DOI: 10.18372/2310-5461.60.18270
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;

ТЕХНОЛОГІЯ ПРИХОВУВАННЯ ІНФОРМАТИВНОГО КОНТЕНТУ В ДИНАМІЧНОМУ ПОТОЦІ ВІДЕОСЕГМЕНТІВ

Вступ

Сучасний світ характеризується критичним загостренням множини суперечностей. Це стосується питань національної безпеки, політичних інтересів, економічного розвитку, соціальної політики, територіальної цілісності та правового аспекту [1, 2]. Наслідками чого є: збройна агресія; локальні військові конфлікти; економічні війни; інформаційні війни та операції; кібернетичні та вірусні атаки. Відповідно питання забезпечення належного чину безпеки та оборони держави є край актуальними [3, 4].

В цьому напрямку одним з ключових факторів є реалізації політики кібербезпеки та інформаційної безпеки державних інформаційних ресурсів в інфокомунікаційних системах [5, 6]. У загальному випадку інформаційні ресурси формуються різними типами даних, в тому числі: текстові електронні ресурси; аудіодані; відеодані [7, 8]. Найбільш вагомими з позиції впливу на прийняття рішень є відеоінформаційні ресурси. Особливо в системах підтримки та прийняття рішень для систем управління критичною інфраструктурою [9, 10]. Відеоінформаційні ресурси, до яких відносяться відеозображення та динамічні відеопотоки, мають найбільший рівень інформативності та сприйняття. При чому таке відбувається, як для автоматизованого, так й для автоматичного режимів аналізу та прийняття рішень [11, 12]. З іншого боку відеоінформаційні ресурси мають: найбільший рівень інформаційної інтенсивності; складність структурно-семантичного контенту. Це, в свою чергу, впливає на можливості інфокомунікаційних технологій щодо забезпечення базових категорій інформаційної безпеки, тобто: доступність, конфіденційність та цілісність [13, 14]. В залежності від прикладної сфери застосування та особливостей реалізації інформаційного забезпечення кожна з цих категорій може мати різний рівень значимості та актуальності.

В умовах воєнного часу, інформаційного протиборства важливим є своєчасне надання достовірної інформації з обмеженим часом актуальності. Прикладами таких ситуацій є організація «живого» доступу до дистанційної інформації в режимі реального часу з використанням безпілотних платформ на значної відстані від центрів прийняття рішень [15, 16]. В загальному випадку безпілотні платформи можуть бути наземного, надводного, повітряного та космічного базування. В цьому випадку на етапі доставки інформації застосовуються бездротові телекомунікаційні технології. Виникають випадки появи дисбалансу між вимогами до забезпечення потрібного рівня категорій інформаційної безпеки та обмеженими можливостями щодо продуктивності дистанційних інфокомунікаційних систем [17, 18]. Наслідками є: втрата доступності та цілісності відеоресурсів; обмежена можливість забезпечити потрібний рівень конфіденційності в умовах жорстких вимог щодо організації доступності відеоінформації [19, 20]. Отже забезпечення потрібного рівня інформаційної безпеки відеоінформаційних ресурсів з використанням інфокомунікаційних технологій на базі безпілотних платформ є ***актуальною науково-прикладною задачею***.

Аналіз останніх досліджень та публікацій

Існуючі концепції реалізації питань інформаційної безпеки відеоданих для бортових комплексів ґрунтуються на концепції послідовною схеми [21, 22]. В цьому випадку технології, які забезпечують кожну з категорій інформаційної безпеки, використовуються послідовно. Зачасти використовується наступна послідовність: технології компресійного кодування; технології криптографічного захисту інформації; технології завадостійкого кодування [23, 24]. Водночас така концепція має певні недоліки. Вони стосуються наступного:

1) для технологій компресійного кодування існує дисбаланс щодо можливістю забезпечення доступності та цілісності відеоінформації [25, 26];

2) існують певні законодавчі обмеження щодо використання криптографічних технологій гаран-

тованого захисту інформації для бортових комплексів [27, 28];

3) для переробки інформації використовуються закордонні технологічні реалізації [29, 30];

4) виникають значні часові затримки, що перевищують критичний поріг відносно вимог до оперативності доставки відеоінформації [31, 32].

