DOI: 10.18372/2310-5461.61.18512
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 ДЕКОДУВАННЯ ІНФОРМАЦІЇ ДЛЯ БЕЗДРОТОВИХ ІНФОКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Вступ

Потреба у захисті бортових відеоінформаційних ресурсів наряду із забезпеченням заданих характеристик інформаційного забезпечення за своєчасністю та цілісністю доставки в системах управління критичною інфраструктурою (КІ) в умовах протиборства зумовлена наступними аспектами [1]:

1) можливістю протиборчої сторони щодо [2]:

- здійснення атак направлених на: знищення бортового комплексу (БК); перехват управління;

- застосування РЕБ;

2) обмеженістю продуктивності бортових інфокомунікаційних систем, що впливає на потенціал відносно використання потужних технологій обробки та захисту інформації [3];

3) нормативно-законодавчі обмеження відносно можливості використання за певних умов технологій гарантованого криптографічного захисту [4];

4) реалізацією технологій обробки інформації на закордонній мікроелементній базі [5];

5) технологічною потребою у збільшенні ефективності комплексних систем захисту інформації (КСЗІ) для БК [6];

6) наявністю можливості використовувати вразливі фактори в системах забезпечення інформаційної безпеки, в тому числі техногенного та антропогенного походження;

7) факторами демаскування спеціальної інформації.

Такі питання можуть вирішуватись різними підходами [7]. Одним з них є сумісне використання для захисту інформації технологій криптографічного та стеганографічного перетворень [8; 9]. Відносно використання стеганографічних систем в КСЗІ є такі сприятливі фактори [10, 11]:

- можливість приховати факт наявності спеціальної інформації у контейнері;

- незначна складність щодо процесу вбудовування інформації;

- можливість використовувати бортові відеоінформаційні ресурси в якості контейнерів для прихованого вбудовування інформації.

В загальному випадку растрові відеоінформаційні ресурси, які можна використовувати в якості контейнерів, представляються потоком відеосегментів (ПВС), що формується наступним відео-контентом [12, 13]:

1) стаціонарні відеозображення або динамічні відеодані (відеопотік) подвійного призначення;

2) панорамні аерофотознімки спеціалізованого призначення;

3) візуалізація інформації, що формується в інших спектральних діапазонах (інфрачервоному, тепловому, радіо спектральному).

В процесі інформаційного забезпечення в КІ на основі використання БК інформацією, що потребує захисту, може бути [14, 15]:

1) динамічні послідовності відеокадрів або панорамних аерофотознімків;

2) окремі фрагменти бортових ресурсів (аерофотознімків), які встановлюються як найбільш значимі за рівнем інформативності структурно-семантичного змісту відеосегменти;

3) мета-інформація, що формується в результаті дешифрування (цілеспрямованої експертної обробки, аналізу та розпізнавання аерофото інформації) аерофотознімків.

В свою чергу, це зумовлює вимоги до стеганографічних технологій (СТТ) захисту інформації з використанням бортових відео-контейнерів (БВК). В першу чергу це стосується збільшення стеганографічної ємності за умов цілісного вилучення прихованої інформації на приймальній стороні [16 – 18].

Однак потенціал існуючих інфокомунікаційних технологій кодування та передачі відеоданих з використанням бездротових інфокомунікаційних технологій є недостатнім щодо створення умов для забезпечення потрібних характеристик СТТ [19–21]. Звідси підвищення ефективності стеганографічних технологій для бортових інфо-

комунікаційних систем за умов наявності протиборства є ***актуальною науково-прикладною задачею***.

Аналіз останніх досліджень та публікацій

На даний час існує певна множина різних технологічних реалізації стеганографічних перетворень. Існуючі методи цифрової стеганографії для відеозображень також можна класифікувати за логікою вбудовування [22–24]. Найчастіше вбудовування інформації проводиться по-бітно. У непрямих методах вбудовування одного біта повідомлення здійснюється шляхом виявлення або створення залежності між певними параметрами зображення-контейнера [25; 26]. При цьому стеганографічний декодер відповідно до зворотного стеганографічного перетворення встановлює відповідність: між значеннями біт «0» або «1»; виявленою залежністю або за змішаною схемою.

