DOI: 10.18372/2310-5461.59.17948
УДК 004.622: 517.927

Д. В. Бараннік,
Харківський національний університет радіоелектроніки
orcid.org/0000-0003-4235-300X
e-mail: d.v.barannik@gmail.com;

МЕТОД СТЕГАНОКОМПРЕСІЙНОГО КОДУВАННЯ НА ОСНОВІ ПОЛІАДИЧНОГО БАЗИСУ

Вступ

Особливості функціонування інформаційної інфраструктури, як базової складової систем управління об'єктами та підрозділами сил оборони та безпеки України (СОБУ), стосуються забезпечення інформаційної безпеки. Найбільшої значимості ці питання набирають в умовах воєнного часу. Це зумовлено:

– з одного боку збільшенням вагомості інформації з позиції її впливу на виникнення ризиків щодо нанесення значних втрат: особового складу; економічного та фінансового рівня, мотиваційного стану в суспільстві; політичного іміджу держави [1–3];

– з іншого боку наявність активної протидії з боку супротивника. Це стосується використання інформаційної та вогневої зброї [4; 5].

Отже потрібно забезпечувати потрібний рівень безпеки спеціальних інформаційних ресурсів (ІРС). Висунута проблематика стає більш наочною в умовах використання для інформаційного обміну відкритих бездротових мереж передачі даних [6; 7].

З одного боку такі мережі дозволяють підвищити ефективність функціонування систем управління в умовах: мобільності центрів аналізу інформації та/або об'єктів управління; важко доступності позиційних районів; використання для отримання інформації дистанційних засобів, в тому числі безпілотних літальних комплексів [8–10].

З іншого боку бездротові мережі мають множину вразливих факторів щодо втрати інформаційної безпеки за такими категоріями, як: конфіденційність, цілісність та доступність.

Звідси підвищення безпеки спеціальних інформаційних ресурсів в бездротових інфокомунікаційних системах є актуальним ***науково-прикладним завданням***.

Аналіз сучасних досліджень та постановка завдання

Питання щодо забезпечення доступності та цілісності вирішується з використанням спеціалізованих інфокомунікаційних протоколів, форматів представлення та кодування інформації. До цього напрямку відносяться технології ефективного кодування (стиснення даних), методи завадостійкого кодування [11–13].

Забезпечення конфіденційності досягається в основному за рахунок використання технологій та методів захисту інформації. На інформаційному рівні це забезпечується на основі криптографічних перетворень [14–17].

Водночас існують такі характерні аспекти [18–21]:

- збільшення ефективності методів крипто аналізу;
- підвищення продуктивності обчислювальних засобів;
- дія систем РЕБ, кібератак та вірусних атак;
- обмеженість часу актуальності інформації;
- вимоги щодо обмеженості часових затримок на обробку та передачі інформації;
- відсутність технологічної або нормативної бази для застосуванням методів криптографічного перетворення;
- необхідність організації прихованого каналу передачі інформації.

Звідси наряду з методами криптографічного шифрування необхідно використовувати методи стеганографічних перетворень [21–23]. Це дозволяє в комплексному застосування досягти:

- підвищення конфіденційності інформації;
- побудувати прихований канал передачі інформації. Наприклад, такий канал можна створити в умовах передачі відеоінформаційних потоків.

Постановка проблеми

В якості контейнерів для приховання інформації пропонується задіяти відеоінформаційні ресурси. Це зумовлено наступним [24–26]:

- значне поширення відеоінформаційних ресурсів в процесах підтримки та прийняття рішень для систем критичної та оборонної інфраструктури;
- наявністю аналогової природи відеоданих;
- наявність значної надмірності відеозображень, в тому числі психовізуальної;
- існуванням технологічного апарату для реалізації різних підходів для вбудовування інформації в відеозображення-контейнери (ВЗК).

В той же час для існуючих методів стеганографічних перетворень з використанням ВЗК проявляються певні недоліки [26–28] :

- обмеженість ємності стеганографічного каналу передачі прихованої інформації;
- недостатній рівень стійкості прихованих повідомлень до методів активного та пасивного стеганоаналізу.

Звідси ***мета досліджень*** полягає у розробці методів стегнаографічного кодування інформації з використанням ВЗК для підвищення ємності прихованого каналу передачі інформації.

Обґрунтування напрямку для розробки методів стеганографічного перетворення

Основні ***системні проблеми*** організації стеганографічних перетворень з використанням відеоконтейнерів, які форматуються на основі технологічної концепції JPEG платформи, полягають в наступному [28–30].

1. Обробка відеоконтейнеру організується без врахування можливого стеганографічного вкладення інформації для її приховування.

При цьому в процесі обробки відеоконтейнеру значиме скорочення об’єму досягається з врахуванням психовізуальної надмірності.