В якості альтернативного підходу пропонується в комплексі з методами криптографічного захисту додатково використовувати технології стеганографічного перетворення.

В цьому випадку з'являється можливість приховувати найбільш значимі інформативні ресурси в загальному відео інформаційному потоці. Наприклад, приховувати у динамічному потоці відеосегментів інформацію щодо найбільш вагомих інформаційних складових. Такими інформаційними складовими можуть бути окремі відеосегменти, які містять інформацію щодо об'єктів інтересу, або цілковиті відеозображення. Динамічний потік відеосегментів в цьому випадку додатково виконує роль контейнеру.

У разі приховування окремих відеосегментів, які мають найбільший інтерес, попередньо необхідно застосовувати технології їх ідентифікації (класифікації) та селекції. Для цього можна використовувати технології, які викладено в наступних наукових працях [33; 34]. Для ідентифікації відеосегментів за рівнем інформативної ваги використовується сукупність структурних ознак. При цьому виявлення та детектування структурних ознак може здійснюватись в просторі яскравості або в спектральному просторі.

Зрозуміло, що в загальному випадку кількість інформативних відеосегментів, інформацію за яких потрібно приховувати, буде змінною. Отже необхідно використовувати стеганографічні перетворення, які створюють можливість для збільшення інформаційної ємності прихованих даних в умовах забезпечення потрібного рівня цілісності в процес і вилучення та візуального маскування.

Постановка проблеми

В загальному випадку базовою вимогою для стеганографічних систем в процесі приховування інформації в динамічному потоці відеосегментів є [18, 19]:

1) швидкість прихованого каналу передачі повідомлень у відеопотоці;

2) візуальна помітність слідів вбудовування повідомлень у відео контейнерах;

3) рівень цілісності прихованих повідомлень, які вилучаються авторизованими користувачами на приймальній стороні (ймовірність виникнення помилок в процесі вилучення прихованих повідолень з контейнеру)

4) рівень впливу на ефективність процесів стиснення відео-контейнерів (рівень втрати ефективності стиснення відео-контейнерів).

Водночас існуючі технології стеганографічних перетворень мають певні недоліки, які проявляються у протиріччі між групами базових показників якості вбудовування інформації [19].

Звідси ***мета досліджень статті*** стосується розробки технології приховування інформативного відеоконтенту в динамічному потоці відеосегментів на основі.

Розробка методу приховування інформації у динамічному потоці відеосегментів на основі стеганокомпресійної концепції

В працях [20–23] запропонований підхід до створення нового підходу щодо побудови технологій стеганографічного перетворення. Для такого випадку на відміну від існуючих пропонується для вбудовування використовувати наявну кількість структурної надмірності у відео-контейнері. При цьому приховування інформації організується безпосередньо в процесі компресійного кодування відео-контейнеру. Тому означений підхід запропоновано визначати, як стеганокомпресійне кодування (СКК). Реалізація СКК-технології базується на методах поліадичного кодування [24; 25].

В працях [26; 27] обґрунтовується те, що запропоноване технологія СКК створює потен-ціал для підвищення ефективності прихованого вбудовування інформації за найбільш вагомими показниками. Сюди відносяться збільшення пропускної здатності прихованого каналу передачі повідомлень з використанням відеоінформаційного потоку для заданих: показника візуального маскування прихованих повідомлень у відеоконтейнері; цілісності вилучених даних авторизованими користувачами [28; 29]. Водночас в працях показано, що у разі використання створеного підходу виникають ситуації з утворенням кількості стеганографічної надмірності [30; 31]. Така ознака може використовуватись в процесі несанкціонованого стеганоаналізу. Тому для усунення даної вразливості в роботі пропонується проводити маскування кількості стеганографічної надмірності. Вона стосується корекції основи поліадичного базису відповідних елементів.

