DOI: 10.18372/2310-5461.69.20950
УДК 004.622: 517.927

В. В. Бараннік, д-р техн. наук, проф.
Харківський національний університет радіоелектроніки
orcid.org/0000-0002-2848-4524
e-mail: vvbar.off@gmail.com;

Д. В. Бараннік
Харківський національний університет радіоелектроніки
orcid.org/0000-0002-7074-9864
e-mail: d.v.barannik@gmail.com;

М. В. Бабенко, канд. техн. наук, доцент,
Дніпровський державний технічний університет
orcid.org/0000-0003-1013-9383
e-mail: mvbab@ukr.net;

Р. О. Прокопенко
Харківський національний університет радіоелектроніки
https://orcid.org/0009-0006-0789-9073
e-mail: rodion.prokopenko@nure.ua;

Н. М. Петруха, канд. економ. наук, доцент
Київський національний університет будівництва і архітектури
https://orcid.org/0000-0002-3805-2215
e-mail: nninna1983@gmail.com

МЕТОД ЗАХИСТУ ВІДЕОІНФОРМАЦІЇ В СИСТЕМАХ АЕРОКОСМІЧНОГО МОНІТОРИНГУ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Вступ

Питання забезпечення інформаційної безпеки в інформаційно-комунікаційних системах особливо в сегменті використання сенсорів реєстрації на базі засобів аерокосмічного моніторингу є вкрай актуальними [1; 2].

Це зумовлено суперечностями, що виникають в процесі забезпечення категорій конфіденційності, цілісності та доступності у разі обробки та передачі відеоінформаційних ресурсів в системі аерокосмічного моніторингу. В їх основі лежить критичність часових затримок на доставку відеоінформації значного бітового об'єму з використанням обмежених за швидкістю передачі інформаційно-комунікаційних засобів [3; 4].

В означених обставинах (умовах) виникає інтерес до технологій захисту інформації в процесі використання систем скорочення бітового об'єму [5; 6]. Одним з варіантів реалізації такого підходу є використання стеганографічних методів приховування інформації до контейнерів візуального походження (КВП) [3; 7]. Такими контейнерами можуть бути відеозображення або їх динамічна послідовність. Відповідно наявність набору різних типів сенсорів реєстрації видової інформації в системі аерокосмічного моніторингу створює відповідні умови для захисту інформації шляхом їх стеганографічного приховування у КВП [8; 9].

Звідси актуальною є науково-прикладна задача, яка стосується забезпечення захисту інформації з потрібним рівнем доступності та цілісності в системі аерокосмічного моніторингу на основі стеганографічних перетворень.

Аналіз сучасних досліджень та постановка завдання

Розглянемо аналіз особливостей реалізації технологій стеганографічних перетворень в залежності від [10–14]:

– методів стегнографічного вбудовування інформації;

– функціональних умов, за якими здійснюється приховування інформації згідно обраного методу вбудовування;

– простору відео-контейнеру, для якого проводиться вбудовування інформації.

Основні методи стеганографічних перетворень поділяються на такі, що за функціональною умовою здійснюють безпосереднє або непряме вбудовування інформації до відео-контейнеру [12; 15].

Підходи, які за функціональною умовою використовують метод безпосереднього вбудовування. Стеганографічний підхід безпосередньої заміни дозволяє вбудовувати біти повідомлення,

що приховується, на позиції бітів відеоконтейнеру за обраним простором. При цьому передбачається, що отримані внаслідок такого вбудовування спотворення відеозображень, будуть залишатися візуально непомітними для особи (процесу) аналізу [16; 17].

Найбільш поширеними методами безпосереднього вбудовування є методи вбудовування в найменш значний біт (LSB – Least Significant Bit) двійкового опису елементів γ-х компонент колірної моделі ВКН [18; 19]. Такий метод має найбільше практичне використання для захисту інформації шляхом її приховування за допомогою стеганографічних перетворень. Це зумовлено наступним [20; 21]:

– достатньою простою технологічної реалізації;

– достатнім рівнем апробування та практичної верифікації для різних стандартизованих інформаційних технологій;

– наявністю розвиненої теоретичної бази та побудови сімейства різних класів реалізації означеного підходу;

– наявність механізмів щодо контролю кількості інформації, яка вбудовується у КВП [22; 23].

Одним з перспективних є розвиток методів вбудовування інформації з використанням механізму LSB у квантований спектральний простір [24; 25]. В цьому разі інформація приховується в найменш значимі бітові групи коефіцієнтів дискретного косинусного перетворення (ДКП). Цей спосіб є подальшим розвитком способів вбудовування в найменш значний біт. Внаслідок застосування ДКП до елементів КВП будується матриця коефіцієнтів [26; 27]. Вбудовування здійснюється шляхом заміни молодших бітів двійкового подання коефіцієнтів ДКП на біти повідомлення, що приховується.

В класичній реалізації метод LSB має певні недоліки стосовно низької стійкості до [28; 29]:

1) активних атак зловмисника. Наприклад, така атака може полягати у перестисканні КВП. Тоді у процесі застосування такої атаки відбувається повторне усунення психовізуальної надмірності. Це призводить до виникнення додаткових спотворень та спричиняє наявності ризиків втрати прихованого повідомлення [30];

2) стегоаналізу. Наприклад, у разі створення маски КВП лише з найменш молодших бітів залишаються контури об’єктів цього відеозображення. Після реалізації стеганографічного вбудовування контури КВП зникають. Отже, у разі застосування методів стегоаналізу зловмисником неможливо забезпечити конфіденційність і цілісність інформації, що приховується.