2. Стеганографічне вбудовування приховуваної інформації у свою чергу має на увазі використання деякої кількості психовізуальної надмірності. Отже, в результаті стеганографічних перетворень на технологічних етапах трансформаційної надбудови створюються умови для зниження значення коефіцієнта стиснення.

Крім того, у разі перевищення сумарної кількості усуваємої психовізуальної надмірності її критичної межі, можуть відбутися втрати інформації з позиції візуальної оцінки відеоресурсу.

3. У технологічних етапах трансформаційної надбудови передбачений механізм квантування. Він використовується для досягнення: по-перше скорочення психовізуальної надмірності шляхом корекції компонент спектрального представлення сегменту відеокадру під модель візуального сприйняття; по-друге створюються умови для підвищення кількості структурно-статистичної надмірності, яка виявляється. На цьому етапі вносяться втрати цілісності візуального сприйняття і втрати інформації. Тому квантування може призвести до втрати приховуваної інформації, яка була вбудована на попередніх етапах процесу форматування відеоконтейнеру. Відповідно це обмежує ефективність стеганографічного вбудовування інформації на тих технологічних етапах процесу обробки відеоконтейнеру, які передують квантуванню. При цьому скорочується варіативність підходів для стеганографічного вбудовування інформації. Звужується технологічний потенціал для побудови концепцій стеганографічних перетворень. Так або інакше він зводиться до технологічного етапу квантування компонент спектрального або спектрально-часового просторів.

4. У разі організації стеганографічних перетворень в спектральному просторі існує технологічна суперечність, яка полягає в тому, що:

– з одного боку низькочастотні компоненти стійкіші до стеганографічних атак. Інакше відбудеться руйнування візуального і семантичного сприйняття самого відеоконтейнеру. З іншого боку модифікація низькочастотних компонент стає помітним з позиції візуального і семантичного сприйняття стеганоконтейнеру;

– в теж час контрольована модифікації значень високочастотних компонент спектру володіє ефектом маскування артефактів з позиції візуального сприйняття стеганоконтейнеру. Але, з іншого боку підвищується уразливість приховуваної інформації до дії руйнуючих стеганографічних атак і канальних перешкод.

При цьому середні частоти не мають чітких меж в трансформанті, і залежать від динамічно змінного семантико-синтаксичного змісту початкового сегменту відеокадру.

5. Оскільки технологічні етапи вбудовування інформації і скорочення структурно-статистичної надмірності виконуються послідовно, то відбувається зниження ступеня стиснення відеоконтейнерів. Це обумовлено тим, що стеганографічна модифікація трансформант призводить до зміни структурно-статистичних закономірностей. У наслідок чого, відбувається часткове руйнування структурно-статистичних закономірностей, а саме змінюються довжини ланцюжків нульових компонент, змінюється статистична модель розподілу ймовірностей компонент трансформант. Отже це знижує ефективність синтаксичного кодування.

6. Одним з проблемних недоліків кодограм, які побудовано з використанням технологій на JPEG платформі є їх критично низька перешкодостійкість. Це означає те, що без використання перешкодостійкого кодування в умовах наявності канальних перешкод відбудеться втрата приховуваної інформації. Інакше потрібно жертвувати або об’ємом вбудовуваної інформації або збільшувати об’єм кодованих даних за рахунок додаткового використання кодової послідовності, що коректує.

7. Для більшості методів безпосереднє вбудовування інформації здійснюється шляхом модифікації на рівні бітового представлення елементів відеоконтейнеру. В цьому випадку потрібні

додаткові часові витрати на бінаризацію трансформант. Кількість алгоритмічних операцій збільшується в середньому на 30 %. Це може бути критичним для додатків реального часу або у разі вбудовування великого бітового об'єму приховуваної інформації.

8. В результаті стеганографічних модифікацій відеокадру відбувається зниження ступеня їх компресійного представлення. Це пояснюється наступними причинами:

- зниженням кількості психовізуальної надмірності, яка потенційно усувається;
- частковим руйнуванням структурно-статистичних закономірностей трансформованих сегментів відеокадрів;
- необхідністю додаткового використання кодів, що коректують.

Це призводить до зниження доступності інформації та створюються умови для стеганографічного аналізу у разі наявності початкового відеоконтейнеру.

9. Використання статистичних кодів обмежує можливість побудови механізму для динамічного прогнозування стеганографічної інтенсивності.

10. Вилучення прихованої інформації неможливе до тих пір, поки не буде декодований структурно-статистичний код. Це по-перше є причиною втрати часу отримання прихованої інформації, а по-друге в результаті канальних перешкод кодові конструкції декодуються з помилками. Відбуваються втрати прихованої інформації, тобто її вилучення буде неможливим.

