УДК 681.32

В.В. КІЛКО, А.В. СОКОЛОВ, Н.М. БАЛАНДИНА

Національний університет Одеська політехніка

СТЕГАНОГРАФІЧНИЙ МЕТОД З КОДОВИМ УПРАВЛІННЯМ ТА СЛІПИМ ДЕКОДУВАННЯМ ДЛЯ ЦИФРОВИХ ВІДЕО

Вступ. Зростання мультимедійного контенту підвищує значення стеганографії для захисту інформації, адже вона приховує сам факт наявності даних на відміну від криптографії, яка вимагає ключа. Попри вже існуючі методи, тривають дослідження для підвищення стійкості до атак, пропускної здатності, надійності й ефективності.

Сучасні ресурсообмежені платформи, зокрема IoT та мобільні пристрої, потребують стеганографічних методів із високою обчислювальною ефективністю. Це актуально для потокових контейнерів, а методи перетворення (дискретне косинусне, вейвлет тощо) можуть не підійти. Одним із прикладів є стеганографія з кодовим управлінням у просторі, яка демонструє високу стійкість. Незважаючи на переваги, цей метод залежить від оригінального контейнера, що може ускладнювати його практичне застосування з цифровим відео.

У цій роботі пропонується модифікація, яка дозволяє сліпе декодування без оригіналу, що є корисним для передачі даних з дронів, де окремий канал для контейнера недоцільний.

Мета: Підвищення ефективності стеганоперетворення відео контейнерів із застосуванням стеганографічного алгоритму з кодовим управлінням та сліпим декодуванням.

1. Практична реалізація алгоритму

Основною ідеєю є можливость сліпого декодування додаткової інформації у стеганографічному методі з кодовим управлінням при роботі з відео контейнерами.

Розглянемо послідовність кадрів відео

$$F_1, F_2, ..., F_g,$$

де g - загальна кількість кадрів, тоді як кожний кадр $F_i, i = 1, 2, ..., g$ представлений трьома матрицями розміру $n \times m$, кожна з яких вміщує значення відповідної кольорової компоненти.

Необхідно зазначити, що у реальних контейнерах - цифрових відео - зміна сцен відбувається повільно, тому присутня значна кореляція між кадрами, зазвичай (за винятком різкої зміни сцен) елементи кадрів змінюються від кадру до кадру несуттєво і повільно.

Як показують проведені експерименти, даний факт може бути застосований для побудови ефективного стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації і сліпим декодуванням для контейнерів - цифрових відео [1].

В якості основи запропонованого стеганографічного методу застосовуються кодові слова T_μ розміру $\mu \times \mu$, що побудовані шляхом послідовного заповнення

елементів матриці T_μ елементами обраного рядка матриці Уолша-Адамара порядку μ^2, яка будується відповідно до конструкції Сільвестра.

$$H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{bmatrix}, H_1 = [1]. \quad (1)$$

Застосування кодових слів, що побудовані на основі рядків матриці Уолша-Адамара порядку μ^2 для вбудовування додаткової інформації у стеганографічному методі з кодовим управлінням, дозволяє домогтися зосередженого впливу на обрану частотну компоненту контейнера.

При цьому, в роботі показані кодові слова, що здійснюють вбудовування додаткової інформації в низькочастотні та середньочастотні компоненти контейнеру, і, таким чином, дозволяють забезпечити стійкість стеганоповідомлення до атак проти вбудованого повідомлення, подальше узагальнення зазначених кодових слів було проведено в роботі.

Зазначені кодові слова пропонується використовувати і в запропонованій модифікації стеганографічного методу.

Наведемо запропонований алгоритм вбудовування додаткової інформації у вигляді конкретних кроків.

Вхід: відеоряд кадрів контейнера $F_i, i = 1,2,...,g$, послідовність бітів додаткової інформації $d_j \in \{0,1\}$, $j = 1,2,...,gmn/2\mu^2$, кодове слово T_μ розміру $\mu \times \mu$, що обрано для вбудовування додаткової інформації.