В той же час для додатків, що пов’язані з використанням аерокосмічного сегменту, характерним є те, що інформація, яку потрібно закрити, має обмежений час «життя». Звідси використання методів стегоаналізу, які потребують часових витрат матиме обмежену актуальність. В свою чергу, механізми стегоаналізу, що включають методи перестиснення відрізняються якраз наявністю значних часових затримок. Такі затримки можуть перевищувати час «життя» інформації, яка приховується [31].

Постановка проблеми

Напрямком подальшого розвитку може бути побудова комбінованих підходів до організації стеганографічних систем в базисі стиснення. При цьому додатковою складовою пропонується використовувати технології, *які за функціональною умовою використовують метод непрямого вбудовування*. Для таких технологій на відміну від методів безпосереднього вбудовування приховування здійснюється шляхом створення та врахування залежності між деякими параметрами сегменту відео-контейнеру. Відповідно методи непрямого вбудовування інформації відрізняються різними техніками щодо створення та врахування параметрів КВП. Зворотне стеганографічне перетворення здійснюється шляхом вилучення деякої оцінки вбудованих даних.

Методи непрямого стеганографічного вбудовування можна поділити на дві базові групи, а саме: методи, для яких в процесі вилучення інформації необхідна наявність прототипу відеоконтейнеру; методи, які в процесі прямих та зворотних перетворень не передбачають наявність прототипу відео-контейнеру.

Методи мають деяку стійкість до активних атак зловмисника. Однак для нього характерна обмежена стеганографічна ємність, тобто відсутня можливість вбудовування повідомлення з великим об’ємом (наприклад, відеокадру).

Наведені методи непрямого стеганографічного перетворення мають спільні недоліки, серед яких можна виділити наступні:

1. Низьке значення стійкості стеганограми до візуальних атак зловмисника. Цей недолік обумовлений тим, що вбудовування інформації досягається шляхом модифікації елементів КВП. Це супроводжується внесенням візуальних спотворень у КВП та погіршенням його якості. У разі наявності у зловмисника початкового КВП може бути виявлений факт наявності прихованого вбудовування в стеганограмі.

2. Незадовільні характеристики за показником стеганографічної ємності, тобто низька можливість до збільшення об’єму інформації, яку потрібно приховати. Навпаки, збільшення об’єму

вбудовуваної інформації супроводжується збільшенням кількості модифікованих елементів, та як наслідок зростанням рівня втрат цілісності КВП.

Значить, необхідно розробити такий підхід для проектування стеганографічної системи, який враховує не лише психовізуальні закономірності у КВП, а й структурні залежності між елементами його синтаксичного опису.

Тому **мета досліджень** статті полягає у створенні стеганографічних перетворень в каскадному психовізуально-структурному просторі відеоконтейнерів в процесі стиснення для підвищення стеганографічної ємності з забезпеченням маскування слідів прихованої інформації.

Обґрунтування підходу для побудови комбінованих підходів до організації стеганографічних систем в базисі стиснення за умов забезпечення доступності та цілісності інформації

Для усунення виявлених недоліків існуючих методів стеганографічного вбудовування інформації пропонується побудувати підхід, який: в процесі вбудовування повідомлень буде враховувати сукупність залежностей, а саме: психовізуальні, структурні та статистичні; процес вбудовування інформації буде здійснюватися в умовах збереження потрібного рівня цілісності відеоконтейнерів; буде інтегровано у процес стиснення КВП.

Відповідно для такого методу процес стеганографічного вбудовування повинен відбуватися за умов:

1. Забезпечити вбудовування повідомлення, бітовий об'єм V_{mes} якого буде не менш заданого

$$V_{mes}^{(mp)} : V_{mes} \geq V_{mes}^{(nes)}.$$

2. Забезпечити мінімальний рівень $h_{\text{стег}}$ візуальних спотворень, що вносяться на кожному етапі стеганографічних перетворень. При цьому загальний рівень спотворень не повинен перевищувати заданий рівень ε: $h_{\text{стег}} \leq \varepsilon$.

3. Здійснювати стеганографічне вбудовування та вилучення інформації шляхом виконання такої кількості $N_{\text{опер}}$ операцій, яка буде пропорційна кількості даних, що обробляються.

В якості складової комбінованої стеганографічної системи пропонується використовувати підхід до вбудовування інформації на основі непрямих функціональних перетворень з виявленням залежностей структурного походження. В цьому напрямку одним з ефективних підходів є метод стеганографії на основі корекцій нерівномірно-вагового позиційного (НРВП) базису Ω_j. Основні принципи такого методу викладаються в роботах [1–3]. В цьому випадку вбудовування елементу λ_ξ повідомлення Λ здійснюється шляхом використання перетворень в НРВП-базисі з коефіцієнтом η корекції значення $r_{i,j}$ основи базису Ω_j. Отже маємо:

$$r'_{i,j} = r_{i,j} + \eta = \min(\max\{S(\beta)_j\}; \delta_i) + \theta \mid \theta = \\ = 1 + sign(\eta)$$

.

