DOI: 10.18372/2310-5461.51.15690

УДК 621.327: 681.5

Н. В. Бараннік
Харківський національний університет
цивільного захисту України
orcid.org/0000-0001-6420-1838
e-mail: barannik11121972@gmail.com

МЕТОДОЛОГІЯ СТВОРЕННЯ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ НЕПРЯМОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ МУЛЬТІАДИЧНИХ ПЕРЕТВОРЕНЬ

Вступ

Одним з актуальних напрямків для підвищення безпеки інформаційних ресурсів при передачі в інфокомунікаційних системах є використання методів стеганографічного вбудовування інформації в відеозображення. Ефективність таких методів значно підвищується у разі використання в комплексі методів приховування, які засновані на принципах безпосереднього та непрямого вбудовування повідомлень. Це дозволяє [1; 2; 3] створити умови для локалізації дисбалансу між своєчасністю доведення скритої інформації (спеціальної інформації) та показником її достовірності [4; 5–7].

Постановка проблеми

Водночас існуючі методи стеганографії використовують у процесі вбудовування інформації в основному лише закономірності, що породжуються особливостями візуального сприйняття відеозображень. У свою чергу, це спричиняє те, що з використанням сучасних телекомунікаційних технологій та технології кодування відеоконтейнерів H26* створюються умови для організації каналу прихованих повідомлень, який дозволяє вбудовувати повідомлення на рівні 3-20 М пікселів для ПВСШ 20 дБ. Це відповідно створює умови для приховування відеозображень формату FullHD [8; 9; 10]. Однак при цьому рівень ПВСШ дорівнює 20 дБ, що означає наявність значних спотворень відеоконтейнерів. Отже, такий рівень ПВСШ не задовольняє потрібному рівню достовірності відеоінформації в системах управління об'єктами критичної інфраструктури. Навпаки, для заданого рівня достовірності (величина ПВСШ сягає 40 дБ) створюються умови для приховування повідомлень бітовим об'ємом лише 1,5 М. Це дозволяє приховувати відеозображення форматом CIF та SD. Але такий формат відеозображень, що приховуються, не задовольняє вимогам відносно повноти відеоінформації [11–15].

Отже ***науково-прикладна задача***, яка полягає в підвищені щільності вбудованих у відеоконтейнер повідомлень з заданим рівнем їх достовірності, є ***актуальною***.

В основі вирішення цього завдання знаходиться вирішення протиріччя, яке стосується того, що підвищення щільності вбудованих даних призводить до зниження бітової швидкості відеоконтейнеру, стійкості до стеганоаналізу, достовірності спеціальної інформації та відеоконтейнеру [14; 16; 17].

Для вирішення цієї суперечності пропонується розробляти стеганографічні методи, які дозволяють вбудовувати повідомлення в умовах виключення потреби (або обмеженості) у використанні психовізуальних закономірностей. Тобто процес вбудовування повідомлень не повинен супроводжуватись внесенням додаткових спотворень в відеоконтейнер [18–20].

Тому ***метою дослідження*** є розробка методології стеганографічного вбудовування інформації з урахуванням закономірностей відеоконтейнеру, які породжені його структурними та структурно-статистичними особливостями.

Аналіз останніх досліджень та публікацій

Вирішення сформульованої задачі в області застосування стеганографічних перетворень пропонується реалізовувати з використанням методів непрямого вбудовування біту скриваємого повідомлення деяку умову або функціональну залежність [21–25].

Але, в свою чергу, для ***існуючих*** методів непрямого стеганографічного перетворення

характерний недолік, який полягає у недостатньому значенні щільності вбудованих даних щодо сучасних вимог [24; 26; 27].

Для усунення недоліків непрямого стеганографічного вбудовування пропонується розробити підхід, який дозволить використовувати для приховування не тільки психовізуальну, але й структурну надмірність відеоконтейнеру [28–34].

