j+1} \right) \right] \\ \text{Sum}_i \leftarrow a \end{array} \right. \\ \text{Sum} \end{array} \right.$$

Накладення модульованого повідомлення на контейнер

$$S := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R) - 1 \\ \quad\quad \left| \begin{array}{l} S_{i,j} \leftarrow R_{i,j} + \left(\text{Sum}_i \right)_j \\ S_{i,j} \leftarrow 255 \text{ if } S_{i,j} > 255 \\ S_{i,j} \leftarrow 0 \text{ if } S_{i,j} < 0 \end{array} \right. \\ S \end{array} \right.$$

Порожній та заповнений контейнери:

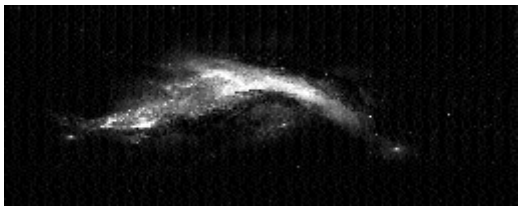
$R =$

	0	1	2	3	4	5
0	10	5	6	4	1	8
1	8	0	7	23	1	19
2	3	7	4	2	0	7
3	0	11	3	6	3	4
4	6	0	5	2	8	0
5	4	0	2	2	1	6
6	9	0	4	2	5	1
7	8	4	0	1	1	4
8	3	3	0	1	1	6
9	0	3	1	3	5	2
10	3	12	2	0	6	...

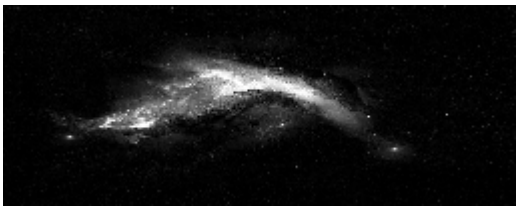
$S =$

	0	1	2	3	4	5
0	2	0	0	12	1	8
1	0	0	0	31	1	19
2	3	0	4	2	8	0
3	0	3	0	14	3	4
4	6	0	0	2	16	8
5	0	0	0	10	1	6
6	0	0	4	2	0	9
7	0	12	0	0	1	20
8	3	3	0	17	0	0
9	0	0	0	11	5	2
10	3	0	2	0	14	...

$$\text{WRITERGB("Stego1.bmp")} := \text{augment}(S, G, B)$$



S



R

" Stego1.bmp"

"Picture.bmp"

Функція розрахунку коефіцієнта кореляції

$$\text{MultString}(A,B) := \left| \begin{array}{l} X \leftarrow 0 \\ \text{for } i \in 0..255 \\ \quad X \leftarrow X + A_i \cdot B_i \\ X \end{array} \right.$$

За результатами обчислень видно, що повідомлення корельовано з ПВП (1, 2, 3, 4), а самі ПВП між собою некорельовані.

$\text{MultString}\left(\text{ArrayFunction}_2, \text{ArrayFunction}_3\right) = 0$ $\quad \text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_1\right) = -1{,}024 \times 10^3$

$\text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_2\right) = -1{,}024 \times 10^3$ $\quad \text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_3\right) = 1{,}024 \times 10^3$

$\text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_4\right) = -1{,}024 \times 10^3$ $\quad \text{MultString}\left(\text{Sum}_0, \text{ArrayFunction}_5\right) = 0$

Вилучення

$C1 := \text{READRGB}(\text{"Stego1.bmp"})$ $\quad G1 := \text{READ\_GREEN}(\text{"Stego1.bmp"})$

$R1 := \text{READ\_RED}(\text{"Stego1.bmp"})$ $\quad B1 := \text{READ\_BLUE}(\text{"Stego1.bmp"})$

Масив рядків контейнера

$$\text{ArrayString} := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R1) - 1 \\ \quad \left| \begin{array}{l} \text{for } j \in 0..\text{cols}(R1) - 1 \\ \quad a_j \leftarrow R1_{i,j} \\ \text{ArrayString}_i \leftarrow a \end{array} \right. \\ \text{ArrayString} \end{array} \right.$$

Порівняння отриманого та вбудованого повідомлень

$$m1 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R1) - 1 \\ \quad \text{for } j \in 0..k - 1 \\ \quad \left| \begin{array}{l} m1_{k \cdot i + j} \leftarrow 1 \text{ if } \text{MultString}\left(\text{ArrayString}_i, \text{ArrayFunction}_{j+1}\right) > 0 \\ m1_{k \cdot i + j} \leftarrow -1 \text{ if } \text{MultString}\left(\text{ArrayString}_i, \text{ArrayFunction}_{j+1}\right) \le 0 \end{array} \right. \\ m1 \end{array} \right.$$