11. У разі, коли сегмент відеокадру є інформативним, то відповідно після його трансформації формуються високочастотні компоненти, які матимуть великі значення. Отже в результаті вбудовування навіть у високочастотні компоненти відбудеться прояв візуально помітних артефактів. Це означає те, що підвищується ефективність реалізації візуальної атаки.

Тому необхідно створити таку технологію стеганографічного перетворення, для якої існуватиме можливість вбудовування інформації на рівні елементів відеоконтейнеру з врахуванням нового виду надмірності, який не зв'язується з психовізуальними закономірностями.

Для вдосконалення існуючих і розробки нових методів стеганографічних перетворень необхідно використовувати *принципово нові підходи,* які повинні базуватися на сучасних і перспективних досягненнях в області теорії інформації, кодування, методів обробки цифрових відеоресурсів, технологій інтелектуального аналізу і методів криптографії. Одним з актуальних напрямків є використання структурних перетворень елементів просторового представлення зображення для виявлення структурно-комбінаторної надмірності на основі поліадичного базису.

Розробка методу структурного стеганографічного кодування на основі корекції поліадичного базису

Розглянемо етапи функціонування стеганокомпресійної системи з маскування стеганографічної надмірності. Дана система дозволяє вбудувати біт приховуваного повідомлення на старшу позицію одновимірного поліадичного числа в процесі стеганографічного кодування (СК). Отримана в результаті такого кодування СК-кодограма складається із службової та інформаційної частин. Реалізація вилучення вбудованих даних відбувається за біполярним принципом, а саме: для авторизованого і неавторизованого користувачів.

Стеганокомпресійна система включає наступні базові складові:

1. Стеганокомпресійне кодування з маскуванням структурної стеганографічної надмірності.

2. Структурно-комбінаторне демаскуюче декодування.

Розглянемо процес стеганокомпресійного кодування. Даний етап включає наступні дії:

1. Імплантацію елементу b_ξ на позицію старшого елементу числа $A(j)$. Тут b_ξ - ξ-й елемент вбудовуваної послідовності $B = \{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0;1]$, $\xi = \overline{1,\nu}$. Імплантація задається наступною формулою:

$$A(j)' = A(j) \cup b_\xi, \text{ для } b_\xi = a'_{1,j} \in [0,\ 1]. \quad (1)$$

Внаслідок імплантації, число $A(j)'$ прийме наступний вигляд:

$$A(j)' = \{ a'_{1,\mathrm{j}};...;a_{i,j};...;a_{m+1,j} \}, \quad (2)$$

де $A(j)'$ - число з імплантованим на старшу позицію елементом $a'_{1,j}$.

2. Формування СК-коду $N(j)'$ для числа $\mathrm{A(j)}'$ з імплантованим елементом $a'_{1,j}$. Враховуючи механізм локалізації кількості структурної стеганографічної надмірності

Отже, необхідно розробити підхід для локалізації структурної стеганографічної надмірності, реалізація якого не пов'язана з корекцією стеганокоду.

При цьому обов'язковою умовою є забезпечення відповідності меду довжиною $q(j)'$ кодограми стеганокоду $N(j)'$ і довжиною $q(j)$ коду-контейнера $N(j)$ в разі неавторизованого доступу до стеганографічно перетвореного зображення.

Для цього пропонується організувати локалізацію структурної стеганографічної надмірності на основі побудови модифікованої системи основ $\Psi'^{(1)}$. Під модифікацією системи основ розуміється корекція значень окремих основ.

Обґрунтування даного підходу полягає в тому, що довжина $q(j)$ кодограми як для кода-контейнеру $N(j)$, так і для стеганокоду $N(j)'$ визначається відповідно на основі накопиченого добутку основ, тобто:

$$q(j) = \log_2 \prod_{i=1}^{m} \psi_{i,j} \ ;$$

$$q(j)' = \log_2 \left(\prod_{i=1}^{\gamma-1} \psi_{i,j}) \cdot \psi'_{\gamma,j} \cdot \prod_{i=\gamma+1}^{m+1} \psi_{i,j} \right).$$

Тому за рахунок корекції окремих основ досягається можливість вирівняти довжину $q(j)'$ стеганокоду $N(j)'$ і довжину $q(j)$ коду-контейнера $N(j)$. В цьому випадку виконується співвідношення:

$$q(j)'' = \log_2 ((\prod_{i=1}^{\eta-1} \psi_{i,j}) \cdot \psi''_{\eta,j} \cdot \prod_{i=\eta+1}^{m} \psi_{i,j}) =$$

$$= \log_2 (2 \cdot \prod_{i=1}^{m} \psi_{i,j}) = q(j)',$$

де $\psi''_{\eta,j}$ – модифіковане основу η-го елемента нерівновагового позиційного числа $A(j)$ вихідної відео послідовності.