В наведеному виразі застосовуються наступні позначення:

1) $S(\beta)_j$ – j-а компонента КВП S з врахування ознаки β наявності попереднього прихованої інформації у КВП (наприклад з використанням методу LSB). При цьому передбачається, що обробка проводитиметься в спектральному або квантованому спектральному просторі КВП. Ознака β приймає такі значення: «0» – у разі відсутності попереднього вбудовування інформації в LSB-області; «1» – якщо ВП-контейнер вже вміщує в собі приховану інформацію, яка додається на попередньому кроці з використанням методу LSB;

2) $s_{i,j}$ – i-й елемент j-го числа в НРВП-базисі Ω_j;

3) $\min(\max\{S(\beta)_j\}; \delta_i)$ – значення функції max(S_j) визначення найбільшого значення серед елементів послідовності S_j з використанням параметру уточнення δ_1. Величина δ_1 використовується для корекції основи НРВП-базису елементів $s_{i,j}$ КВП S_j з врахуванням структурних залежностей i-х рядків. При цьому додатково обліковується наявність впливу на значення елементів ВП-контейнеру з боку процесу вбудовування інформації в LSB-області;

4) $r'_{i,j}$ – модифіковане значення основи в НРВП-базисі.

Звідси основними відмінностями комбінованої стеганографічної системи буде використання непрямого методу вбудовування інформації на основі перетворень в НРВП-базисі. При цьому забезпечуються наступні властивості комбінованих стеганографічних перетворень:

– здійснюється виявлення кількісних ознак структурного походження шляхом виявлення залежностей в КВП та побудови НРВП-базису;

– виявлення структурних залежностей для кожного КВП проводиться з врахуванням попередньої семантико-орієнтовної класифікації;

– враховується можливий вплив наявності вбудованої на попередньому етапі інформації на значення кількісних ознак структурного простору в процесі побудови НРВП-базису;

– створюються умови для вилучення прихованої інформації без втрат цілісності.

Водночас необхідно встановити ефективність такого підходу за цілісністю відновлених ВП-контейнерів у разі неавторизованого відновлення, тобто рівень приховування факту наявності вбудованої інформації (рівень стійкості до атак візуального аналізу).

Для цього потрібно забезпечити наявність технологічних механізмів щодо усунення цифрових слідів прихованої інформації у стегано-КВП у разі спроби неавторизованого доступу.

Розглянемо базові компоненти стиснення в стеганографічному НРВП-базисі.

Основним етапом перетворень з стегано-КВП в процес стиснення є обчислення значення коду N'_j для числа в НРВП-базисі. Тут велична N'_j для адаптивного ПЧ S_j в базисі Ω_j організується вже з обліком модифікованого ОПЧ $r'_{i,j}$. Для цього маємо таке співвідношення:

$$N'_j = \sum_{i=1}^{m} s_{i,j} \cdot f_{wc}(\Omega_j; r'_{i,j} | \sigma = 0) = \sum_{i=1}^{m} s_{i,j} \cdot W'(\sigma = 0)_{i,j}.$$

В даному виразі використовуються такі позначення:

$f_{wc}(\Omega_j; r'_{i,j} | \sigma = 0)$ – функціонал визначення вагових коефіцієнтів з врахуванням модифікації ОПЧ в НРВП базисі за умов $(r'_{i,j} | \sigma = 0)$ нівелювання впливу на втрату інформації за показником середньоквадратичного відхилення σ;

$W'(\sigma = 0)_{i,j}$ – ваговий коефіцієнт для *i*-го елементу КВП за умов виключення впливу стеганографічних перетворень на цілісність елементів контейнеру.

Сукупність кодових значень N'_j утворює перехідний формат представлення стегано-контейнеру. Остаточний формат будується за результатами виконання перетворення величин N'_j в системі «АПЧ – НРВП-базис» до двійкового опису. Це стосується побудови кодограми E'_j за двома її складовими E'_j та $E'(N_j)$.

Отже за умов побудови системи функціональних перетворень СТС в НРВ базисі кодовий опис системи «АПЧ – НР базис» включає до себе службово-параметричну складову $E'(\Omega_j)$ і інформаційну складову $E'(N_j)$. Це має такий опис:

$$E'_j = f_{eb}(\Omega'_j; m; E'(N_j)) = f_{eb}(\Omega'_j; m; \{\sum_{i=1}^{m} s_{i,j} \cdot W'(\sigma = 0)_{i,j}\}_2)$$

де $\{\sum_{i=1}^{m} s_{i,j} \cdot W'(\sigma = 0)_{i,j}\}_2$ – двійковий зміст кодограми $E'(N_j)$;

$f_{eb}(\Omega'_j; m; \{\sum_{i=1}^{m} s_{i,j} \cdot W'(\sigma = 0)_{i,j}\}_2)$ – функціонал формування кодограми $E'(N_j)$ для кодового значення N'_j в системі «АПЧ – НРВ базис» за умов вбудовування прихованої інформації без втрат цілісності ВП-контейнеру.

В процесі вбудовування на основі СТС в НРВ базисі необхідно враховувати можливість виникнення слідів зміни процесу стиснення. Це відбувається, коли довжина $V(N')_j$ кодограми $E'(N_j)$ збільшується відносно довжини $V(N)_j$ кодограми $E(N_j)$ за умов відсутності вбудованої інформації. Маємо наслідки, що описуються нерівністю: $E'(N_j) \geq E(N_j)$.

Означена особливість стеганографічних перетворень трактується, як виникнення кількості штучно-генерованої надмірності. Причиною такого прояву зумовлено процесом модифікації величини ОПЧ в НРВ базисі. Схематично процес внесення штучної надмірності та виникнення слідів стеганографічних перетворень з ВП-контейнером представлено на рис. 1.