Розглянемо функціонування стеганографічної системи на основі корекції нерівновагового базису основ. Дана система дозволяє вбудувати біт приховуваного повідомлення на другу позицію поліадичного числа в процесі стеганографічного кодування.

Маємо для приховування послідовність $B = \{[b_1]_2;...;[b_\xi]_2;...;[b_v]_2\}$ інформативного кон-

тенту. Де $[b_\xi]_2$ $-\xi$-й двійковий елемент такої послідовності, $[b_\xi]_2 \in [0;1]$. Відповідно довжина послідовності В дорівнює ν. Приховування відбувається до поліадичного числа $A^{(j)}$, $A^{(j)} = \{a(1)_i;...;a(j)_i;...;a(m)_i\}$. Тому $A^{(j)}$ є числом-контейнером. В загальному випадку послідовність $A^{(j)}$ є компонентою динамічного потоку відеосегментів. Наприклад, $A^{(j)}$ може бути рядком, стовбцем або діагональною послідовністю відеосегменту (трансформанти). Довжина такого числа позначається, як m.

Стеганографічна система включає до себе два базових процеси: пряме стеганографічне перетворення – вбудовування інформації до контейнеру; зворотне стеганографічне перетворення – вилучення прихованої інформації з контейнеру.

Розглянемо перший процес – стеганографічне кодування з корекцією нерівновагового базису основ $\Psi'^{(1)}$. Він базується наступними технологічними процесами:

1. Імплантація двійкового елементу $[b_\xi]_2$ інформативного контенту на другу позицію в числі $A^{(j)}$ контейнеру. Відповідно такий етап описується наступним математичним виразом: $A'^{(j)} = A^{(j)} \bigcup [b_\xi]_2$, для $[b_\xi]_2 = a'_{2,j}$. Після чого матимемо стегано-послідовність $A'^{(j)}$, тобто $A'^{(j)} = \{a(1)_i;a'(2)_i;...;a(j)_i;...;a(m+1)_i\}$. Тут на позиції $i=2$ знаходиться біт $a'(j)_2$ прихованого контенту.

2. Реалізується процес компресійного кодування. Послідовністю для кодування є стеганочисло $A'^{(j)}$. Звідси утворюється стегано-кодове значення $N'^{(j)}$. Для цього використовується наступне співвідношення:

$$N'^{(j)} = a(j)_1 V'_{1,j} + a'(j)_2 V'_{2,j} + \varphi(a(j)_i)_3^{m+1}$$

$$V'_{2,j} = \varphi_3^{m+1}; \qquad V'_{1,j} = \psi'_{2;j} \cdot \varphi_3^{m+1},$$

де $\psi'_{2;j} \cdot \varphi_3^{m+1}$ – функціонал визначення ваги $V'_{1,j}$ першого елементу СТЧ; φ_3^{m+1} – функціонал визначення ваги $V'_{2,j}$ вбудованого двійкового елементу; $\psi'_{2;j}$ – основа вбудованого елементу; $\psi_{i;j}$ – основа $(i;\ j)$-го елементу СТЧ $A'^{(j)}$.

3. Здійснюється маскування ознак, які вказують щодо наявності кількості структурної стеганографічної надмірності. Для цього проводиться попередня корекція початкового поліадичного базису $\Psi^{(1)}$. Відповідні перетворення реалізуються операцією збільшення значення основи першого елементу СПЧ $A'^{(j)}$. В роботі [33; 34] показано основу $\psi_{1;j}$ потрібно збільшити в 2 рази, $\psi''_{1;j} = \psi_{1;j} \times 2$. Відповідно формується модифікований поліадичний базис $\Psi'^{(1)}$. Він описується наступним чином:

$$\Psi'^{(1)} = \{2 \cdot \psi_{1;j}; \psi_{2;j};...;\psi_{i;j};...;\psi_{m;j}\} =$$

$$= \{\psi''_{1;j}; \psi_{2;j};...;\psi_{i;j};...;\psi_{m;j}\}.$$

Тут потрібно зауважити на те, що саме модифікований базис буде використовуватись для поліадичного декодування ДПВС у разі несанкціонованого доступу. В статті [33; 34] обґрунтовано, що запропонований підхід дозволяє уникнути візуальних спотворень. Тобто зменшується успіх візуальної стеганографічної атаки.