Перетворюємо повідомлення на бінарний вид

$m2 := m2b(m1)$

$$M1 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(m2) - 8 \\ \quad \left| \begin{array}{l} l \leftarrow \text{floor}\left(\frac{i}{8}\right) \\ \text{for } j \in 0..7 \\ \quad V_j \leftarrow m2_{l \cdot 8 + j} \\ M_l \leftarrow B2D(V) \end{array} \right. \\ M \end{array} \right.$$

$$WRITEBIN("STEGOTXT1.txt", "byte", 1) := M1$$

Розрахунок ймовірності помилкового вилучення інформаційних бітів

$$Posh = 0$$

$$Posh := \left| \begin{array}{l} a \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(m2) - 1 \\ \quad a \leftarrow a + 1 \text{ if } m2_i \neq M\_b_i \\ Posh \leftarrow \frac{a}{\text{rows}(m2)} \\ Posh \end{array} \right.$$

$$W\_k := \begin{pmatrix} 0 & 0 \\ 1 & 0,39 \\ 2 & 0,39 \\ 4 & 0,586 \\ 8 & 0,871 \\ 16 & 1,244 \\ 32 & 1,723 \\ 64 & 2,385 \\ 128 & 3,286 \\ 256 & 4,5 \end{pmatrix} \quad Posh\_k := \begin{pmatrix} 0 & 0 \\ 1 & 0,006 \\ 2 & 0,053 \\ 4 & 0,093 \\ 8 & 0,121 \\ 16 & 0,126 \\ 32 & 0,145 \\ 64 & 0,148 \\ 128 & 0,148 \\ 255 & 0,15 \end{pmatrix}$$

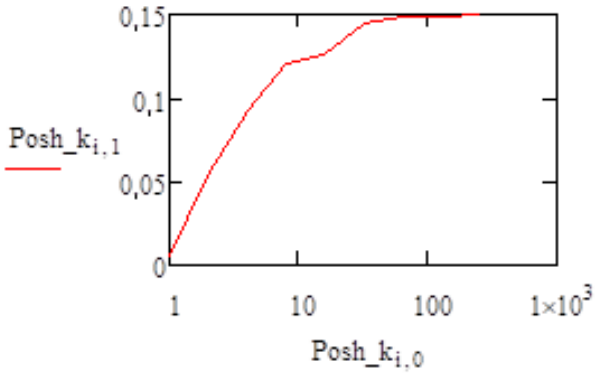
$$W\_g := \begin{pmatrix} 1 & 0,586 \\ 2 & 1,17 \\ 3 & 1,754 \\ 4 & 2,338 \end{pmatrix} \quad Posh\_g := \begin{pmatrix} 1 & 0,093 \\ 2 & 0,018 \\ 3 & 0,003 \\ 4 & 0 \end{pmatrix}$$

Розрахунок частки внесених викривлень в контейнер-повідомлення:

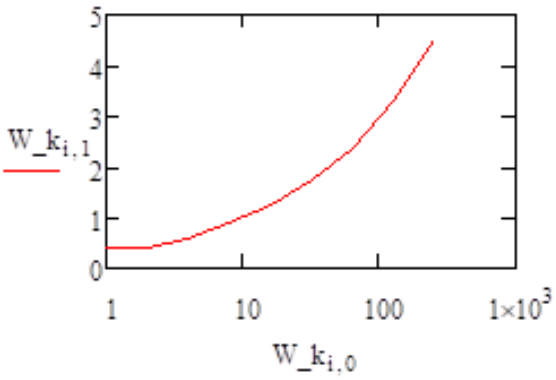
$$w := \left| \begin{array}{l} w \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(R1) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R1) - 1 \\ \quad\quad w \leftarrow w + \left| R1_{i,j} - R_{i,j} \right| \\ w \leftarrow \frac{w \cdot 100}{\text{rows}(R1) \cdot \text{cols}(R1) \cdot 256} \\ w \end{array} \right.$$