Оскільки в нерівновагове позиційне число імплантується тільки один елемент приховуваного повідомлення, то досить корекції тільки однієї основи. Хоча в загальному випадку можлива одночасна корекція основ кількох елементів. Корекція основи повинна проводиться з урахуванням того, що основа вбудованого елементу дорівнює двом, $\psi'_{\gamma,j} = 2$. Значить, і довжина $q(j)'$ кодового представлення стеганокоду $N(j)'$ буде більше довжини $q(j)$ кодограми коду-контейнера на один біт. Тому для корекції досить змінити основу одного елемента. Корекцію осно-ви пропонується проводити на базі наступної умови:

$$q(j)'' = q(j)'$$

або

$$q(j)'' = \log_2 \left(\prod_{i=1}^{\eta-1} \psi_{i,j}) \cdot \psi''_{\eta,j} \cdot \prod_{i=\eta+1}^{m} \psi_{i,j} = \right.$$

$$\left. = \log_2 (2 \cdot \prod_{i=1}^{m} \psi_{i,j} \right) = q(j)'.$$

Для скорочення кількості операцій пропонується використовуватися правило, яке задано формулою:

$$\psi''_{\eta,j} = 2 \cdot \psi_{\eta,j},$$

де $\psi_{\eta,j}$ – основа η-го елемента нерівновагового позиційного числа $A(j)$ вихідної відео послідовності.

Розглянемо варіанти вибору позиції елемента нерівновагового позиційного числа, для якого будемо проводити коригування основи. На вибір такої позиції впливає те, що необхідно забезпечити наступні вимоги:

1) забезпечити умову без помилкового вилучення вбудованої інформації;

2) забезпечити мінімізацію спотворень зображення, реконструйованого як для авторизованого, так і для неавторизованого користувача.

Для реалізації першої умови сформулюємо наступне.

Твердження. (Умова безпогрешного вилучення вбудованої інформації). Для реалізації першого напрямку корекційна основу $\psi''_{\eta,j}$ має відповідати елементу НП числа, що займає більш старшу позицію η в порівнянні з позицією γ вбудованого елемента $a'_{\gamma,j}$, Тобто

$$a'_{\gamma,j} = a''_{\gamma,j}, \text{ коли } \psi''_{\eta,j} | \eta > \gamma. \qquad (3)$$

Розглянемо другу вимогу, коли вибір позиції вбудовування елемента $a'_{\gamma,j}$ повинен забезпечити мінімізацію внесених спотворень при реконструкції елементів $a'''_{i,j}$ вихідної відеопослідовності. Як показник мінімізації спотворень пропонується використовувати умова, що складається в мінімізації різниці між значенням коду-контейнера $N(j)$ і стеганокодом $N(j)'$. Для цього використовується наступне співвідношення:

$$\Delta N(j) = N(j)' - N(j),$$

де $\Delta N(j)$ – значення пульсації стеганокода.

При цьому враховується те, що значення вбудованого елемента приймає значення $a'_{\gamma,j} = [0; 1]$, а його основу $\psi'_{\gamma,j}$ вибрано мінімально можливим і одно $\psi'_{\gamma,j} = 2$, отриманий вираз прийме наступний вигляд:

$$\Delta N(j) = \begin{cases} F(a_{i,j}; V_{i,j})_{\gamma-1}, & \to a'_{\gamma,j} = 0; \\ F(a_{i,j}; V_{i,j}; V'_{\gamma,j})_{\gamma-1}, & \to a'_{\gamma,j} = 1. \end{cases}$$

Тут $F(a_{i,j}; V_{i,j})_{\gamma-1}$ - функціонал визначення кодових перетворень в поліадичні системі.

Тоді величина $\Delta N(j)$ буде прагнути до нульового значення в разі, коли позиція вбудованого елемента γ буде приймати мінімальні значення, тобто:

$$\gamma \to \min.$$

Значить, можна зробити висновок, що для запропонованого механізму локалізації структурної стеганографічної надмірності коректовані основа повинна відповідати елементу нерівновагового позиційного числа на більш старшої позиції в порівнянні з позицією вбудованого елемента.

В той же час для забезпечення стійкості вбудованої інформації до стегоатакам необхідно щоб значення вагового коефіцієнта вбудованого елемента було найбільшим. З огляду на цей факт пропонується будувати правило маскування стеганографічної надмірності на основі наступних принципів:

1) вбудовувати елемент $a'_{\gamma,j}$ приховуваного повідомлення на другу позицію $\gamma = 2$ в нерівноваговому позиційному числі;

2) піддавати корекції основі першого елемента НП числа.