Вихід: відеоряд кадрів з вбудованим стеганоповідомленням $S_i, i = 1,2,...,g$.

Крок 1. Визначаємо значення лічильників $i = 1, i_{AI} = 1$.

Крок 2. Послідовно обираємо пару кадрів F_i і F_{i+1}, розбиваємо кожний з кадрів на блоки $X_{l,(F_1)}$ та $X_{l,(F_2)}$ $l = 1,2,...,mn/\mu^2$ заданого розміру $\mu \times \mu$.

Крок 3. Для вбудовування у пару кадрів F_i і F_{i+1} обираємо чергові біти $d'_k = d_{i_{AI}\mu^2+k}, k = 1,2,...,nm/\mu^2$ інформації з послідовності d_j, $j = 1,2,...,gmn/2\mu^2$.

Крок 4. Здійснюємо вбудовування додаткової інформації у блоки кадру F_i адитивним способом, де кожний блок стеганоповідомлення визначається як

$$\begin{cases} M_{l,(F_1)} = X_{l,(F_1)} + (-1)^{\overline{d_k}} T_\mu, \\ M_{l,(F_2)} = X_{l,(F_2)} + (-1)^{d_k} T_\mu, \end{cases} \quad (2)$$

де $M_{l,(F_1)}$ і $M_{l,(F_2)}$, $l = 1,2,...,mn/\mu^2$ - блоки стеганоповідомлення кадрів S_i, S_{i+1} розміру $\mu \times \mu$, запис $\overline{d_k}$ означає інверсію біта d_k.

Крок 5. Збільшити лічильники $i = i + 2, i_{AI} = i_{AI} + 1$. Якщо $i \geq g$ зупин, інакше - перейти на Крок 2.

Наведемо запропонований алгоритм вилучення додаткової інформації у вигляді конкретних кроків:

Вхід: відеоряд кадрів з вбудованим стеганоповідомленням $S_i, i = 1,2,...,g$,

кодове слово T_μ розміру $\mu \times \mu$, що відповідає кодовому слову, яке застосовувалося для вбудовування додаткової інформації.

Вихід: послідовність бітів додаткової інформації $d_j \in \{0,1\}$, $j = 1, 2, ..., gmn/2\mu^2$.

Крок 1. Визначаємо значення лічильників $i = 1, i_{AI} = 1$.

Крок 2. Послідовно обираємо пару кадрів S_i і S_{i+1}, розбиваємо кожний з кадрів на блоки $M_{l,(F_1)}$ та $M_{l,(F_2)}$ $l = 1, 2, ..., mn/\mu^2$ заданого розміру $\mu \times \mu$.

Крок 3. Знаходимо для кожної пари кадрів S_i і S_{i+1} матрицю різниці

$$\Delta_l = M_{l,(F_2)} - M_{l,(F_1)}, l = 1, 2, ..., mn/\mu^2 . \quad (3)$$

Крок 4. Знаходимо значення вбудованих у дану пару кадрів mn/μ^2 бітів додаткової інформації

$$d_{i_{AI}\mu^2 + l} = \sum_{i_1=1}^{\mu} \sum_{i_2=1}^{\mu} \Delta_l(i_1, i_2) T_\mu(i_1, i_2) , \quad (4)$$

де запис $\Delta_l(i_1, i_2)$ і $T_\mu(i_1, i_2)$ означає вибірку елементу з індексами i_1, i_2 з відповідних матриць.

Крок 5. Збільшити значення лічильників $i = i + 2, i_{AI} = i_{AI} + 1$. Якщо $i \geq g$ зупин, інакше - перейти на Крок 2.