Для побудови стеганографічної системи в умовах виконання необхідних вимог ***пропонується*** використовувати мультіадичні перетворення [35–37]. У цьому випадку досягається таке.

1. Закономірності виявляються адаптивно для кожного масиву даних, мають структурно-комбінаторне походження та описуються кількісно у вигляді оцінок ψ_i динамічних діапазонів елементів масиву даних. Тобто :

$$\psi_i = \max_{1 \le i \le m} \{a_{i,j}\} + 1 \qquad j = \overline{1,n},$$

де $a_{i,j}$, j-й елемент i-го рядку масиву A.

2. Існує можливість за відновленими елементами масиву даних встановити з заданою цілісністю відповідну умовну залежність. Це забезпечує умову для вилучення прихованого повідомлення інформації без втрат [38; 39].

У цьому випадку процес вилучення прихованої інформації буде здійснюватися шляхом аналізу значень початкової Ψ та модифікованої Ψ' службової інформації.

Модифікації в області структурно-комбінаторних закономірностей створює можливість щодо уникнення її впливу на значення елементів відеоданих. Тому є потенціал відносно уникнення спотворень в масивах відеоданих [40; 41].

Пропонується масив даних розглядати як контейнер для непрямого вбудовування інформації в спектральній області.

Це зумовлено тим, що для трансформанти ДКП створюються умови для виявлення й скороченні більшої кількості структурно-комбінаторної надмірності ніж в просторово-часовій області [42; 43].

Отже, для трансформанти ДКП підвищується потенціал відносно вбудовування прихованого повідомлення за рахунок модифікації в області закономірностей за динамічними діапазонами в умовах наявності відповідної кількості структурно-комбінаторної надмірності

Таким чином, обґрунтовано вибір мультіадичної системи для організації непрямого приховування інформації в умовах забезпечення уникнення втрат, як вбудованої інформації, так і додаткових спотворень контейнеру.

Створення методології стеганографічної системи непрямого приховування інформації

Мультіадична система (МАС) — система $F_{mads}(A_j; E_j; \Psi; \delta_j = 0)$ взаємно однозначного $(\delta_j = 0)$ формування кодових значень E_j для послідовностей A_j в мультіадичному просторі з встановленою системою Ψ основ. Тут δ_j — середньоквадратичне відхилення елементів декодованого мультіадичного числа відносно елементів початкового МАД числа. Це описується виразом :

$$\delta_j = \sqrt{\frac{\sum_{i=1}^{m} (a_{i,j}^{(\theta)} - a_{i,j})^2}{m}},$$

де m — кількість елементів в мультіадичному числі; $a_{i,j}^{(\theta)}$, $(i; j)$-й елемент для θ-го варіанта відновлення початкового мультіадичного числа A_j; $A_{\theta,j}$ — j-є мультіадичне число для θ-го варіанта побудови системи Ψ_θ основ, $A_{\theta,j} = (a_{1,j}^{(\theta)}; ...; a_{i,j}^{(\theta)}; ...; a_{m,j}^{(\theta)})$.

Мультіадична система складається з двох базових операторів $\varphi_{emad}(A_j; \Psi)$, $\varphi_{dmad}(E_j; \Psi)$.

Отже:

$$F_{mads}(A_j; E_j; \Psi; \delta_j = 0) = \{\varphi_{emad}(A_j; \Psi); \varphi_{dmad}(E_j; \Psi)\}.$$

Тут $\varphi_{emad}(A_j; \Psi)$, $\varphi_{dmad}(E_j; \Psi)$ — оператори, які реалізують технологію прямого (кодування) та зворотного (декодування) мультіадичного перетворень відповідно.

Уведемо поняття базової МАС. Під базовою (опорною) мультіадичної системою розуміють таку систему, яка формується безпосередньо для конкретного масиву даних (блок відеоданих, трансформанта).