Оцінка стеганографічного бітрейту для розробленої стеганокомпресійної системи

Для розробленої системи безпосереднього вбудовування оцінимо величину стеганографічного бітрейту стеганокомпресійної (СК) системи, який визначається на основі наступного виразу:

$$S_b = \lim_{\substack{P_{\text{вил}} \to 1 \\ h \to \infty}} (f(w_{\text{вбд}}, Z_{\text{ряд}} Z_{\text{стб}}, P_{\text{вил}}, h)),$$

де $f(\bullet)$ - функціональне перетворення, яке використовується для визначення стеганографічного бітрейту СК-системи; $w_{\text{вбд}}$ - величина абсолютної стеганографічної ємкості СК-системи, тобто максимальний об'єм повідомлення, яке можна вбудувати в зображення, вимірюється в бітах; $Z_{\text{ряд}} Z_{\text{стб}}$ - мінімально необхідний розмір зображення, достатній для вбудовування інформації об'ємом $w_{\text{вбд}}$ на основі оцінюваної стеганокомпресійної технології; $P_{\text{вил}}$ - ймовірність безпомилкового вилучення вбудованих даних; h - величина пікового відношення сигнал/шум.

Фізичний зміст стеганографічного бітрейту S_b полягає в тому, що дана величина характеризує кількість пікселів, яка необхідна для вбудовування одного біту приховуваного повідомлення. Стеганографічний бітрейт вимірюється в бітах на піксель (біт/піксель).

На практиці використовується наступний вираз для визначення стеганографічного бітрейту:

$$S_b = \frac{w_{\text{вбд}}}{Z_{\text{ряд}} Z_{\text{стб}}}, \qquad (4)$$

де $w_{\text{вбд}}$ - величина абсолютної стеганографічної ємкості, тобто максимальний об'єм повідомлення, який можна вбудувати в зображення, вимірюється в бітах.

На рис. 1 представлена діаграма залежності величини $S_b^{(m)}$ стеганографічного бітрейта розробленої СК-системи від різної довжини $m = 2; 3; 4; 6$ сформованих одновимірних поліадичних чисел.

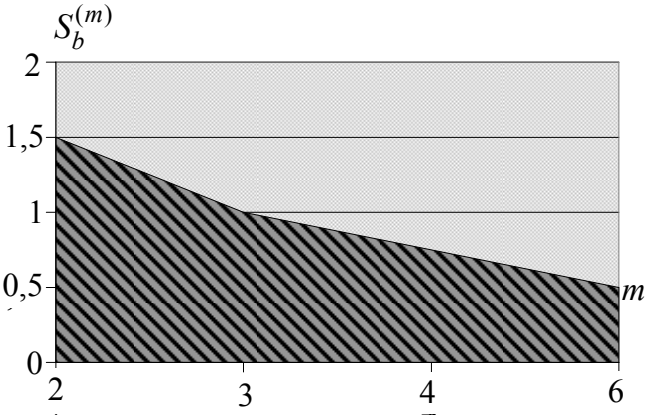

Рис. 1. Залежність величини $S_b^{(m)}$ стеганографічного бітрейту розробленого СК-методу від m

З аналізу діаграми на рис. 1 можна зробити висновок, який полягає в тому, що в разі формування одновимірного поліадичного числа довжиною $m = 2$, величина $S_b^{(m)}$ пропускної спроможності розробленої СК-системи набуває найбільшого значення, рівного 1,5 біт на піксель. Навпаки, при формуванні ОПЧ довжиною $m = 6$ стеганокомпресійна система володіє найменшою пропускною спроможністю – 0,5 біт на піксель.

Тепер проведемо порівняльну оцінку величини стеганографічного бітрейту $S_b^{(m)}$ для розробленої СК-системи та існуючих методів безпосереднього вбудовування в зображення-контейнер. Порівняльну оцінку проводитимемо для наступних методів:

1. Метод вбудовування інформації в найменш значимий біт (НЗБ) компонент спектрального представлення контейнеру після квантування.

2. Метод вбудовування інформації на основі розширення спектру (РС).

На рис. 2 представлені діаграми залежності значення величини S_b та величини h пікового відношення сигнал/шум середньо насичених зображень для методів найменш значимого біта, розширення спектру і розробленого методу.