$w = 1,699$ $\quad i := 0..9$

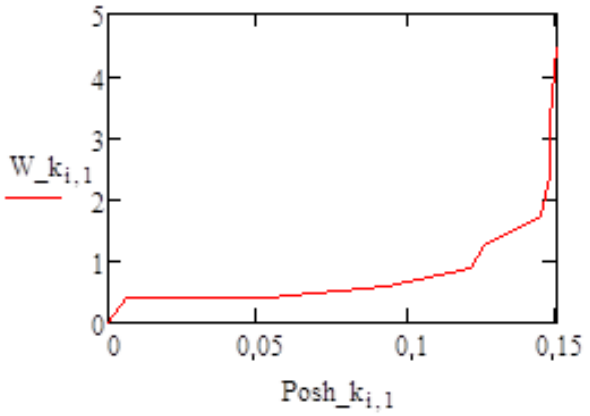
Ймовірність помилки від кількості вбудованих бітів



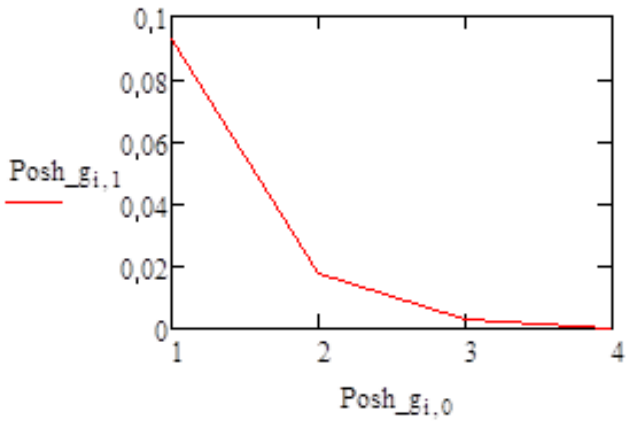
Коефіцієнт внесених спотворень від кількості вбудованих бітів



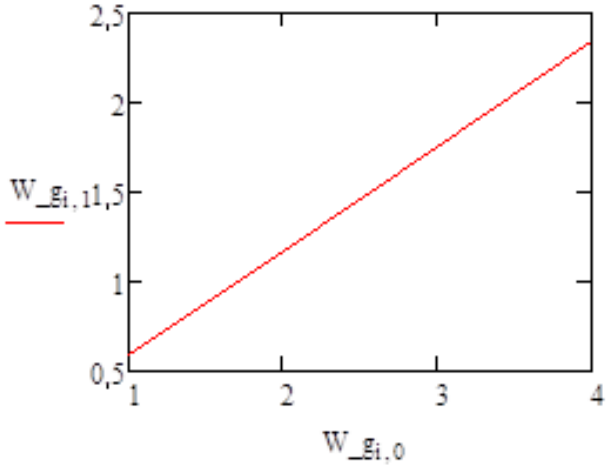
Залежність внесених спотворень та ймовірність правильного вилучення



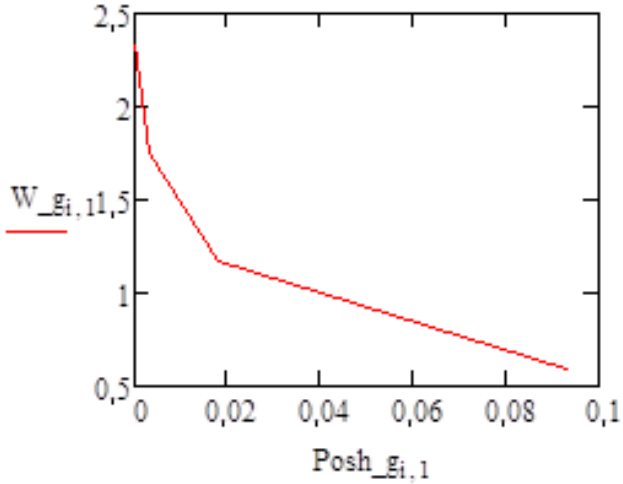
Залежність правильного вилучення від коефіцієнта посилення



Залежність внесених спотворень від коефіцієнта посилення



Залежність внесених спотворень та ймовірності правильного вилучення



Багатоосновне стеганографічне кодування

Формуємо квазіортогональні дискретні сигнали

```
ArrayFunction1 := | for i ∈ 0..1023
                  |   for j ∈ 0..255
                  |     b ← ceil(rnd(2)) − 1
                  |     a_j ← 1  if b = 1
                  |     a_j ← −1  if b = 0
                  |   ArrayFunction1_i ← a
                  | ArrayFunction1
```

$$\mathrm{MultString}\left(\mathrm{ArrayFunction1}_1, \mathrm{ArrayFunction1}_2\right) = 8$$

$$\mathrm{MultString}\left(\mathrm{ArrayFunction1}_2, \mathrm{ArrayFunction1}_3\right) = 10$$

$$\mathrm{MultString}\left(\mathrm{ArrayFunction1}_1, \mathrm{ArrayFunction1}_3\right) = 18$$