4. На завершальному етапі побудови синтаксичного опису компактного представлення стеганочисла $A'^{(j)}$ проводиться формування стеганокодограми $\tilde{N}'^{(j)}$. Вона утворюється для двійкового опису величини $N'^{(j)}$, та має такий вигляд: $\tilde{N}'^{(j)} = \{c_1,...,c_\tau,...,c_{q(j)'}\}$. Тут $q(j)'$ – довжина стегано-кодограми $\tilde{N}'^{(j)}$. величина $q(j))$ визначається виразом $q(j)' = [(\sum_{i=1}^{m+1} \ell og_2 \psi_{i;j})] + 1$.

Розглянемо другий процес стеганокомпресійної системи – стеганографічне декодування з врахуванням модифікованого базису $\Psi'^{(1)}$. Він враховує варіанти неавторизованого та авторизованого відновлення ДПВС. Тому такий принцип можна формулювати, як біполярне зворотне стеганографічне перетворення.

Варіант відновлення ДПВС в неавторизованому режимі. В цьому випадку здійснюється: візуальна атака щодо встановлення факту наявності вбудованого інформативного контенту у динамічному потоці відеосегментів; проводиться спроба несанкціонованого вилучення прихованого контенту. В цьому випадку для неавторизованого користувача відсутні такі відомості :

1) інформація щодо позиції, на яку здійснюється імплантація двійкового елементу $[b_\xi]_2$ прихованого контенту В, тобто є невідомою позиція елемента $a'(j)_2$;

2) інформація щодо координат розташування стегано-кодограми в загальному синтаксичному описі компактного представлення ДПВС.

Відповідна інформація є складовою ключа, який використовується в процесі прихованого вбудовування інформативного контенту до стегано-послідовностей ДПВС.

Отже у разі несанкціонованого доступу до ДПВС відомими є:

- встановлена послідовність технологічних дій щодо відновлення ДПВС;

- модифікований базис $\Psi'^{(1)}$.

З врахуванням чого неавторизований користувач здійснює відновлення ДПВС за загальним технологічним конвеєром. Відповідно виконуються такі перетворення:

1. Вилучення з стегано-кодограми $\tilde{N}'^{(j)}$ стегано-кодового значення $N'^{(j)}$ за допомогою модифікованого базису $\Psi'^{(1)}$.

2. Відновлення елементів вихідної послідовності відеосегментів ДПВС на основі поліадичного декодування.

В цьому випадку відновлення елементів $a'''(j)_i$ проводиться з використанням модифікованого базису $\Psi'^{(1)}$. Тому декодування першого елементу $a'''(j)_i$ вихідної відеопослідовності організується за допомогою основи $\psi''_{1,j}$, яка є модифікованою. Відповідно співвідношення для декодування має наступний вигляд :

$$a'''(j)_1 = F_d(N'^{(j)}; \psi''_{1;j}; V_{1,j}).$$

Тут $F_d(N'^{(j)}; \psi''_{1;j}; V_{1,j})$ – функціонал структурного декодування за інформацією щодо стегано-кодового значення $N'^{(j)}$ та основи $\psi''_{1;j}$.

Зрозуміло те, що реконструкція першого елементу $a'''(j)_1$ послідовності $A'''^{(j)}$ відеосегменту ДПВС супроводжується появою спотворень, які мають контрольовані та обмежені значення. Водночас декодування всіх інших елементів $a'''(j)_i$, $i \in [2; m]$ забезпечується без внесення втрат цілісності інформації.