Різницю H_j між величинами $V(N')_j$ та $V(N)_j$ визначатимемо, як кількість надлишкової надмірності стеганографічних перетворень. Оцінимо величину H_j кількості надмірності. Зрозуміло, що надлишкова надмірність з'являється для кодограми $E'(N_j)$ бітового опису інформативної частини ВП-контейнеру в наслідок стеганографічного вбудовування інформації шляхом модифікації величини r_j ОПЧ в НРВ базисі. Відповідно до фізичного походження величина H_j буде за умови $r'_{1,j} \geq r_{1,j}$ приймати значення за наступним математичним описом:

$$H_j = V(N')_j - V(N)_j.$$

Конкретизуємо математичний вираз для оцінювання величини H_j. Для цього потрібно надати розгорнутий запис величин $V(N')_j$ та $V(N)_j$. Такий запис базується на властивостях НРВ-позиційного базису, та залежатиме від потужності m алфавіту базису та величин ОПЧ: $r'_{i,j}$ і $r_{i,j}$. З оглядом на це матимемо:

$$H_j = \left[\ell og_2\left(W_j^{(\max)} + \eta \cdot r_j^{m-1}\right)\right] + 1 - \left[\ell og_2 W_j^{(\max)}\right] + 1 \text{(біт)}.$$

З огляду даного виразу слідує те, що кількість H_j надлишкової надмірності за умов стеганографічного вбудовування інформації залежить від величини η – коефіцієнту модифікації значення $r_{i,j}$ ОПЧ в НРВ базисі. Звідси зрозумілим є те, що для локалізації можливої кількості стеганографічної надмірності та усунення наслідків приховування інформації, ***пропонується*** обирати величину коефіцієнту на рівні η = 1.

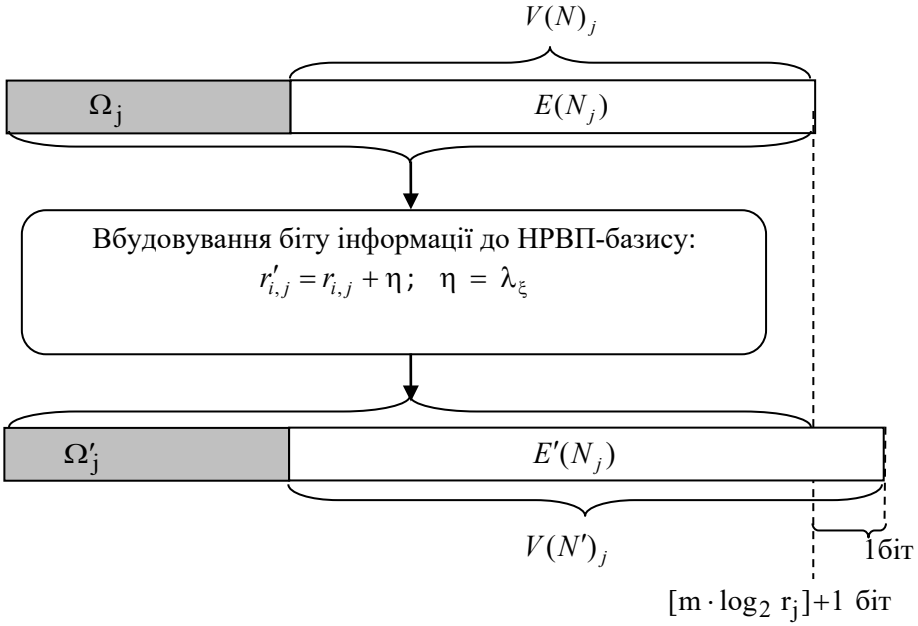

Рис. 1. Схема утворення штучної надмірності в процесі формування кодограми кодового опису чисел в НРВП-базисі за рахунок модифікації основи

Дійсно, тоді матимемо

$$H_j = \left\lceil \ell og_2 \left(W_j^{(\max)} + \eta \cdot r_j^{m-1} \right) \right\rceil + 1 - \left\lceil \ell og_2 W_j^{(\max)} \right\rceil + 1 \geq \geq \left\lceil \ell og_2 \left(W_j^{(\max)} + 1 \cdot r_j^{m-1} \right) \right\rceil - \left\lceil \ell og_2 W_j^{(\max)} \right\rceil \xrightarrow{r_{1,j}=1} 1 \text{ біт}.$$

Тому для зменшення кількості H_j доданої надмірності, що вноситься в процесі вбудовування інформації необхідно здійснювати вбудовування інформації з базуванням на її двійковий опис. Тобто фактично $\eta = \lambda_\xi$, та відповідно значення вбудованих елементів будуть обмежуватись величиною η = 1.

З оглядом на те, що стеганографічне вбудовування інформації шляхом корекції НРВП-базису буде управлятися значенням λ_ξ, тобто:

$$r'_{i,j} = \min(\max\{S_j\}; \delta_1) + 1 + \lambda_\xi = \begin{cases} \min(\max\{S(\beta)_j\}; \delta_1) + 1, \to \lambda_\xi = 0; \\ \min(\max\{S(\beta)_j\}; \delta_1) + 2, \to \lambda_\xi = 1. \end{cases}$$

Дане співвідношення дозволяє безвтратно вбудовувати інформацію непрямим способом з виявленням структурних залежностей шляхом управляючої корекції НРВП-базису за умов: наявності попередньо-вбудованої інформації; усунення цифрових слідів наявності прихованої інформації.