Розбиваємо повідомлення на блоки по 10 бітів та формуємо десятковий масив даних

```
M_d := | for i ∈ 0..rows(R) − 1
       |   a ← 0
       |   for j ∈ 0..9
       |     a ← a + M_b_(10·i+j)·2^j
       |   M_d_i ← a
       | M_d
```

Замінюємо блок з 10 бітів на відповідну йому ПВП

$$g := 4$$

```
Sum1 := | for i ∈ 0..rows(R) − 1
        |   Sum1_i ← g·ArrayFunction1(M_d_i)
        | Sum1
```

Вбудовуємо отримане модульоване повідомлення в контейнер

```
S1 := | for i ∈ 0..rows(R) − 1
      |   for j ∈ 0..cols(R) − 1
      |     S1_(i,j) ← R_(i,j) + (Sum1_i)_j
      |     S1_(i,j) ← 255  if S1_(i,j) > 255
      |     S1_(i,j) ← 0  if S1_(i,j) < 0
      | S1
```

Перетворюємо вилучене повідомлення на бітовий вигляд

$$M\_b2 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(M\_d1) - 1 \\ \quad x \leftarrow M\_d1_i \\ \quad \text{for } j \in 0..9 \\ \quad\quad M\_b2_{i\cdot 10+j} \leftarrow \text{mod}(x, 2) \\ \quad\quad x \leftarrow \text{floor}\left(\frac{x}{2}\right) \\ M\_b2 \end{array} \right.$$

$$M2 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(M\_b2) - 8 \\ \quad l \leftarrow \text{floor}\left(\frac{i}{8}\right) \\ \quad \text{for } j \in 0..7 \\ \quad\quad V_j \leftarrow M\_b2_{l\cdot 8+j} \\ \quad M_l \leftarrow B2D(V) \\ M \end{array} \right.$$

WRITEBIN("STEGOTXT2.txt","byte" ,1) := M2

Розрахунок ймовірності помилкового вилучення інформаційних бітів

$$Posh := \left| \begin{array}{l} a \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(M\_b2) - 1 \\ \quad a \leftarrow a + 1 \text{ if } M\_b2_i \neq M\_b_i \\ Posh \leftarrow \frac{a}{\text{rows}(M\_b2)} \\ Posh \end{array} \right.$$

Posh = 0,199

$$Posh\_g1 := \begin{pmatrix} 1 & 0{,}493 \\ 5 & 0{,}479 \\ 10 & 0{,}464 \\ 15 & 0{,}434 \\ 20 & 0{,}368 \\ 25 & 0{,}238 \\ 30 & 0{,}2 \\ 35 & 0{,}151 \\ 40 & 0{,}104 \end{pmatrix}$$

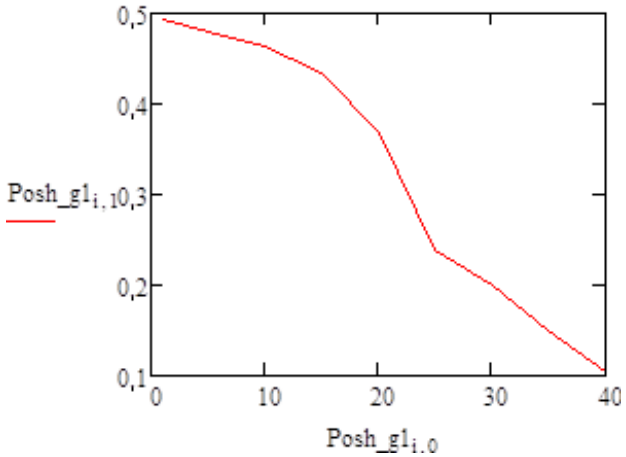
Розрахунок частки внесених спотворень в контейнер-зображення

$$w := \left| \begin{array}{l} w \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(R2) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\ \quad\quad w \leftarrow w + \left| R2_{i,j} - R_{i,j} \right| \\ w \leftarrow \frac{w\cdot 100}{\text{rows}(R2)\cdot\text{cols}(R2)\cdot 256} \\ w \end{array} \right.$$