Відповідно усуваються додаткові можливості та ознаки, які використовуються в процесі стеганоаналізу з боку зловмисної сторони.

Варіант відновлення ДПВС в авторизованому режимі. При цьому проводиться одночасне вилучення прихованого контенту. Для цього використовується структурне стеганографічне декодування. Відповідно в авторизованому режимі відомою є ключова інформація. Отже маємо:

1) інформацію відносно позиціонування стегано-кодограми в загальному синтаксичному описі компактного представлення ДПВС;

2) інформацію відносно позиції двійкового елементу $[b_\xi]_2$ прихованого контенту В в стеганочислі. Отже відомою є позиція елементу $a'(j)_2$ в СПЧ;

3) інформація відносно основи $\psi'_{2;j}$ елементу $a'(j)_2$ прихованого контенту в СПЧ. Відповідно відомим є процес маскування ознак наявності кількості структурної стеганографічної надмірності.

Тоді з врахуванням наявної ключової інформації процес зворотного структурного стеганографічного перетворення в авторизованому режимі представляється наступними технологічними діями:

1. Вилучення з стегано-кодограми $\tilde{N}'^{(j)}$ стегано-кодового значення $N'^{(j)}$.

2. Декодування елементу $a'(j)_2$, який містить інформацію щодо відповідного елементу $[b_\xi]_2$ прихованого контенту. Для цього використовуються ключові відомості відносно координати вбудованого елементу в СПЧ та його модифікованої основи $\psi'_{2;j} = 2$. Відповідно до чого декодування вбудованого елементу організується наступним співвідношенням:

$$a''(j)_2 = F_d(N'^{(j)}; \psi'_{2;j}; V'_{1,j}).$$

Тут $F_d(N'^{(j)}; \psi'_{2,j}; V'_{1,j})$ – функціонал структурного декодування за інформацією щодо стегано-кодового значення $N'^{(j)}$ та основи $\psi'_{2;j}$.

За результатом означеного процесу стеганографічного декодування маємо значення елементу $a''_{2,j}$, яке відповідає біту $[b_\xi]_2$ прихованого контенту В, тобто $[b_\xi]_2 := a''(j)_2$.

3. Процес декодування всіх інших елементів $a(j)^*_i$ відеосегменту ДПВС організується з врахуванням модифікованого базису $\Psi'^{(1)}$. В даному випадку можливе демаскування структурної стеганографічної надмірності шляхом відновлення початкового значення величини $\psi_{1;j}$. Така дія проводиться за допомогою формули:

$$\psi_{1;j} = \frac{\psi''_{1;j}}{2}.$$

Водночас потрібно враховувати те, що значення модифікованої основи $\psi''_{1;j}$ не використовується в процесі реконструкції елементів $a(j)^*_i$. Тоді структурне стеганографічне декодування забезпечується без демаскування структурної стеганографічної надмірності. Це дозволить знизити кількість операцій, які витрачаються на загальний процес структурного стеганографіч-ного декодування (вилучення прихованого інформативного контенту), та відновлення відеосегментів ДПВС.

Висновки

1. Створено правило приховування інформативного контенту в процесі структурного стеганокомпресійного кодування. Таке правило базується на тому, що:

1) один двійковий елемент прихованого контенту імплантується на другу позицію поліадичного числа;

2) для маскування ознак наявності кількості стеганографічної надмірності проводиться модифікація основа першого елементу. Такий процес реалізується на основі збільшення значення відповідної основи в два рази.

Використання такого стеганографічного правилу в процесі побудови стеганокомпресійного кодування дозволяє:

1) узгодити довжини кодограм коду-контейнера та стегано-кодограми;

2) організувати декодування та вилучення елементу прихованого контенту без втрати його синтаксичної цілісності;

3) провести відновлення елементів відеосегментів ДПВС без втрати їх семантичної цілісності. При цьому обмежені спотворення можуть виникати в незначній кількості елементів відеосегментів.