2. Експерименти зі стійкістю

Експеримент 1. Визначення стійкості запропонованого стеганографічного методу до атак стисненням алгоритмом MPEG-4 проти вбудованого при застосуванні кодових слів, що впливають на високочастотну трансформанту перетворення Уолша-Адамара (2,2):

$$T_{16,(2,2)} = \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix}, \quad (5)$$

на трансформанту перетворення Уолша-Адамара (1,9):

$$T_{16,(1,9)} = \begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\ -1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1 \end{bmatrix}, \quad (6)$$

а також кодове слово, що впливає на постійну складову (1,1):

$$T_{\mu,(1,1)} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}. \quad (7)$$

Атаки стисненням проти вбудованого повідомлення є природною частиною як зберігання так і передавання стеганоповідомлень, наприклад із застосуванням сучасних ІМ месенджерів. Таким чином, для сучасного стеганографічного методу важливою є можливість протистояти таким атакам.

Для проведення даного експерименту була використана база з 150 цифрових відео з різними властивостями відеоряду, в які здійснювалося вбудовування додаткової інформації із застосуванням модифікованого стеганографічного методу.

При цьому для забезпечення найбільшої стійкості до атаки стисненням, вбудовування додаткової інформації виконувалося у компоненту Y у просторі YCbCr кадрів зображення як було зазначено в роботі, тоді як для вбудовування додаткової інформації застосовувалися кодові слова (5), (6), (7).

Отримане стеганоповідомлення стискалося за допомогою алгоритму стиснення MPEG-4. Далі із стисненого відео проводилося вилучення додаткової інформації із фіксацією кількості помилок, що відбулися при декодуванні додаткової інформації. Результати щодо кількості помилок наведені у таблиці 1.

Таблиця 1 - Відсотки помилок декодування під впливом атаки стисненням проти вбудованого повідомлення для різних кодових слів

Кодове слово / QF	**100**	**90**	**80**	**70**	**60**	**50**	**40**	**30**	**20**	**10**
$T_{16,(2,2)}$	10.3	11.4	15.5	24.6	37.1	47.8	50	50	50	50
$T_{16,(1,9)}$	1.3	1.3	1.5	2.6	6.0	13.1	22.1	30.2	36.8	44.4
$T_{8,(1,1)}$	1.6	1.6	1.8	3.0	6.4	13.2	21.7	29.1	35.5	42.7

Аналіз даних табл. 1 дозволяє дійти висновку, що найкращими властивостями у сенсі протистояння атакам проти вбудованого повідомлення володіє кодове слово $T_{16,(1,9)}$, що впливає на низькочастотні складові контейнеру та забезпечує найнижчі показники відсотку помилок при вилученні додаткової інформації для значень $QF = 60...100$.

При нижчих значення QF кодове слово $T_{8,(1,1)}$ показує незначно кращі результати у порівнянні з кодовим словом $T_{16,(1,9)}$, тим не менш такі низькі значення QF нечасто застосовуються на практиці [2].

Окремо зазначимо, що кодове слово $T_{16,(2,2)}$, що впливає на високочастотні складові контейнеру показує найгірші результати навіть при значенні $QF = 100$, незважаючи на найнижчий рівень спотворень, що вносяться матрицею змін ε (рисунок 1), що обумовлено значним спотворенням, що вносяться алгоритмом стиску відео MPEG-4, навіть при високих значеннях показника якості QF. Таким чином, практичне застосування кодового слова $T_{16,(2,2)}$ не може бути рекомендованим при роботі з відео.

Висновок. Розроблено інноваційний алгоритм з кодовим управлінням та сліпим декодуванням, який функціонує з відео контейнерами. Цей алгоритм ретельно досліджено, зокрема вплив стиснення JPEG на можливість правильного декодування додаткової інформації, використовуючи різні кодові слова.

Результати показали, що ці кодові слова демонструють високі показники відновлення інформації навіть при стиску якості від 60 до 100, що забезпечує надійність і стабільність передачі прихованих даних.

Перелік використаних джерел.

1. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. Informatics and Mathematical Methods in Simulation. 2021. Vol. 11, No. 3, P. 147-161.

2. Надвоцький О.Ю., Кобозєва А.А.. Метод розв'язку задачі про вибір контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій. URL: http://immm.op.edu.ua/files/archive/n3_v11_2021/immm_n3_v11 _2021.pdf