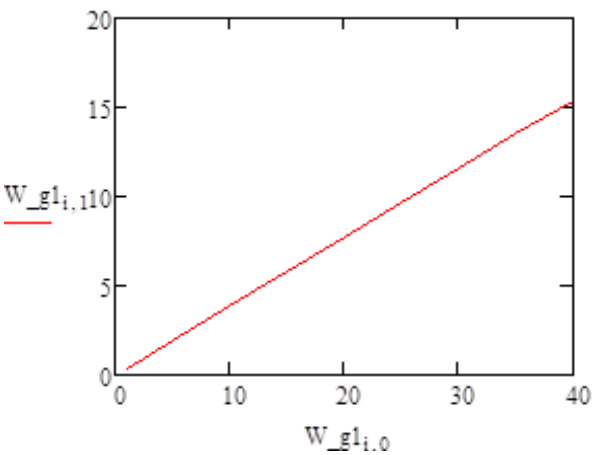
$$W\_g1 := \begin{pmatrix} 1 & 0{,}39 \\ 5 & 1{,}951 \\ 10 & 3{,}897 \\ 15 & 5{,}838 \\ 20 & 7{,}771 \\ 25 & 9{,}692 \\ 30 & 11{,}596 \\ 35 & 13{,}473 \\ 40 & 15{,}331 \end{pmatrix}$$

w=1,286

Залежність ймовірності помилки від коефіцієнта посилення



Залежність внесених спотворень від коефіцієнта посилення



Адаптивне формування дискретних сигналів

```
R_Arr := | for i ∈ 0.. rows(R) − 1
         |     for j ∈ 0.. 255
         |       a_j ← R_(i,j)
         |     R_Arr_i ← a
         | R_Arr
```

Адаптивно формуємо квазіортогональні дискретні сигнали

```
ArrayFunction2 := | i ← 0
                  | while i < 1024
                  |     for j ∈ 0.. 255
                  |         b ← ceil(rnd(2)) − 1
                  |         a_j ← 1 if b = 1
                  |         a_j ← −1 if b = 0
                  |     ArrayFunction2_i ← a
                  |     b ← 0
                  |     jj ← 0
                  |     while jj < rows(R_Arr) ∧ b = 0
                  |         a ← MultString(R_Arr_jj, ArrayFunction2_i)
                  |         b ← b + 1 if |a| > 1000
                  |         jj ← jj + 1
                  |     i ← i + 1 if b = 0
                  | ArrayFunction2
```

$\text{MultString}(R\_Arr_2, ArrayFunction2_2) = 29 \quad \text{MultString}(ArrayFunction_1, ArrayFunction2_2) = -2$

Вилучаємо блоки по 10 бітів з рядків контейнера

```
M_d2 := | for i ∈ 0.. rows(R3) − 1
        |     a ← 0
        |     for j ∈ 0.. 1023
        |       if MultString(ArrayString2_i, ArrayFunction2_j) > a
        |           a ← MultString(ArrayString2_i, ArrayFunction2_j)
        |           M_d2_i ← j
        | M_d2
```

Перетворюємо вилучене повідомлення на бітовий вигляд

$$M\_b3 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(M\_d2) - 1 \\ \quad \left| \begin{array}{l} x \leftarrow M\_d2_i \\ \text{for } j \in 0..9 \\ \quad \left| \begin{array}{l} M\_b3_{i \cdot 10 + j} \leftarrow \text{mod}(x, 2) \\ x \leftarrow \text{floor}\left(\frac{x}{2}\right) \end{array} \right. \end{array} \right. \\ M\_b3 \end{array} \right.$$

$$M3 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(M\_b3) - 8 \\ \quad \left| \begin{array}{l} l \leftarrow \text{floor}\left(\frac{i}{8}\right) \\ \text{for } j \in 0..7 \\ \quad V_j \leftarrow M\_b3_{l \cdot 8 + j} \\ M_l \leftarrow B2D(V) \end{array} \right. \\ M \end{array} \right.$$

WRITEBIN("STEGOTXT3.txt","byte" ,1) := M3

Розрахунок ймовірності помилкового вилучення інформаційних бітів

$$Posh := \left| \begin{array}{l} a \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(M\_b3) - 1 \\ \quad a \leftarrow a + 1 \text{ if } M\_b3_i \neq M\_b_i \\ Posh \leftarrow \frac{a}{\text{rows}(M\_b3)} \\ Posh \end{array} \right.$$

$$Posh\_g3 := \begin{pmatrix} 1 & 0{,}47 \\ 2 & 0{,}43 \\ 3 & 0{,}373 \\ 4 & 0{,}224 \\ 5 & 0{,}121 \\ 6 & 0{,}051 \\ 7 & 0{,}015 \\ 8 & 0{,}005 \\ 9 & 0 \end{pmatrix} \qquad Posh\_g := \begin{pmatrix} 1 & 0{,}093 \\ 2 & 0{,}018 \\ 3 & 0{,}003 \\ 4 & 0 \end{pmatrix}$$