На основі правила побудовано структурне стеганокомпресійне кодування з модифікованим базисом. Це дозволяє вбудовувати двійковий елемент на другу позицію в СПЧ. Забезпечується приховування контенту в умовах:

1) відсутності корекції стегано-кодограми;

2) зниження кількості спотворень, які можуть виникати в стегано-кодовому значені;

3) досягається стійкість прихованого контенту щодо стегано-атак.

Наукова новизна. Вперше розроблено структурне стеганокомпресійне кодування на основі імплантації біту приховуваного контенту на другу позицію в СПЧ з модифікованим базисом. Відмінною рисою методу є те, що без внесення спотворень в стегано-кодограму забезпечується усунення ознак наявності кількості стеганографічної структурної надмірності. Це дозволяє зни-зити можливість встановлення факту наявності прихованого контенту у разі несанкціонованого доступу.

2. Розроблено стеганографічне декодування на основі одночасного відновлення елементів відеопослідовності та вбудованого на другій її позиції елементу прихованого контенту. Процес декодування не передбачає усунення ознак локалізації кількості структурної стеганографічної надмірності. Декодування ґрунтується такими етапами:

1) структурне стеганографічне декодування, яке забезпечує відновлення поліадичного числа з імплантованим її другій позиції елементом прихованого контенту;

2) вилучення елемента приховуваного контенту.

Наукова новизна. Вперше розроблено структурне стеганографічне декодування без усунення ознак локалізації кількості структурної стеганографічної надмірності. Відмінною рисою методу є те, що вилучення прихованої інформації та відновлення відеосегменту проводиться на основі реконструкції стегано-кодограми за біполярним принципом без демаскування ознак кількості стеганографічної надмірності. Це дозволяє підвищити ефективність вилучення приховуваного контенту та локалізувати атаки зловмисної сторони щодо виявлення факту вбудовування.

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 і 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. Комп'ютерна стенографія. 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 ефективність криптокомпресійного кодування зображень в диференційованому базисе. *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. та ін. Обґрунтування значимих загроз безпеки відеоінформаційного ресурсу систем відеоконференцзв'язку профільних систем

управління. Інформаційно-управляючі системи 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] Бараннік В. В., Сидченко С. А., Бараннік Д. В. Метод криптокомпресійного представлення зображень на основі двокаскадного узагальненого позиційного кодування в базисі по верхнім межам. *Радіоелектроніка та інформатика*. 2017. № 1(76). С. 22–27.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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.

[20] Конахович Г. Ф. та ін. Сучасні методи квантової стеганографії. Захист інформації. № 2 (51), 2011. С. 5–9.

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

[22] 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.

[23] 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.

[24] Задирака В. К., Кошкина Н. В., Никитенко Л. Л. Статистичний аналіз систем з цифровими водяними знаками. Штучный інтелект. 2008. № 3. С. 315–324.

[25] 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.

[26] 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.

[27] Бараннік В. В., Баранник Д. В., Бекиров А. Е. Основи теорії структурно-комбинаторного стеганографічного кодування: монография. Х.: В-во «Лідер», 2017. 256 с.

[28] 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.

[29] 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.

[30] 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

[31] 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.

[32] 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, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference on, 2018, pp. 542–545. DOI: 10.1109/TCSET.2018.8336260

[33] 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.

[34] Бараннік Д. В. Метод стеганокомпресійного кодування на основі поліадичного базису. Наукоємні *технології*. №3. 2023. С. 17 – 26.

Бараннік Д. В.