Деякі стеганографічні методи можна класифікувати як підходи на основі змішаного вбудовування. В цьому випадку пряме стеганографічне перетворення здійснюється з врахуванням вбудованого елементу [27]. Навпаки, вилучення вбудованої інформації здійснюється на основі непрямого підходу шляхом порівняння і виявлення залежності [28]. Для методів безпосереднього вбудовування послідовності секретного повідомлення здійснюється шляхом заміни даних контейнера на значення біт приховуваного повідомлення [29; 30].

Водночас існуючі методи побудови СТТ мають недостатні характеристики щодо збільшення стеганографічної ємності в умовах компресійного кодування відео-контейнерів [30; 31].

Постановка проблеми

Один з напрямків підвищення ефективності СТТ є застосування методі стеганокомпресійного кодування. Такі методи викладено в наступних наукових працях [32, 33]. В даному випадку вбудовування інформації здійснюється безпосередньо в процесі компресійного кодування БВК. Забезпечується збільшення рівня стеганографічної ємності. Водночас для забезпечення в умови щодо потрібного рівня цілісності прихованої інформації під час її санкціонованого вилучення на приймальній стороні необхідно розробити метод стеганокомпресійного декодування. Звідси ***мета досліджень статті*** полягає у створення методу стеганокомпресійного декодування прихованої у БВК інформації.

Розробка методу зворотних стеганодекомпресійних перетворень

Стеганокомпресійне представлення з маскуванням базового поліадичного базису під форматований стегано-ПБ дозволяє здійснювати відновлення в умовах дотримання політики інформаційної безпеки. В цьому разі для створеного СК-представлення передбачається можливість відновлення інформації в двох режимах: перший режим – маскований. Він автоматично реалізується для несанкціонованого доступу; другий режим – демаскований, який підтримується для санкціонованого доступу до відеоресурсів та/або прихованої інформації. Відповідно до чого *пропонується* розробляти метод СК-декодування на основі каскадної технологічної концепції

Перший каскад реалізує декодування послідовності відеосегментів в маскованому режимі. На даному шарі реконструкції доступними для використання є: маскований базовий ПБ базис $Q''(\alpha)^{(2,k,\ell)}$; двійковий зміст $\left[\tilde{C}'(\alpha)_j^{(k,\ell)}\right]_2$ синтаксичного опису СК-кодограми $\tilde{C}'(\alpha)_j^{(k,\ell)}$. Це дозволяє реконструювати відеоресурси для несанкціонованого доступу в умовах приховування факту наявності вбудованих повідомлень. Отже потрібно на основі використання МБПБ та стегано-кодового значення забезпечити відновлення такої складової $A''(\alpha)_j^{(k,\ell)}$, яка буде відповідати складовій $A(\alpha)_j^{(k,\ell)}$ початкового ВС за умов відсутності вбудовування інформації, тобто $A''(\alpha)_j^{(k,\ell)} \to A(\alpha)_j^{(k,\ell)}$. Такий процес має наступну математичну трактовку:

$$A''(\alpha)_j^{(k,\ell)} = f_{unac}(\tilde{v}(\alpha)_j^{(k,\ell)};$$
$$\tilde{N}'(\alpha)_j^{(k,\ell)}; Q''(\alpha)^{(2,k,\ell)}),$$
$$\mathrm{i}=\overline{1,\ \mathrm{n}},\ \alpha=\overline{1,\ \mathrm{n}_\alpha},\ \mathrm{j}=\overline{1,\ \mathrm{n}},$$
$$\begin{cases} Q''(\alpha)^{(2,k,\ell)} = \{q''(\alpha)_{i,j}^{(k,\ell)}\}_{\alpha=\overline{1,\ n_\alpha}}; \\ A''(\alpha)_j^{(k,\ell)} = \{a''(\alpha)_{i,j}^{(k,\ell)}\}_{\alpha=\overline{1,\ n_\alpha}}; \\ a''(\alpha)_{i,j}^{(k,\ell)} \le q''(\alpha)_{i,j}^{(k,\ell)},\ \alpha=\overline{1,\ n_\alpha}, \end{cases}$$