За таких умов процес вилучення прихованої інформації в базисі стиснення описується у вигляді структурно-функціональної схеми на рис. 2.

Порівняльна характеристика методів стиснення

Розглянемо оцінку величини $v_{relativ}^{(m)}$ відносної стеганографічної ємності методів вбудовування інформації. Значення відносної стеганографічної ємності показує відношення об'єму $v_{hid}^{(m)}$ вбудованої інформації відносно об'єму V_{vcn} відеозображення-КВП у відсотках. Така величина використовується для оцінки ефективності стеганографічної системи за усередненим об'ємом вбудованої інформації відносно об'єму відеозображення-КВП.

Величина $v_{relativ}^{(m)}$ відносної стеганографічної ємності системи визначається формулою:

$$v_{relativ}^{(m)} = \frac{v_{hid}^{(m)}}{V_{vcn}} = \frac{3 \cdot Q_{row} \cdot Q_{col}}{m \cdot V_{vcn}}.$$

Фізичний зміст даної величини кроїться у тому, що визначається оцінка кількості біт почат-

кового відеозображення-ВКН, яке відповідає одному біту прихованого повідомлення.

У відсотках значення відносної стеганографічної ємності системи оцінюється за допомогою виразу:

$$v_{relativ}^{(m)} = \frac{v_{hid}^{(m)}}{V_{vcn}} \cdot 100\% = \frac{3 \cdot Q_{row} \cdot Q_{col}}{m \cdot V_{vcn}} \cdot 100\%.$$

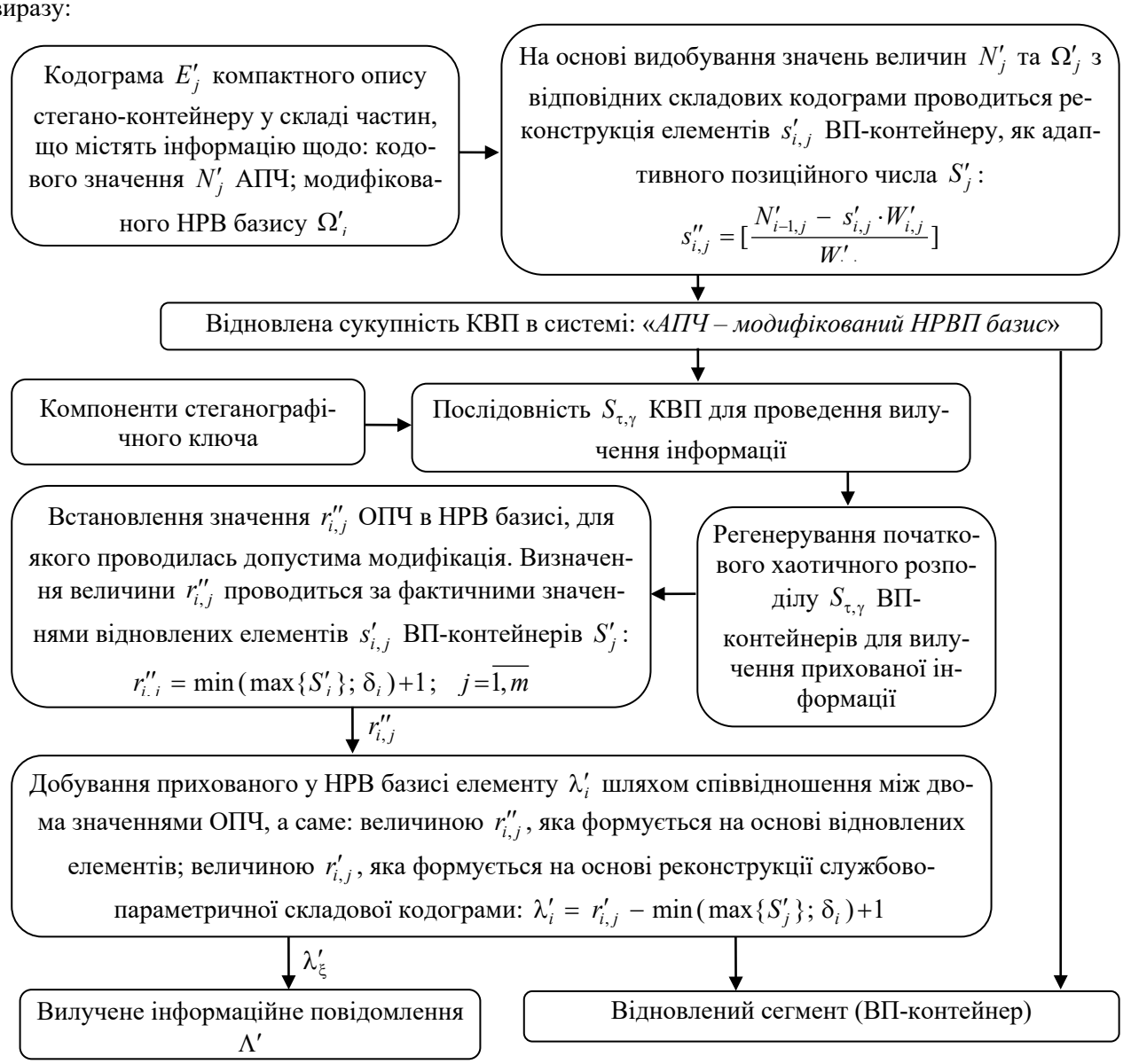

Рис. 2. Схема зворотного процесу стеганографічних перетворень щодо вилучення інформації під час декомпресії КВП в корегованому НРВП-базисі

Проведемо порівняльне оцінювання відносної бітової стеганографічної ємності $v_{relativ}^{(m)}$ для розробленої комплексної стегано-системи (РКМ) та методу вбудовування LSB. Порівняльне оцінювання будемо проводити для методу LSB в умовах його застосування для спектрального простору з різними параметрами m щодо кількості біт вбудованих на кількість спектральних елементів. При цьому обирається параметр процесу квантування q.