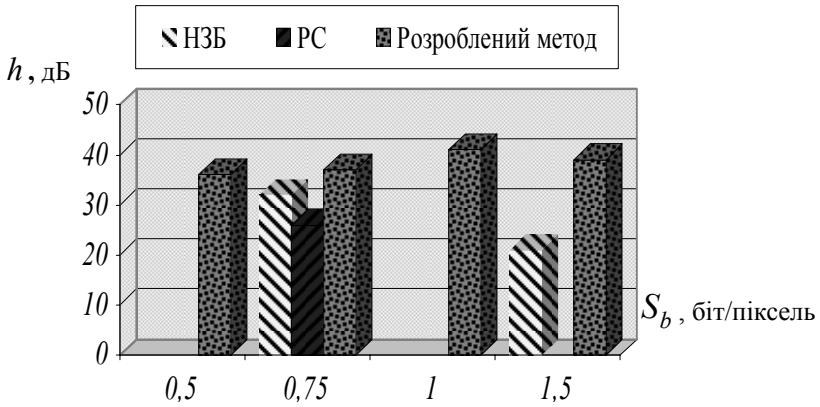

Рис. 2. Діаграма значень величини S_b і h для середньонасиченого зображення, яке декодоване на основі методу НЗБ, РС і розробленого СК-методу

З аналізу діаграм на рис. 2 можна зробити наступні висновки:

1) для розробленого стеганокомпресійного методу найбільше значення стеганографічного бітрейту досягається у разі формування одновимірних поліадичних чисел довжиною $m = 2$ - 1,5 біта на піксель, і навпаки найменше значення величини S_b спостерігається для одновимірних поліадичних чисел довжиною $m = 6$ - 0,5 біта на піксель;

2) виграш для розробленого СК-методу відносно методів НЗБ та РС по величині стеганографічного бітрейту досягає в середньому до 25 %.

Висновки

1. Розроблено структурно-комбінаторне стеганокомпресійне кодування з маскуванням, що базується на наступних етапах:

- формування поліадичного базису для фрагменту відеозображення;
- структурне стеганокомпресійне кодування в поліадичному базисі основ;
- маскування структурної стеганографічної надмірності шляхом її локалізації на основі корекції довжини стеганограми.

Друга базова концептуальна відмінність створеної стеганокомпресійної системи. Вперше розроблено структурно-комбінаторне стеганокомпресійне кодування з маскуванням. На відміну від інших методів забезпечується вбудовування приховуваної інформації в процесі ОПК з подальшою локалізацією стеганографічної надмірності. Це дозволяє знизити можливість виявлення протиборчою стороною факту наявності вбудованої інформації (локалізувати атаку виявлення факту наявності вбудованої інформації).

2. ***Створено правило*** вбудовування інформації для структурно-комбінаторного стеганокомпресійного кодування, яке полягає в тому, що:

1) один біт приховуваного повідомлення вбудовується на старшу позицію одновимірного поліадичного числа в двовимірному базисі;

2) локалізація стеганографічної надмірності досягається на основі відкидання молодшого біта стеганограми.

ЛІТЕРАТУРА

[1] Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. К.: НАУ, 2013. 432 с.

[2] ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Чинний від 01.03.2016. Вид. офіц. Київ, Держспоживстандарт України, 2016. 228 с.

[3] Valeri Barannik, "Technology of Structural-Binomial Coding to Increase the Efficiency of the Functioning of Computer Systems," *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2022, pp. 96–100, doi: 10.1109/ATIT58178.2022.10024205.

[4] Конахович Г. Ф., Пузиренко А. Ю. Компьютерна стеганографія. Теорія та практика [Текст]/ Київ: МК-Пресс, 2016. 288 с.

[5] Одарченко Р., Іванова М., Рябенко М., Аль-Мудхафар Акіл Абдулхусейн М. Метод аналізу взаємодії параметрів qoe та qos на основі алгоритмів керування машинами. *Наукоємні*

технології. 2022. № 4 (56). С. 305–316. DOI: https://doi.org/ 10.18372/2310-5461.56.17130.

[6] Баранник В., Сидченко С., Баранник Д., Баранник В. Оцінка впливу недетермінованих характеристик на ефективність криптокомпресійного кодування забражень в диференціованому базисі. *Безпека інформації*. 2020. Том 26. № 3. С. 168–180.

[7] ДСТУ ГОСТ 28147:2009. Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89). Чинний від 01.02.2009. Вид. офіц. Київ, Держспоживстандарт України, 2009. 20 с.

[8] Chen T.-H., Wu Ch.-S. Efficient multi-secret image sharing based on Boolean operation. Signal Processing. 2011. Vol. 91, Iss. 1. P. 90–97. DOI: 10.1016/j.sigpro.2010.06.012.

[9] Козловський В., Савченко А., Толстікова О., Клобукова Л. Критерії вибору спектрально-ефективних сигналів у бездротових інформаційних мережах. *Наукоємні технології*. 2022. № 4 (56). С. 286–273. DOI: https://doi.org/ 10.18372/2310-5461.56.17125.

[10] Krasnorutsky A., Onyshchenko R., Barannik D. and Barannik V. "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.