де $A''(\alpha)_j^{(k,\ell)}$ - α-я складова j-го стовпця $(k;\ell)$-го ВС, яка реконструюється в режимі несанкціонованого доступу; $a''(\alpha)_{i,j}^{(k,\ell)}$ – $(i;\ j)$-й елемент для складової $A''(\alpha)_j^{(k,\ell)}$; $Q''(\alpha)^{(2,k,\ell)}$ - маскована α – складова базового поліадичного базису; $q''(\alpha)_{i,j}^{(k,\ell)}$ – $(i;\ j)$-а компонента базису $Q''(\alpha)^{(2,k,\ell)}$; $f_{unac}\left(\tilde{v}(\alpha)_j^{(k,\ell)};\ \tilde{N}'(\alpha)_j^{(k,\ell)}; Q''(\alpha)^{(2,k,\ell)}\right)$ – загальний функціонал відновлення складових ВС для несанкціонованого доступу (unauthorized access).

Для першого каскаду передбачається виконання наступних технологічних функцій:

1. Вилучення стегано-кодового значення $\tilde{N}'(\alpha)_j^{(k,\ell)}$ для позиціонованої за довжиною $v''(\alpha)_j^{(k,\ell)}$ СК-кодограми $\tilde{C}'(\alpha)_j^{(k,\ell)}$. Даний функціонал реалізується двома операційними етапами:

1) встановлення позицій та довжини $v''(\alpha)_j^{(k,\ell)}$ СК-кодограми $\tilde{C}'(\alpha)_j^{(k,\ell)}$ з використанням компонент $q''(\alpha)_{i,j}^{(k,\ell)}$ МБПБ базису $Q''(\alpha)^{(2,k,\ell)}$. Тут потрібно враховувати те, що базис $Q''(\alpha)^{(2,k,\ell)}$ будується таким чином, що б забезпечити умову $v''(\alpha)_j^{(k,\ell)} = \tilde{v}(\alpha)_j^{(k,\ell)}$. Завдяки чому, на приймальній стороні досягається встановлення позицій СК-кодограми $\tilde{C}'(\alpha)_j^{(k,\ell)}$ без втрат її синтаксичної цілісності. Відповідно даний етап дозволяє позиціонувати (встановити) двійковий зміст

$$\left[\tilde{C}'(\alpha)_j^{(k,\ell)}\right]_2,$$

$$\left[\tilde{C}'(\alpha)_j^{(k,\ell)}\right]_2 = \left\{\tilde{c}'(\alpha;j)_1^{(k,\ell)};...;\right.$$

$$\left.\tilde{c}'(\alpha;j)_\psi^{(k,\ell)};....;\tilde{c}'(\alpha;j)_\Psi^{(k,\ell)}\right\}.$$

поточної α-ї СК-кодограми $\tilde{C}'(\alpha)_j^{(k,\ell)}$ в загальному бітовому потоці послідовності компактно-представлених ВС;

2) вилучення стегано-кодового значення $\tilde{N}'(\alpha)_j^{(k,\ell)}$ з двійкової кодограми довжиною $\Psi = |\tilde{C}'(\alpha)_j^{(k,\ell)}| = \tilde{v}(\alpha)_j^{(k,\ell)}$ біт здійснюється на основі блокового двійкового кодування.

Відновлення величини $\tilde{N}'(\alpha)_j^{(k,\ell)}$ проводиться без втрат синтаксичної цілісності, що ґрунтується на умові маскування базового ПБ під форматований РСПБ базис.

2. Позиційне декодування величини $\tilde{N}'(\alpha)_j^{(k,\ell)}$ в МБПБ базисі $Q''(\alpha)^{(2,k,\ell)}$. Процес декодування стегано-кодового значення в МБПБ базисі здійснюється за умов врахування властивостей позиційних кодових систем в поліадичному базисі та особливостей форматування РСПБ базису з послідуючим маскуванням під нього базового, а саме:

- значення маскованого ПОБ $q''(\alpha)_{1,j}^{(k,\ell)}$ відповідає елементу ППЧ на першій старшій позиції, та як слідство не впливає на відновлення елементів складової $A''(\alpha)_j^{(k,\ell)}$ ВС;

- елемент повідомлення, що приховується, додається на другу позицію стегано-ППЧ. Звідси його ПОБ не впливає на визначення позиційно-комбінаторної ваги $w(\alpha)_{i,j}^{(k,\ell)}$ молодших елементів ППЧ.