Відповідні оцінки представлені в табл. 1. Значення пікового відношення сигнал/шум (ПВСШ) розраховується з обліком впливу параметру процесу квантування та додаткової модифікації спектральних елементів в результаті вбудовування біту прихованого повідомлення.

З аналізу даних в табл. 1 можна заключити, що при однакових значеннях відносної стеганографічної ємності перевага для розробленого методу відносно методу LSB за рівнем ПВСШ складає: для параметру квантування $q=1$ в середньому 10 %; для параметру квантування $q=2$ від 10 % до 15 % в залежності від розміру фрагменту-ВКН та відношення кількості вбудованих біт до кількості спектральних елементів.

Висновки

1. Створено метод безвтратного вбудовувати інформацію непрямим способом з виявленням структурних залежностей шляхом управляючої корекції НРВП-базису за умов: наявності попередньо-вбудованої інформації; усунення цифрових слідів наявності прихованої інформації.

2. Розроблено метод вилучення інформації в стегано-корегованому НРВП-базисі. Відмінності методу стосуються того, що вилучення інформації здійснюється з виключенням втрат шляхом порівняння реального та контрольного значень основ НРВП-базису в умовах усунення впливу на стегано-підкладку попереднього етапу стеганоперетворень в квантовано-спектральному просторі КВП. Це дозволяє підвищити рівень стеганографічної ємності за умов виключення втрат прихованої інформації та синтаксичного опису ВКП.

Таблиця 1

Залежність величини $v_{relativ}^{(m)}$ від ПВСШ

Відносна ємність, $v_{relativ}^{(m)}$ % (біт/пкс)	Метод стеганографічного вбудовування		Значення ПВСШ, дБ	
			Складне за змістом відеозображення	Низько-інформативне відеозображення
6,25 (50 біт/пкс) 1 біт - 2 елементи	LSB(m ; q)	$q=1$	26,67	29,62
		$q=2$	23,17	25,13
		$q=4$	18,69	21,79
	РКМ	$m=4$, $q=1$	28,7	30,1
	РКМ	$m=4$, $q=2$	25,074	27,052
3,1 (25 біт/пкс) 1 біт - 4 елементи	LSB(m ; q)	$q=1$	32,12	34,43
		$q=2$	24,43	27,45
		$q=4$	21,54	23,03
	РКМ	$m=4$, $q=2$	27,4	28,3
1,56 (12,5 біт/пкс) 1 біт - 8 елементів	LSB(m ; q)	$q=2$	27	30
	РКМ	$m=4$, $q=2$	29	31

3. Експериментальне оцінювання методів стеганографічних перетворень встановило наступне. Для однакових значеннях відносної стеганографічної ємності перевага для розробленого методу відносно методу LSB за рівнем цілісності (показник пікового відношення сигнал/шум – ПВСШ) складає: для параметру квантування $q=1$ в середньому 10 %; для параметру квантування $q=2$ від 10% до 15 % в залежності від розміру фрагменту-контейнеру та відношення кількості вбудованих біт до кількості спектральних елементів.

ЛІТЕРАТУРА

[1] Barannik, V., Yudin, O., Boiko, Y., Ziubina, R., Vyshnevska, N. (2019). Video Data Compression Methods in the Decision Support Systems. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. DOI: 10.1007/978-3-319-91008-6_30.

[2] V. Barannik, D. Barannik, V. Fustii, M. Parkhomenko. Evaluation of Effectiveness of Masking Methods of Aerial Photographs. 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 415–418, DOI: 10.1109/AIACT.2019.8847820.

[3] Баранник В.В. Основы теории структурно-комбинаторного стеганографического кодирования: монография / В. В. Баранник, Д. В. Баранник, А.Е. Бекиров. Х.: Издательство «Лидер», 2017. 256 с.

[4] Kim-Hui Yap, Wenyang Liu, Yi Wang, Lap-Pui Chau. Bitstream-Corrupted JPEG Images Are Restorable: Two-Stage Compensation and Alignment Framework for Image Restoration. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023, PP. 9979-9988.

[5] A. Alimpiev, V. Barannik, S. Podlesny, O. Suprun, A. Bekirov. The video information resources integrity concept by using binomial slots. 2017. XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, Ukraine, 2017, pp. 193-196, DOI: 10.1109/MEMSTECH.2017.7937564.

[6] V. V. Barannik, A. V. Hahanova and V. N. Krivonos. "Coding tangible component of transforms to provide accessibility and integrity of video data," East-West Design & Test Symposium (EWDTS 2013), Rostov on Don, Russia, 2013, pp. 1–5, DOI: 10.1109/EWDTS.2013.6673179.

[7] Songyang Zhang, Yuan Liu, Jiacheng Chen, Zhaohui Yu, Kai Chen, Dahua Lin. Improving Pixel-based MIM by Reducing Wasted Modeling Capability. 2023 IEEE/CVF International Conference on Computer Vision (ICCV). 2023. pp. 5338–5349. DOI: 10.1109/ICCV51070.2023.00494.