Отже, у цьому випадку ***базова система*** Ψ основ ψ_i це така система, значення основ якої визначаються за правилами :

$$\psi_i = \max_{1 \le j \le n} \{a_{i,j}\} + 1, \; i = \overline{1, m}.$$

Тобто значення основ ψ_i для базової системи Ψ визначаються як динамічні діапазони елементів в рядках масиву даних.

Визначення основ ψ_i за динамічним діапазоном не для окремих елементів $a_{i,j}$ мультіадичних чисел, а за сукупністю елементів в рядках, тобто $A_i = \{a_{i,1}; ...; a_{i,j}; ...; a_{i,n}\}$, зумов-

лено необхідністю зменшення бітового об'єму службової складової. Тоді в середньому на кожен елемент стовпця масиву даних (трансформанти) буде припадати в середньому $(\log_2\psi_i / n)$ двійкових розрядів. Звідки, зі зростанням кількості стовпців n величина $(\log_2\psi_i / n)$ буде зменшуватися. Отже, буде скорочуватися загальний бітовий об'єм компресійного представлення масиву даних (трансформанти) у результаті мультіадичного кодування його стовпців.

Зрозуміло, що для можливості непрямого приховування інформації в мультіадичний системі на рівні структурних мета-ознак потрібно щоб МАС була притаманна така властивість (характеристика).

Властивість МАС. Властивість мультіадичної системи (МАС) щодо можливості формування та безпомилкового відновлення одного мультіадичного числа A_j декількома кодовими значеннями $E_{\theta,j}$ в різних системах Ψ_θ основ.

Тобто відносно безпомилкового прямого та зворотного перетворень одного мультіадичного числа A_j у різних мультіадичних системах $F_{mads}(A_j; E_j; \Omega(\Psi); \delta_j = 0)$ де $\Omega(\Psi)$ — множина мультіадичних базисів Ψ_θ, для яких забезпечується дана властивість МАС.

Для ствердження такої властивості МАС сформулюємо та доведемо таке ***твердження***.

Для узагальнення висновків твердження будемо розглядати її без прив'язки до конкретної трансформанти або масиву відеоданих. Тут A_j початкове одновимірне мультіадичне (МАД) число, $A_j = \{a_{1,j}; ...; a_{i,j}; ...; a_{m,j}\}$ в базисі $\Psi = \Psi_\theta$ основ $\psi_i = \psi_i^{(\theta)}$, $i = \overline{1, m}$, для якого знаходиться кодове значення $E_j = E_{\theta,j}$.

Отже, в даному випадку відповідає таке формулювання твердження.

Твердження про наявність множини допустимих мультіадичних систем для однієї послідовності (про модифікації системи основ)

Існує така множина $\Omega(\Psi)$ систем основ Ψ_θ, $\theta = \overline{1, \Theta}$, для яких за допомогою множини $\Omega(E)$ відповідних кодових значень $E_{\theta,j}$, $\theta = \overline{1, \Theta}$ для однієї послідовності A_j досягається взаємно однозначне (безпомилкове) пряме та зворотне мультіадичне перетворення, а саме:

$$A_j = \varphi_{dmad}(E_{\theta,j}; \Psi_\theta), \text{ щодо}$$

$$E_{\theta,j} = \varphi_{emad}(A_j; \Psi_\theta),$$

де $W_{\theta,i}$ — ваговий коефіцієнт i-го елементу послідовності A_j у разі використання θ-го варіанта побудови системи Ψ_θ основ.

Дане твердження дозволяє встановити умови модифікації системи основ мультіадичного простору, для яких забезпечується відновлення елементів початкової послідовності без втрат інформації. Отже, існує безліч $\Omega(\Psi)$ варіантів модифікацій системи Ψ_θ основ, для яких виключаються втрати інформації в процесі реконструкції елементів мультіадичних (МАД) чисел з використанням відповідних кодових значень. Взаємне однозначне перетворення між кодовими значеннями $E_{\theta,j}$ та відповідним МАД числом A_j ***буде*** виконуватись у разі:

- вибору системи Ψ_θ основ $\psi_i^{(\theta)}$, яка входить до допустимої множини $\Omega(\Psi)$ варіантів побудови;
- формування відповідних кодових значень $E_{\theta,j}$ у допустимих системах Ψ_θ основ.