Тому за результатами виконання двох технологічних функцій маємо відновлене ППЧ $A''(\alpha)_j^{(k,\ell)}$:

$$A''(\alpha)_j^{(k,\ell)} = \left\{a(\alpha)_{1,j}^{(k,\ell)} \pm \varepsilon(\alpha)_{1,j}^{(k,\ell)};\ a(\alpha)_{2,j}^{(k,\ell)};..;\right.$$

$$\left.a(\alpha)_{i,j}^{(k,\ell)};...;\ a(\alpha)_{n_\alpha,j}^{(k,\ell)}\right\},$$

яке відповідає α-ї складової j-го стовпця $(k;\ell)$-го ВС.

При цьому досягається відновлення складових ВС без втрат потрібного рівня семантичної або синтаксичної цілісності. Це створює умови для забезпечення приховування факту наявності у ВС вбудованої інформації у разі несанкціонованого доступу.

Другий каскад реалізує технологічні СК-перетворення для демаскованого режиму. При цьому демаскований режим використовує відомості, що попередньо отримано для першого каскаду загального процесу обробки, а саме:

- вилучене з СК-кодограми $\tilde{C}'(\alpha)_j^{(k,\ell)}$ стегано-кодове значення $\tilde{N}'(\alpha)_j^{(k,\ell)}$;

- компоненти $q''(\alpha)_{i,j}^{(k,\ell)}$ МБПБ $Q''(\alpha)^{(2,k,\ell)}$ базису.

Це дозволяє побудувати ***три*** базові технологічні функції другого шару загального процесу зворотних СК-перетворень.

Перша технологічна функція f_{unmask} - демаскування (*unmasking*) форматованого РСПБ базису за компонентами МБПБ $Q''(\alpha)^{(2,k,\ell)}$ базису:

$$\tilde{q}'(\alpha)_{i,j}^{(k,\ell)} = f_{unmask}\left(q''(\alpha)_{i,j}^{(k,\ell)}\right).$$

Тут враховується відповідність між компонентам $\tilde{q}'(\alpha)_{i,j}^{(k,\ell)}$, $q''(\alpha)_{i,j}^{(k,\ell)}$ відповідно форматованого РСПБ $\tilde{Q}'(\alpha)^{(2,k,\ell)}$ та МБПБ базисів $Q''(\alpha)^{(2,k,\ell)}$.

Саме таке функціональне перетворення є основною процесу демаскування (це перше технологічна функція для другого шару СК-перетворень – демаскування форматованого РСПБ базису за компонентами МБПБ $Q''(\alpha)^{(2,k,\ell)}$ базису).

Після чого реалізується ***друга технологічна*** функція f_{rec}:

$$\tilde{a}'(\alpha)_{i,j}^{(k,\ell)} = f_{\text{rec}}\left(\tilde{N}'(\alpha)_{j}^{(k,\ell)}; \tilde{Q}'(\alpha)^{(2,k,\ell)}\right).$$

Це стосується санкціонованого відновлення (*reconstruction*) елементів $\tilde{a}'(\alpha)_{i,j}^{(k,\ell)}$, які несуть інформацію щодо стегано-ППЧ $\tilde{A}'(\alpha)_{j}^{(k,\ell)}$. Для такого випадку функціонал f_{rec} реалізує процес позиційного декодування стегано-кодового значення $\tilde{N}'(\alpha)_{j}^{(k,\ell)}$ в форматованому РСПБ $\tilde{Q}'(\alpha)^{(2,k,\ell)}$.