[11] Баранник В. В., Сидченко С. А., Баранник Д. В. Метод криптокомпресійного представлення зображень на основі двохкаскадного узагальненого позиціного кодування в базисі по верхніх границях. *Радіоелектроніка та інформатика*. 2017. № 1(76). С. 22–27.

[12] Barannik V., Sidchenko S., Barannik D. Technology for protecting video information resources in the info-communication space. *Advanced Trends in Information Theory (ATIT 2020)*: proceedings of IEEE 2nd Intern. Conf. Kyiv, 2020. P. 29–33.

[13] Tsai Ch.-L., Chen Ch.-J., Hsu W.-L. Multi-morphological image data hiding based on the application of Rubik's cubic algorithm. Carnahan Conference on Security Technology (ICCST): proceedings of the IEEE International Conference. 2012. P. 135–139. DOI: 10.1109/CCST.2012.6393548.

[14] T. Belikova and S. Sidchenko, "The Method Drawing up the Text with the Set Suggestive Orientation to Create a Hidden Channel," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 106–110, doi: 10.1109/ ATIT58178.2022.10024206.

[15] Barannik V., Sidchenko S., Barannik D., Shulgin S., Barannik V., Datsun A. Devising a conceptual method for generating cryptocompression codograms of images without loss of information quality. *Eastern-European Journal of Enterprise Technologies*. 2021. Vol. 4. No. 2(112). P. 6–17.

[16] Barannik D., Barannik V., Korotin S., Bekirov A., Veselska O., Wieclaw L. Method of safety of informational resourses on the basis of use of the indirect steganography The Technology of Structural Classification of Video Frames in Intelligent Info-Communication Systems. Proceeding of the VIII International Conference of Students, PhD Students and Young Scientists, *Springer* Nature Switzerland AG2020, editors S. Zawislak, Volume 70, ISSN 2211-0984. "*Development of technology analys for the content semantics,"* in Engineer of XXI Century – We Design the Future, Bielsko-Biała, Poland: ATH, 2020. P. 195-202. doi.org/10.1007/978-3-030-13321-4_17.

[17] Barannik D. and Barannik V. "Steganographic Coding Technology for Hiding Information in Infocommunication Systems of Critical Infrastructure", 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 88–91, doi: 10.1109/ATIT58178.2022.10024185.

[18] Конахович Г. Ф., Шевченко О. В., Кінзеревий В. М., Хохлачова Ю. Е. Сучасні методи квантової стеганографії. *Захист інформації*. 2011. № 2 (51). С. 5–9.

[19] Конахович Г. Ф. Оцінка ефективності методів стегонографічного вбудовування інформації в спектральну область зображень. *АСУ та прилади автоматики*. 2014. Вип. 168. С. 23-29.

[20] Information technology – JPEG 2000 image coding system: Secure JPEG 2000 [Text]. International Standard ISO/IEC 15444-8, ITU-T Recommendation T.807, 2007. 108 p.

[21] Minemura K., Moayed Z., Wong K., Qi X., Tanaka K. JPEG image scrambling without expansion in bitstream size. Image Processing: proceedings of the 19th IEEE International Conference, 2012. P. 261–264. https://doi.org/ 10.1109/ICIP.2012.6466845.

[22] 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, Switzerland, Cham. https://doi.org/ 10.1007/978-3-031-24963-1_26.

[23] Dmitry Barannik, Mikolaj Karpiinski, Natalia Barannik, Eliseev Evgeniy, Olga Veselska, Aigul Shaikhanova, Balzhan Smailova

Technology Of Improving Data Transfer With The Use Of The Steganographic Approach In Automated Specialized Control Systems. System IEEE IDAACS-SWS 2020. 5th IEEE International Symposium on Smart and Wireless «Systems within the International Conferences On Intelligent Data Acquisition And Advanced Computing Systems» 17-18 September, 2020, Dortmund University of Applied Sciences and Arts, Dortmund, Germany.

[24] Бараннік В. В., Бараннік Д. В., Бекиров А. Е. Основи теорії структорно-комбінаторного стеганографічного кодування: монография. Х.: «Лідер», 2017. 256 с.

[25] Barannik, V. and Barannik, N. and Barannik, D.: Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System. In.: 15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020), pp. 699–702 (2020) DOI: 10.1109/TCSET49122.2020.235522.

[26] Barannik D. V., Barannik V. V., Shulgin S. S., Ryabukha U. N., Tverdokhlib V. V. Video segment coding method for bit rate control information technology. *Science-Based Technologies*. 2020. № 3, pp. 49–52.

[27] Бараннік Д. В. Концепція структурного стеганографічного кодування з маскуванням. *АСУ та прилади автоматики*. 2014. Вип. 168. С. 4-11.