[8] Rivest R. L., Shamir A., Adleman L. M. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978. Vol. 21. Iss. 2. P. 120–126. DOI: 10.1145/359340.359342.

[9] V. Barannik and A. Shiryaev, "Quadrature compression of images in polyadic space," Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science, 2012, pp. 422–422. INSPEC Accession Number: 12713484.

[10] Belikova T. Decoding Method of Information-Psychological Destructions in the Phonetic Space of Information Resources. Advanced Trends in Information Theory (ATIT): proceedings of the 2nd IEEE International Conference, 2020. P. 87–91. https://ieeexplore.ieee.org/document/9349300.

[11] Barannik, V. et al. (2023). A Method of Scrambling for the System of Cryptocompression of Codograms Service Components. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transformation Age. TCSET 2022. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. DOI: 10.1007/978-3-031-24963-1_26.

[12] Zhuxian Liu, Yingkai Huang, Qiwen Wu, Xiaolong Liu. Robust image steganography against JPEG compression based on DCT residual modulation. Signal Processing. Vol. 219. 2024. DOI: 10.1016/j.sigpro.2024.109431.

[13] Zhou J., X., Au O. C., Liu Tang Y. Y. Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation. IEEE Transactions on Information Forensics and Security. 2014. Vol. 9, No. 1. P. 39–50. DOI: 10.1109/TIFS.2013.2291625.

[14] A. Krasnorutsky, R. Onyshchenko, D. Barannik and V. Barannik, "The Methods of Intellectual Processing of Video Frames in Coding Systems in Progress Aeromonitor to Increase Efficiency and Semantic Integrity," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 53–56, DOI: 10.1109/ATIT58178.2022.10024208.

[15] Guojun Fan, Zhibin Pan, Quan Zhou, Jing Dong, Xiaoran Zhang. Pixel type classification based reversible data hiding for hyperspectral images. Knowledge-Based Systems. – vol. 254. – 2022. DOI: 10.1016/j.knosys.2022.109606.

[16] V. Barannik, S. Shulgin, N. Barannik and V. Barannik, "Method of Coding Subbands of Non-Homogeneous Spectrum of Video Segments in Uneven Diagonal Space," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 72–75, DOI: 10.1109/ATIT58178.2022. 10024236.

[17] Tong Qiao, Shuai Wang, Xiangyang Luo, Zhiqiang Zhu. Robust steganography resisting JPEG compression by improving selection of cover element. Signal Processing. vol. 183. 2021. DOI: 10.1016/j.sigpro.2021.108048.

[18] Bo Liu, Xiuli Bi, Wuqing Yan, Bin Xiao, Weisheng Li, Xinbo Gao. Self-Supervised Image Local Forgery Detection by JPEG Compression Trace. - The Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI-23). vol. 37 (No. 1). pp. 232–240. DOI: 10.1609/aaai.v37i1.25095.

[19] Shoko Imaizumi, Genki Hamano, Hitoshi Kiya. Effects of JPEG Compression on Vision Transformer Image Classification for Encryption-then-Compression Images. Sensors. vol. 23. pp. 1–19. 2023. DOI: 10.3390/s23073400.

[20] Конахович Г.Ф Оценка эффективности методов стеганографического встраивания информации в спектральную область изображений / Г.Ф. Конахович // АСУ та прилади автоматики. 2014. Вип.168. С. 23–29.

[21] Конахович Г. Ф., Пузиренко А. Ю. Комп'ютерна стеганографія. Теорія та практика [Текст]. Київ: МК-Пресс, 2016. 288 с.

[22] Barannik V. et al. The method of masking overhead compaction in video compression systems, Radioelectronic and Computer Systems, 2(2021), 2021, 51–63. DOI: 10.32620/reks.2021.2.05.

[23] Wong K. W. Image encryption using chaotic maps. Intelligent Computing Based on Chaos. 2009. Vol. 184. P. 333–354. DOI: 10.1007/978-3-540-95972-4_16.

[24] Barannik V., Krasnorutsky A., Kolesnyk V., Barannik V., Pchelnikov S., Zeleny P. Method of compression and ensuring the fidelity of video images in infocommunication networks. Radioelectronic and computer systems, 2022, vol. 4, pp. 129–142. DOI: 10.32620/reks.2022.4.10.

[25] Kiya, H., Aprilpyone, M., Kinoshita, Y., Imaizumi, S., Shiota, S. An Overview of Compressible and Learnable Image Transformation with Secret Key and Its Applications. APSIPA Trans. Signal Inf. Process. 2022, 11, e11. DOI: 10.1561/116.00000048.

[26] Aprilpyone, M.; Kiya, H. Privacy-Preserving Image Classification Using an Isotropic Network. IEEE Multimed. 2022. 29. pp. 23–33. DOI: 10.1109/MMUL.2022.3168441.

[27] Задирака В. К.Статистический анализ систем с цифровыми водяными знаками / В. К. Задирака,

Н. В. Кошкина, Л. Л. Никитенко // Штучный інтелект. 2008. № 3. С. 315–324.

[28] João Ascenso, Elena Alshina, Touradj Ebrahimi. The JPEG AI Standard: Providing Efficient Human and Machine Visual Data Consumption. IEEE MultiMedia. vol 30 (Issue 1). 2023. DOI: 10.1109/MMUL.2023.3245919.