Відповідно до умов форматування РСПБ базису відновлення стегано-ППЧ $\tilde{A}'(\alpha)_{j}^{(k,\ell)}$ забезпечується без втрат синтаксичної цілісності їх елементів $\tilde{a}'(\alpha)_{i,j}^{(k,\ell)}$. Отже за результатами декодування стегано-кодового значення $\tilde{N}'(\alpha)_{j}^{(k,\ell)}$ відновлюється СППЧ $\tilde{A}'(\alpha)_{j}^{(k,\ell)}$:

$$\tilde{A}'(\alpha)_{j}^{(k,\ell)} = \left\{\tilde{a}'(\alpha)_{1,j}^{(k,\ell)};...;\tilde{a}'(\alpha)_{i,j}^{(k,\ell)};...;\tilde{a}'(\alpha)_{n_\alpha+1,j}^{(k,\ell)}\right\}.$$

Даним технологічним етапом здійснюється ***рекомбінація (вилучення з стегано-кодового значення)*** вбудованого елементу $g(u)_{\chi} = \tilde{a}'(\alpha)_{2,j}^{(k,\ell)}$ до СППЧ:

Процес відновлення доданого елементу у складі стегано-ППЧ на основі зворотних стеганокомпресійних перетворень, а саме вилучення з СК-кодограми та позиційного декодування стегано-кодового значення позначатимемо ***двокаскадною кодовою рекомбінацією прихованої інформації***.

Отже в залежності від позицій елементів $\tilde{a}'(\alpha)_{i,j}^{(k,\ell)}$ в стегано-ППЧ досягається реконструкція елементів $a(\alpha)_{i,j}^{(k,\ell)}$ складових $A(\alpha)_{j}^{(k,\ell)}$ ВС-контейнерів та безпосередньо-вбудованих елементів $g(u)_{\chi}$ прихованого повідомлення G_u.

За результатами відновлення всіх складових $A(\alpha)_{j}^{(k,\ell)}$ будується зміст початкового відеосегменту (ВС) $A^{(k,\ell)}$, а саме:

$$A^{(k,\ell)} = \bigcup_{j=1}^{n} A_j^{(k,\ell)} = \bigcup_{j=1}^{n}\bigcup_{\alpha=1}^{n_\alpha} A(\alpha)_{j}^{(k,\ell)}.$$

Це дозволяє перейти до ***третьої технологічної функції*** f_{ind} загального процесу СК-перетворень. На цьому етапі процес обробки стосується організації непрямого вилучення (*indirect withdrawal*) другого елементу $g(u)_{\chi+1}$ прихованого повідомлення G_u.

Таким чином, на основі зворотних СК-перетворень для кожної α-ї складової *j*-го стовпця $(k;\ell)$ -го відеосегменту матимемо:

1) вилучені два двійкових елементи $g(u)_{\chi}$, $g(u)_{\chi+1}$ прихованого повідомлення G_u - відновлюються на основі змішаних зворотних стеганокомпресійних перетворень в форматованому РСПБ та маскованому БПБ базисах;

2) відновлені елементи $a(\alpha)_{i,j}^{(k,\ell)}$ складової $A(\alpha)_{j}^{(k,\ell)}$ ВС, який використовується в якості контейнеру – реалізується: знаходження стегано-кодового значення за допомогою нерівномірного двійкового кодування за змістом СК-кодограми в умовах МБПБ; позиційне декодування стегано-кодового значення в форматованому РСПБ.

Висновки

1. Розроблено зворотний процес стеганокомпресійних перетворень з виключенням додаткових (надлишкових) відомостей, який враховує умови авторизації (політики доступ) та базується на каскадній концепції:

1) технологічні функції першого каскаду забезпечують ***маскований режим*** відновлення елементів відеосегментів за вилученим з СК-кодограми стегано-кодовим значенням в маскованому базовому поліадичному базисі. Реконструкція ВС досягається з потрібним рівнем синтаксичної та семантичної цілісності;

2) технологічні функції другого каскаду реалізують демаскований режим, який без втрати синтаксичної цілісності забезпечує:

а) відновлення ВС на основі масковано-залежного позиційного декодування стегано-кодових значень в форматованому РСПБ;

б) змішане стеганокомпресійне декодування прихованої інформації, а саме:

- двокаскадну кодову рекомбінацію безпосередньо прихованих елементів з послідуючим їх вилученням з відновлених стегано-ППЧ в форматованому стегано-поліадичному базисі;

- вилучення непрямо прихованих елементів на основі демаскування МБПБ базису з врахуванням залежності між старшими компонентами форматованого РППБ та маскованого БПБ базисів.