В окремому випадку для двох допустимих систем Ψ_θ, Ψ_ϑ основ, тобто $\Psi_\vartheta, \Psi_\theta \in \Omega(\Psi)$, $\theta \neq \vartheta$, в умовах формування кодових значень за виразами:

$$E_{\theta,j} = \varphi_{emad}(A_j; \Psi_\theta); \quad E_{\vartheta,j} = \varphi_{emad}(A_j; \Psi_\vartheta),$$

буде досягатися декодування початкової послідовності без втрат інформації, а саме :

$$\varphi_{dmad}(E_{\theta,j}; \Psi_\theta) = \varphi_{dmad}(E_{\vartheta,j}; \Psi_\vartheta) = a_{i,j} \in A_j,$$
$$i = \overline{1, m}, \; j = \overline{1, n}.$$

Водночас потрібно зважати на те, що згідно з технологічними вимогами щодо цифризації повнокольорових відеозображень значення елементів кожної кольорової складової не може перевищувати величину 255. Тоді динамічний діапазон кожного елементу буде знаходитись у таких межах: $0 \le a_{i,j} \le 255$.

Звідки значення основи $\psi_i^{(\theta)}$ буде обмежено за максимальним значенням величиною 256, а саме:

$$a_{i,j} \le \psi_i^{(\theta)} - 1 \le 255, \; i = \overline{1, m}. \qquad (1)$$

Нерівності (1) описують умови для формування допустимої множини $\Omega(\Psi)$ систем Ψ_θ основ, що створюють умови для побудови взаємно однозначних мультіадичних систем.

Із виразу (1) отримується величина $_\Delta\psi_i^{(\theta)}$, яка визначає діапазон допустимої зміни значень

основ відносно елементів $a_{i,j}$ мультіадичного числа, тобто

$$_{\Delta}\psi_i^{(\theta)} \le 256 - \psi_i^{(\theta)}.$$

Загалом отримуємо таке співвідношення, що обмежує значення величин $_{\Delta}\psi_i^{(\theta)}$:

$$1 \le {}_{\Delta}\psi_i^{(\theta)} \le 256 - \psi_i^{(\theta)}.$$

Це дозволяє визначити об'єм $|\Omega(\Psi)|$ множини $\Omega(\Psi)$ допустимих систем основ відносно значень елементів $a_{i,j}$ МАД числа, а саме:

$$|\Omega(\Psi)| = \Theta = \prod_{i=1}^{m}\left({}_{\Delta}\psi_i^{(\theta)} - 1\right). \qquad (2)$$

Із аналізу формули (2) випливає те, що $|\Omega(\Psi)| > 1$, якщо $({}_{\Delta}\psi_i^{(\theta)} - 1 \ge 1)$. Остання умова виконується тоді, коли $a_{i,j} <<< 255$, тобто коли елементи мультіадичних чисел мають обмежений динамічний діапазон $\psi_i^{(\theta)}$. Отже, об'єм множини $\Omega(\Psi)$ залежить від кількості структурно-комбінаторної надмірності, яка породжується обмеженістю динамічних діапазонів елементів мультіадичних чисел.

Водночас, як показують практичні дослідження, формування мультіадичного базису в спектральному просторі з використанням дискретного косинусного перетворення (ДКП) забезпечує наявність закономірностей такого походження.

Звідки випливає, що мультіадичній системі, яка створюється в спектральному просторі трансформант ДКП, притаманний потенціал відносно формування множини допустимих модифікацій систем основ. У свою чергу, така характерна особливість створює можливість для побудови ***непрямих*** стеганографічних перетворень в мультіадичному базисі на основі модифікації структурних мета-ознак.