Posh = 0,062

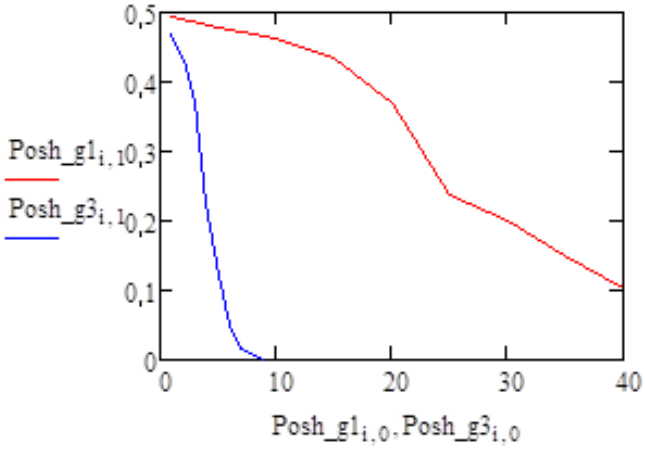
Розрахунок частки внесених спотворень в контейнер-зображення

$$w := \left| \begin{array}{l} w \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(R3) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R3) - 1 \\ \quad\quad w \leftarrow w + \left| R3_{i,j} - R_{i,j} \right| \\ w \leftarrow \frac{w \cdot 100}{\text{rows}(R3) \cdot \text{cols}(R3) \cdot 256} \\ w \end{array} \right.$$

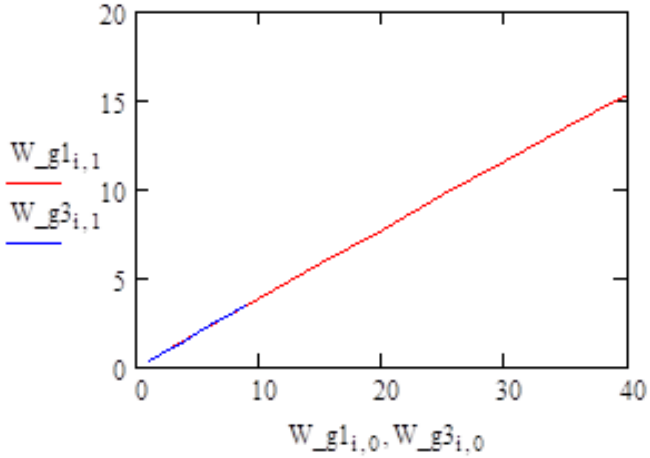
$$W\_g3 := \begin{pmatrix} 1 & 0{,}39 \\ 2 & 0{,}78 \\ 3 & 1{,}171 \\ 4 & 1{,}561 \\ 5 & 1{,}951 \\ 6 & 2{,}34 \\ 7 & 2{,}73 \\ 8 & 3{,}119 \\ 9 & 3{,}508 \end{pmatrix} \qquad W := \begin{pmatrix} 1 & 0{,}586 \\ 2 & 1{,}17 \\ 3 & 1{,}754 \\ 4 & 2{,}338 \end{pmatrix}$$

w = 1,285

Залежність помилки вилучення від коефіцієнта посилення



Залежність внесених спотворень від коефіцієнта посилення



Навчальне видання

Кузнецов Олександр Олександрович
Полуяненко Микола Олександрович
Кузнецова Тетяна Юріївна

ПРИХОВУВАННЯ ДАНИХ У ПРОСТОРОВІЙ ОБЛАСТІ НЕРУХОМИХ ЗОБРАЖЕНЬ НА ОСНОВІ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА

Методичні рекомендації
до лабораторної роботи з дисципліни «Стеганографія»
для студентів спеціальності 125 «Кібербезпека»

Коректор *Б. О. Хільська*
Комп'ютерне верстання *Л. П. Зябченко*
Макет обкладинки *І. М. Дончик*

Формат 60×84/16. Ум. друк. арк. 3,78. Наклад 50 пр. Зам № 143/19.

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009

Видавництво ХНУ імені В. Н. Каразіна
Тел. 705-24-32