Наукова новизна

Вперше створено метод стеганокомпресійного декодування інформації на основі врахуванням змішано-маскованого поліадичного базису.

Відмінності методу полягають у тому що реконструкція стегано-ППЧ організується за двокаскадною концепцією, на основі маскованозалежного позиційного декодування стеганокодового значення в форматованому стеганоніадичному базисі з попереднім вилученням з позиціонованої СК-кодограми за допомогою нерівномірного двійкового блокового кодування її змісту. Це забезпечує: умови для відновлення початкових ВС та вилучення безпосередньоприхованої інформації без втрат синтаксичної цілісності; скорочення кількості обчислювальних операцій для СК-перетворень.

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] Ільяшов О. А., Бурячок В. Л. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу. *Наука и оборона*. 2010. № 4. С. 35–41.

[4] 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.

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

[6] Роман Одарченко, Марина Іванова, Максим Рябенко, 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.

[7] Бараннік В., Сидченко С., Бараннік Д., Бараннік В. Оцінка впливу недетермінованих характеристик на эфективність криптокомпресійного кодування зображень в диференційованому базисі. Безпека інформації. 2020. Том 26. № 3. С. 168–180.

[8] 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.

[9] Бараннік В. В., Власов А. В., Сидченко С. А. Обгрунтування значимих загроз безпеки відеоінформаційного ресурса систем відеоконференцз'вязку профільных систем управління. Інформаційно-управляючісистеми на залізничному транспорті. 2014. № 3. С. 24–31.

[10] Валерій Козловський, Аліна Савченко, Олена Толстікова, Лариса Клобукова 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.

[11] 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.

[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] 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.

[14] Задирака В. К., Никитенко Л. Л. Нові підходи до розробки алгоритмів приховування інформації. Штучный інтелект. 2008. № 4. С. 353–357.

[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] D. Barannik, V. Barannik, S. Korotin, A. Bekirov, O. Veselska, L. Wieclaw 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] D. Barannik and V. Barannik, "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 Оцінка ефективності методів стеганографічного вбудовування інформації в спектральную область зображень. АСУ та прилади автоматики. 2014. Вип. 168. С. 23-29.
[19] 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.
[20] Задирака В. К., Кошкина Н. В. , Никитенко Л. Л. Статистичний аналіз систем з цифровими водяними знаками. Штучный інтелект. 2008. № 3. С. 315–324.
[21] 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/10.1007/978-3-031-24963-126.
[22] 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.
[23] Баранник В. В., Баранник Д. В. , Бекиров А. Е. Основи теорії структурно-комбінаторного стеганографічного кодування: монографія, Х.: Вид-во «Лідер», 2017. 256 с.
[24] 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.
[25] Barannik V., Alimpiev A., Barannik D., Barannik N. Detections of sustainable areas for steganographic embedding // East-West Design & Test Symposium (EWDTS). IEEE, 2017. P. 555–558. DOI: 10.1109/EWDTS.2017.8110028.
[26] Barannik D., Barannik V., Shatun O., Dodukh O., Tverdokhleb V. The indirect method of steganographic embedding of data in an image container based on the information of the contour // 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology. 2018, p. 490–494. DOI: 10.1109/INFOCOMMST.2018.8632155
[27] V. Barannik, D. Barannik, S. Korotin, Olga Veselska Method of Safety of Informational Resources Utilizing the Indirect Steganography. "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.
[28] V. Barannik, D. Barannik, A. Lekakh "A steganographic method based on the modification of regions of the image with different saturation", Advanced Trends in Radioelecrtronics, Telecommuni-cations and Computer Engineering (TCSET), 2018 14th International Conference on, 2018, pp. 542–545. DOI: 10.1109/TCSET.2018.8336260
[29] 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.
[30] Бараннік Д. В. Метод стеганокомпресійного кодування на основі поліадичного базису. *Наукоємні технології*. № 3. 2023. С. 17–26.

Баранник Д. В.