Висновки

1. Доведено можливість створення стеганографічних перетворень щодо непрямого вбудовування та вилучення прихованої інформації в мультіадичному базисі шляхом модифікації базової системи основ у межах допустимої множини.

2. Доведено наявність множини допустимих мультіадичних систем для однієї послідовності так, що досягається взаємно однозначне (без помилкове) пряме та зворотне кодове перетворення. Це дозволяє встановити умови модифікації системи основ мультіадичного простору, для яких забезпечується відновлення елементів початкової послідовності без втрат інформації, а саме:

– вибору системи основ, яка входить до допустимої множини варіантів побудови;

– формування відповідних кодових значень в допустимих системах основ.

3. Обґрунтовано, що мультіадичній системі, яка створюється в спектральному просторі трансформант ДКП, притаманний потенціал відносно формування множини допустимих модифікацій систем основ. У свою чергу, така характерна особливість створює можливість для побудови ***непрямих*** стеганографічних перетворень в мультіадичному базисі на основі модифікації структурних мета-ознак.

ЛІТЕРАТУРА

[1] JPEG Privacy & Security Abstract and Executive Summary. 2015. URL: https://jpeg.org/items/20150910_privacy_security_summary.html. (7.04.2021).

[2] Barannik, V. Technology for Protecting Video Information Resources in the Info-Communication Space [Text] / V. Barannik, S. Sidchenko, D. Barannik // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). 2020. P. 29–33. DOI: 10.1109/ATIT50783.2020.9349324.

[3] Barannik, V. Development of the method for encoding service data in cryptocompression image representation systems [Text] / V. Barannik, S. Sidchenko, N. Barannik, V. Barannik // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 3 № 9 (111). P. 112 – 124.

[4] Security key indicators assessment for modern cellular networks [Text] / Roman Odarchenko, Viktor Gnatyuk, Sergiy Gnatyuk, Anastasiia Abakumova // IEEE First International Conference on System Analysis & Intelligent Computing (SAIC). 2018, P 1–7. DOI**:** 10.1109/SAIC.2018.8516889

[5] Data Encryption Standard (DES) [Text]. Federal Information Processing Standards Publication 46-3, 1999. 26 p.

[6] ДСТУ ГОСТ 28147:2009. Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89) [Текст]. Введ. 2009-02-01. Київ : Держспоживстандарт України, 2008. 20 с.

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

[8] Barannik, V. Significant Microsegment Transformants Encoding Method to Increase the Availability of Video Information Resource [Text] / V. Barannik, Yu. Babenko, O. Kulitsa, V. Barannik, A. Khimenko, O. Matviichuk-Yudina // IEEE 2nd International Conference on Advanced Trends in Information

Theory (IEEE ATIT 2020). 2020. P. 52–56. DOI: 10.1109/ATIT50783.2020.9349256.

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

[10] Barannik, V. Methodological Fundamentals of Deciphering Coding of Aerophotography Segments on Special Equipment of Unmanned Complex [Text] / V. Barannik, S. Shulgin, A. Krasnorutsky, O. Slobodyanyuk, P. Gurzhii, N. Korolyova // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). 2020. P. 38–43. DOI: 10.1109/ATIT50783.2020.9349257.

[11] Li, F. Two-step providing of desired quality in lossy image compression by SPIHT [Текст] / F. Li, S. Krivenko, V. Lukin // Радіоелектронні і комп'ютерні системи. 2020. №. 2(94). С. 22-32. DOI: 10.32620/reks.2020.2.02.

[12] Еремеев, О. І. Комбінована метрика візуальної якості зображень дистанційного зондування на основі нейронної мережі [Текст] / О. І. Еремеев, В. В. Лукин, К. Окарма // Радіоелектронні і комп'ютерні системи. 2020. № 4 (96). С. 4-15. DOI: 10.32620/reks.2020.4.01.