[29] Бараннік Д. В. Технологія приховування інформативного контенту в динамічному потоці відеосегментів // Наукоємні технології. 2023. № 4. С. 408-415. DOI: 10.18372/2310-5461.60.18270.

[30] Barannik V., Lytvinenko M., Okladnoy D., Suprun O. Description of the OFDM symbol with the help of mathematical laws. Analysis of technologies that were used in this case. 2017. 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings, art. no. 8020095, pp. 183-187. DOI: 10.1109/AIACT.2017.8020095.

[31] Nikolay Ponomarenko, Lina Jin, Oleg Ieremeiev, Vladimir Lukin, Karen Egiazarian, Jaakko Astola, Benoit Vozel, Kacem Chehdi, Marco Carli, Federica Battisti, C-C Jay Kuo. Signal processing: Image communication, 2015, no. 30, pp. 57–77.

Баранник В. В., Бараннік Д. В., Бабенко М. В., Прокопенко Р. О.

МЕТОД ЗАХИСТУ ВІДЕОІНФОРМАЦІЇ В СИСТЕМАХ АЕРОКОСМІЧНОГО МОНІТОРИНГУ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

В статті показано, що в процесі забезпечення інформаційної безпеки наявні суперечності. Вони виникають під час забезпечення категорій конфіденційності, цілісності та доступності у разі обробки та передачі відеоінформаційних ресурсів в системі аерокосмічного моніторингу. В їх основі лежить критичність часових затримок на доставку відеоінформації значного бітового об'єму з використанням обмежених за швидкістю передачі інформаційно-комунікаційних засобів. В означених обставинах (умовах) виникає інтерес до технологій захисту інформації в процесі використання систем скорочення бітового об'єму. В статті обґрунтовано, що одним з варіантів реалізації такого підходу є використання стеганографічних методів приховування інформації до контейнерів візуального походження (КВП). Встановлюються базові недоліки методів вбудовування інформації на основі прямих стеганографічних перетвореннях. Напрямком подальшого розвитку може бути побудова комбінованих підходів до організації стеганографічних систем в базисі стиснення. При цьому додатковою складовою пропонується використовувати технології, які за функціональною умовою використовують метод непрямого вбудовування. Водночас для них властивим є низькі значення стеганографічної ємності. Значить, необхідно розробити такий підхід для проектування стеганографічної системи, який враховує не лише психовізуальні закономірності у КВП, а й структурні залежності між елементами його синтаксичного опису. Створено метод безвтратного вбудовувати інформацію непрямим способом з виявленням структурних залежностей шляхом управляючої корекції нерівномірно-вагового позиційного (НРВП) базису за умов: наявності попередньо-вбудованої інформації; усунення цифрових слідів наявності прихованої інформації. Розроблено метод вилучення інформації в стегано-корегованому НРВП-базисі. Відмінності методу стосуються того, що: вилучення інформації здійснюється з виключенням втрат шляхом порівняння реального та контрольного значень основ НРВП-базису в умовах усунення впливу на стегано-підкладку попереднього етапу стегано-перетворень в квантовано-спектральному просторі КВП. Це дозволяє підвищити рівень стеганографічної ємності за умов виключення втрат прихованої інформації та синтаксичного опису ВКП.

Ключові слова: аерокосмічний моніторинг; інформаційно-комунікаційні системи; контейнери візуального походження; надмірність; структурні залежності; позиційний базис.

Barannik V., Barannik D., Babenko M., Prokopenko R., Petrukha N.

METHOD OF PROTECTING VIDEO INFORMATION IN AEROSPACE MONITORING SYSTEMS BASED ON STEGANOGRAPHIC TRANSFORMATIONS

The article shows that there are contradictions in the process of ensuring information security. They arise when ensuring the categories of confidentiality, integrity and availability in the case of processing and transmitting video information resources in the aerospace monitoring system. They are based on the criticality of time delays for the delivery of video information of a significant bit volume using information and communication means limited in transmission speed. In the above circumstances (conditions), interest arises in information protection technologies in the process of using bit volume reduction systems. The article substantiates that one of the options for implementing such an approach is the use of steganographic methods of hiding information in containers of visual origin (CVO). The basic shortcomings of information embedding methods based on direct steganographic transformations are established. The direction of further development may be the construction of combined approaches to the organization of

steganographic systems in the compression basis. In this case, as an additional component, it is proposed to use technologies that, according to the functional condition, use the indirect embedding method. At the same time, they are characterized by low values of steganographic capacity. This means that it is necessary to develop an approach to designing a steganographic system that takes into account not only psychovisual regularities in the CVP, but also structural dependencies between the elements of its syntactic description. A method has been created for lossless embedding of information in an indirect way with the detection of structural dependencies by means of controlled correction of the unevenly weighted positional (NWP) basis under the conditions of: the presence of pre-embedded information; elimination of digital traces of the presence of hidden information. A method has been developed for extracting information in a steganographic-corrected NWP basis. The differences of the method are that: information extraction is carried out with the exclusion of losses by comparing the real and control values of the bases of the NRVP basis under the conditions of eliminating the influence on the stegano-substrate of the previous stage of stegano-transformations in the quantized-spectral space of the KVP. This allows to increase the level of steganographic capacity under the conditions of excluding losses of hidden information and syntactic description of the VKP.

Keywords: aerospace monitoring; information and communication systems; containers of visual origin; redundancy; structural dependencies; positional basis.

Дата першого надходження: 17.02.2026 р.
Дата прийняття до друку: 10.03.2026 р.
Дата публікації: 27.04.2026 р.