ТЕХНОЛОГІЯ ПРИХОВУВАННЯ ІНФОРМАТИВНОГО КОНТЕНТУ В ДИНАМІЧНОМУ ПОТОЦІ ВІДЕОСЕГМЕНТІВ

В статті показано, що в умовах воєнного часу, інформаційного протиборства важливим є своєчасне надання достовірної інформації з обмеженим часом актуальності. Прикладами таких ситуацій є організація «живого» доступу до дистанційної інформації в режимі реального часу з використанням безпілотних платформ на значної відстані від центрів прийняття рішень. Обґрунтовується наявність випадків появи дисбалансу між вимогами до забезпечення потрібного рівня категорій інформаційної безпеки та обмеженими можливостями щодо продуктивності дистанційних інфокомунікаційних систем. Наслідками є : втрата доступності та цілісності відеоресурсів; обмежена можливість забезпечити потрібний рівень конфіденційності в умовах жорстких вимог щодо організації доступності відеоінформації. Отже в статті доводиться те, що актуальним є забезпечення потрібного рівня інформаційної безпеки відеоінформаційних ресурсів з використанням інфокомунікаційних технологій на базі безпілотних платформ. Показано, що існуючі концепції реалізації питань інформаційної безпеки відеоданих для бортових комплексів ґрунтуються на концепції послідовною схеми. Водночас така концепція має певні недоліки. В статті в якості альтернативного підходу пропонується в комплексі з методами криптографічного захисту додатково використовувати технології стеганографічного перетворення. В цьому випадку з'являється можливість приховувати найбільш значимі інформативні ресурси в загальному відео інформаційному потоці. Водночас стверджено, що існуючі технології стеганографічних перетворень мають певні недоліки, які проявляються у протиріччі між групами базових показників якості вбудовування інформації. Викладається створення правила приховування інформативного контенту в процесі структурного стеганокомпресійного кодування. Вперше розроблено структурне стеганокомпресійне кодування на основі імплантації біту приховуваного контенту на другу позицію в стегано-послідовності з модифікованим базисом. Відмінною рисою методу є те, що без внесення спотворень в стегано-кодограму забезпечується усунення ознак наявності кількості стеганографічної структурної надмірності. Розроблено стеганографічне декодування на основі одночасного відновлення елементів відеопослідовності та вбудованого на другій її позиції елементу прихованого контенту.

Ключові слова: інформаційна безпека, відеозображення, стеганокомпресійне кодування, стеганографічна надмірність.

Barannik D.

TECHNOLOGY FOR HIDING INFORMATIVE CONTENT IN THE DYNAMIC STREAM OF VIDEO SEGMENTS

The article shows that in the conditions of wartime, information confrontation, it is important to provide timely reliable information with limited time of relevance. Examples of such situations are the organization of "live" access to remote information in real time using unmanned platforms at a considerable distance from decision-making centres. The existence of cases of imbalance between the requirements for ensuring the required level of information security categories and limited capabilities for the performance of remote infocommunication systems is substantiated. The

consequences are: loss of availability and integrity of video resources; limited ability to ensure the required level of confidentiality in the face of strict requirements for the organization of the availability of video information. Thus, the article proves that it is important to ensure the necessary level of information security of video information resources using infocommunication technologies based on unmanned platforms. It is shown that the existing concepts of implementation of issues of information security of video data for on-board complexes are based on the concept of a sequential scheme. At the same time, this concept has certain disadvantages. As an alternative approach, the article proposes to additionally use steganographic conversion technologies in combination with cryptographic protection methods. In this case, it becomes possible to hide the most significant informative resources in the general video information flow. At the same time, it is argued that the existing technologies of steganographic transformations have certain shortcomings, which are manifested in the contradiction between the groups of basic indicators of the quality of information embedding. The creation of a rule for hiding informative content in the process of structural steganocompression coding is outlined. For the first time, structural steganocompression coding was developed based on the implantation of a bit of concealed content in the second position in the quilted sequence with a modified basis. A distinctive feature of the method is that without introducing distortions into the stegano-codogram, it is ensured that the signs of the presence of a number of steganographic structural redundancy are eliminated. Steganographic decoding based on the simultaneous restoration of elements of the video sequence and the element of hidden content embedded in its second position has been developed.

Keywords: information security, video imaging, steganocompression coding, steganographic redundancy.

Стаття надійшла до редакції 03.11.2023 р.
Прийнято до друку 19.12.2023 р.