[13] Barannik, V. A Model for Representing Significant Segments of a Video Image Based on Locally Positional Coding on a Structural Basis [Text] / V. Barannik, D. Jancarczyk, Yu. Babenko, O. Stepanko, J. Nikodem, S. Zawislak // IEEE 5nd International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IEEE IDAACS-SWS 2020). 2020. P. 1–5. DOI: 10.1109/IDAACS-SWS50031.2020.9297068.

[14] Barannik, V. Technology of Composite Code Forming in The Spatial-Spectral Description Significant Microsegments [Text] / V. Barannik, V. Himenko, Yu. Babenko, A. Hahanova, V. Fustii // IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (IEEE TCSET 2020). 2020. P. 703–706. DOI: 10.1109/TCSET49122.2020.235523.

[15] Wu, Yu. Sudoku Associated Two Dimensional Bijections for Image Scrambling [Text] / Yu. Wu, S. Agaian, J. Noonan // IEEE Transactions on multimedia. 2012. 30 p. URL: https://arxiv.org/abs/1207.5856v1. 7.04.2021.

[16] Barannik, V. A method to control bit rate while compressing predicted frames [Text] / V. Barannik, N. Kharchenko; O. Othman Shadi; A. Musienko // IEEE International Conference on The Experience of Designing and Application of CAD Systems in Microelectronics (IEEE CADSM 2015). 2015. P. 36–38. DOI: 10.1109/CADSM.2015.7230789.

[17] Coding tangible component of transforms to provide accessibility and integrity of video data / Vladimir Barannik, Anna Hahanova, Vladimir Krivonos // International Symposium on East-West Design & Test Symposium (EWDTS). 2013. P. 1–5. DOI**:** 10.1109/EWDTS.2013.6673179.

[18] A fast image encryption algorithm based on chaotic map and lookup table [Text] / P. Cheng, H. Yang, P. Wei, W. Zhang // Nonlinear Dynamics. 2015. Vol. 79, Iss. 3. P. 2121–2131. DOI: 10.1007/s11071-014-1798-y.

[19] A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2 [Text] / R. Guesmi, M.A.B. Farah, A. Kachouri, M. Samet // Nonlinear Dynamics. 2016. Vol. 83, Iss. 3. P. 1123–1136. DOI: 10.1007/s11071-015-2392-7.

[20] Barannik, V. Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones [Text] / V. Barannik, V. Barannik // 15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020). 2020. - P. 775–780. DOI: 10.1109/TCSET49122.2020.235540.

[21] Kurihara, K. An encryption-then-compression system for JPEG XR standard [Text] / K. Kurihara, O. Watanabe, H. Kiya // IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). 2016. P. 1–5. DOI: 10.1109/BMSB.2016.7521997.

[22] Barannik, V. Description of the OFDM symbol with the help of mathematical laws. Analysis of technologies that were used in this case [Text] / V. Barannik, M. Lytvinenko, D. Okladnoy, O. Suprun // IEEE 2nd International Conference on Advanced Information and Communication Technologies (IEEE AICT 2017). 2017. P. 183–187. DOI: 10.1109/AIACT.2017.8020095.

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

[24] Barannik, V. The method of crypto-semantic presentation of images based on the floating scheme in the basis of the upper boundaries [Text] / V. Barannik, D. Barannik, V. Fustii, M. Parkhomenko // IEEE 3rd International Conference on Advanced Information and Communications Technologies (IEEE AICT 2019). 2019. P. 415–418. DOI: 10.1109/AIACT.2019.8847820.

[25] 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.

[26] Barannik, V. V. Structural slotting with uniform redistribution for enhancing trustworthiness of information streams [Text] / V. V. Barannik, Yu. N. Ryabukha, S. A. Podlesnyi // Telecommunications and Radio Engineering.