МЕТОД СТЕГАНОКОМПРЕСІЙНОГО ДЕКОДУВАННЯ ІНФОРМАЦІЇ ДЛЯ БЕЗДРОТОВИХ ІНФОКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

В статті обґрунтовується потреба у захисті бортових відеоінформаційних ресурсів наряду із забезпеченням заданих характеристик інформаційного забезпечення в системах управління критичною інфраструктурою (КІ) в умовах протиборства. Стверджується значимість та сприятливі умови щодо використання стеганографічних перетворень в комплексних системах захисту інформації. Одним з них можливість використовувати бортові відеоінформаційні ресурси в якості контейнерів для прихованого вбудовування інформації. При цьому інформацією, що потребує захисту, може бути окремі фрагменти бортових ресурсів (аерофотознімків), які встановлюються як найбільш значимі за рівнем інформативності структурно-семантичного змісту відеосегменти. В свою чергу, це зумовлює вимоги до стеганографічних технологій (СТТ) захисту інформації з використанням бортових відео-контейнерів (БВК). В першу чергу це стосується збільшення стеганографічної ємності за умов цілісного вилучення прихованої інформації на приймальній стороні. В статті стверджується те, що потенціал існуючих інфокомунікаційних технологій кодування та передачі відеоданих з використанням бездротових інфокомунікаційних технологій є недостатнім щодо створення умов для забезпечення потрібних характеристик СТТ. Один з напрямків підвищення ефективності СТТ є застосування методі стеганокомпресійного кодування. В даному випадку вбудовування інформації здійснюється безпосередньо в процесі компресійного кодування БВК. Забезпечується збільшення рівня стеганографічної ємності. Водночас для забезпечення в

умови щодо потрібного рівня цілісності прихованої інформації під час її санкціонованого вилучення на приймальній стороні необхідно розробити метод стеганокомпресійного декодування. Розроблено зворотний процес стеганокомпресійних перетворень з виключенням додаткових (надлишкових) відомостей, який враховує умови авторизації (політики доступ) та базується на каскадній концепції: технологічні функції першого каскаду забезпечують ***маскований режим*** *відновлення елементів відеосегментів за вилученим з СК-кодограми стегано-кодовим значенням в маскованому базовому поліадичному базисі; технологічні функції другого каскаду реалізують демаскований режим без втрати синтаксичної цілісності прихованої інформації.*

Ключові слова: стиснення, відеозображення, стеганокомпресійне декодування, стеганографічна ємність.

Barannik D.

METHOD STEGANOCOMPRESSION DECODING OF INFORMATION FOR DROT-FREE COMMUNICATION TECHNOLOGIES

The article substantiates the need to protect on-board video information resources along with ensuring the specified characteristics of information support in critical infrastructure management systems (CI) in the conditions of confrontation. The significance and favorable conditions for the use of steganographic transformations in complex information security systems are asserted. One of them is the ability to use onboard video information resources as containers for covert embedding of information. At the same time, the information that needs to be protected can be individual fragments of onboard resources (aerial photographs), which are established as the most significant video segments in terms of the level of informativeness of structural and semantic content. In turn, this determines the requirements for steganographic technologies (STT) for information protection using on-board video containers (BVC). First of all, this concerns the increase in steganographic capacity under conditions of holistic extraction of hidden information on the receiving side. The article argues that the potential of existing infocommunication technologies for encoding and transmitting video data using wireless infocommunication technologies is insufficient in terms of creating conditions to ensure the required characteristics of STT. One of the ways to improve the effectiveness of STT is the use of the steganocompression coding method. In this case, the embedding of information is carried out directly in the process of BVC compression coding. An increase in the level of steganographic capacity is provided. At the same time, in order to ensure the required level of integrity of hidden information during its authorized extraction on the receiving side, it is necessary to develop a method of steganocompression decoding. The reverse process of steganocompression transformations with the exclusion of additional (redundant) information has been developed, which takes into account the conditions of authorization (access policy) and is based on the cascade concept: the technological functions of the first stage provide a masked mode of restoration of video segment elements according to the stegano-code value extracted from the SC-codegram in the masked basic polyadic basis; The technological functions of the second stage implement the unmasked mode without losing the syntactic integrity of the hidden information.

Keywords: compression, video, steganocompression decoding, steganographic capacitance.

Стаття надійшла до редакції 23.02.2024 р.
Прийнято до друку 22.03.2024 р.