[28] Бараннік Д. В. Баранник В. В., Бекиров А. Е. Стеганографічна система на основі нерівноважного позиційного кодування. *Радіоелектроніка та інформатика*. 2014. № 4. С. 37–46.

[29] Бараннік В. В., Баранник Д. В. Аналіз можливості використання маскування при виявленні областей для стеганографічного вбудовування. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: коллективная монография [под редакцией В. В. Баранника, В. М. Безрука]. Х.: ТОВ «Видвництво « Лідер»», 2017. С. 375–389.

[30] Barannik, D. Stegano-Compression Coding in a Non-Equalible Positional Base // *IEEE 2 nd International Conference on Advanced Trends in Information Theory (ATIT 2020)*, 2020, pp. 83–86.

Бараннік Д. В.

МЕТОД СТЕГАНОКОМПРЕСІЙНОГО КОДУВАННЯ НА ОСНОВІ ПОЛІАДИЧНОГО БАЗИСУ

В статті розкриваються особливості функціонування інформаційної інфраструктури, як базової складової систем управління об'єктами та підрозділами сил оборони та безпеки України, стосуються забезпечення інформаційної безпеки. Найбільшої значимості ці питання набирають в умовах воєнного часу. Отже потрібно забезпечувати потрібний рівень безпеки спеціальних інформаційних ресурсів. Висунута проблематика стає більш наочною в умовах використання для інформаційного обміну відкритих бездротових мереж передачі даних. Звідси підвищення безпеки спеціальних інформаційних ресурсів в бездротових інфокомунікаційних системах є актуальним науково-прикладним завданням. Забезпечення конфіденційності досягається в основному за рахунок використання технологій та методів захисту інформації. Обґрунтовано те, що наряду з методами криптографічного шифрування необхідно використовувати методи стеганографічних перетворень. В той же час для існуючих методів стеганографічних перетворень з використанням відеозображення контейнера (ВЗК) проявляються певні недоліки : обмеженість ємності стеганографічного каналу передачі прихованої інформації; недостатній рівень стійкості прихованих повідомлень до методів активного та пасивного стеганоаналізу. Звідси мета досліджень полягає у розробці методів стегнаографічного кодування інформації з використанням ВЗК для підвищення ємності прихованого каналу передачі інформації. Розроблено структурно-комбінаторне стеганокомпресійне кодування з маскуванням, що базується на наступних етапах: формування поліадичного базису для фрагменту відеозображення; структурне стеганокомпресійне кодування в поліадичному базисі основ; маскування структурної стеганографічної надмірності шляхом її локалізації на основі корекції довжини стеганограми. Створено правило вбудовування інформації для структурно-комбінаторного стеганокомпресійного кодування, яке полягає в тому, що: один біт приховуваного повідомлення вбудовується на старшу позицію одновимірного поліадичного числа в двовимірному базисі; локалізація стеганографічної надмірності досягається на основі відкидання молодшого біта стеганограми.

Ключові слова: інформаційна безпека, стеганографічне кодування, відеозображення, структурна надмірність, бітрейд.

Barannik D.

STEGANOCOMPRESSION CODING METHOD BASED ON POLYADIC BASIS

The article reveals the features of the functioning of the information infrastructure, as a basic component of the management systems of objects and units of the defence and security forces of Ukraine, related to the provision of information security. These issues are gaining the greatest significance in wartime. Therefore, it is necessary to ensure the required level of security of special information resources. The problems put forward become more evident in the context of the use of open wireless data transmission networks for information exchange. Hence, improving the security of special information resources in wireless infocommunication systems is an urgent scientific and applied task. Ensuring confidentiality is achieved mainly through the use of technologies and methods of information protection. At the same time, the existing methods of steganographic transformations with the use of video image of the container (VIC) have certain disadvantages: limited capacity of the steganographic channel for transmitting hidden information; insufficient level of resistance of hidden messages to the methods of active and passive steganoanalysis. Hence, the purpose of the research is to develop methods for hippographic information encoding using VIC to increase the capacity of the latent information transmission channel. Structural-combinatorial steganocompression coding with masking has been developed, which is based on the following stages: formation of a polyadic basis for a fragment of a video image; structural steganocompression coding in the polyadic basis of bases; masking structural steganographic redundancy by localizing it based on steganogram length correction. A rule for embedding information for structural-combinatorial steganocompression coding has been created, which consists in the following: one bit of the concealed message is embedded in the highest position of a one-dimensional polyadic number in a two-dimensional basis; Localization of steganographic redundancy is achieved by rejecting the low bit of the steganogram.

Keywords: information security, steganographic encoding, video imaging, structural redundancy, bittrade.

Стаття надійшла до редакції 15.08.2023 р.
Прийнято до друку 11.10.2023 р.