2017. Vol. 76 No. 7. P. 607-615. DOI: 10.1615/TelecomRadEng.v76.i7.40.

[27] Barannik, V. The method of increasing accessibility of the dynamic video information resource / V. Barannik, S. Shulgin // IEEE 13th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (IEEE TCSET 2016). 2016. P. 621–623. DOI: 10.1109/TCSET.2016.7452133.

[28] Wong, K. DCT based scalable scrambling method with reversible data hiding functionality [Text] / K. Wong, K. Tanaka // 4th International Symposium on Communications, Control and Signal Processing (ISCCSP). 2010. P. 1–4. DOI: 10.1109/ISCCSP.2010.5463307.

[29] The issue of timely delivery of video traffic with controlled loss of quality [Text] / V. Barannik, N. Kharchenko, V. Tverdokhleb, O. Kulitsa // 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). - 2016, P. 902–904. DOI: 10.1109/TCSET.2016.7452220.

[30] Method coding efficiency segments for information technology processing video [Text] / V. Barannik, D. Tarasenko // 4th International Scientific-Practical Conference on Problems of Infocommunications. Science and Technology (PIC S&T). 2017. P. 551–555. DOI: 10.1109/INFOCOMMST.2017.8246460.

[31] JPEG image scrambling without expansion in bitstream size / K. Minemura, Z. Moayed, K. Wong, X. Qi, K. Tanaka // 19 th IEEE International Conference on Image Processing. 2012. P. 261–264. DOI: 10.1109/ICIP.2012.6466845.

[32] The technology of the video stream intensity controlling based on the bit-planes recombination / V. Barannik, M. Karpinski, V. Tverdokhleb, D. Barannik, V. Himenko, M. Aleksander // IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS`2018). - 2018. P. 25–28. DOI: 10.1109/IDAACS-SWS.2018.8525560.

[33] Ji, Sh. Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator [Text] / Sh. Ji, X. Tong, M. Zhan. 2012. URL: https://arxiv.org/abs/1208.0999. 7.04.2021.

[34] Barannik Valeriy. Fast Coding of Irregular Binary Binomial Numbers with a Set Number of Units Series [Text] // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). 2020. P. 72–76. DOI: 10.1109/ATIT50783.2020.9349356.

[35] Barannik, D. Stegano-Compression Coding in a Non-Equalible Positional Base // IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). 2020. P. 83–86. DOI: 10.1109/ATIT50783.2020.9349328.

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

[37] Barannik, V. The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents [Text] / V. Barannik, T. Belikova, P. Gurzhii // IEEE International Conference on Advanced Trends in Information Theory (ATIT`2019). 2019. - P. 656–661. DOI: 10.1109/ATIT49449.2019.9030432.

[38] Barannik, V. V. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems [Text] / V. V. Barannik, Yu. N. Ryabukha, O. S. Kulitsa // Telecommunications and Radio Engineering. 2017. - Vol. 76 No. 9. P. 785–797. DOI: 10.1615/TelecomRadEng.v76.i9.40.

[39] Development Second and Third Phase of the Selective Frame Processing Method [Text] / V. Barannik, V. Barannik, D. Havrylov, A. Sorokun // 3rd International Conference on Advanced Information and Communications Technologies (AICT`2019). 2019. P. 54–57. DOI: 10.1109/AIACT.2019.8847897.

[40] Methodological basis for determining the energy significance of the structural unit of a video frame based on the estimation of low-frequency components of the matrices of the DCT blocks of the luminance component [Text] / V. Barannik, D. Komolov, A. Musienko, R. Tarnopolov // 13th International Conference on Modern Problems of Radio Engineering on Telecommunications and Computer Science (TCSET). 2016. P. 739–741. DOI: 10.1109/TCSET.2016.7452168.

[41] Komolov, D. Selective Method For Hiding Of Video Information Resource In Telecommunication Systems Based On Encryption Of Energy-Significant Blocks Of Reference I-Frame [Text] / D. Komolov, D. Zhurbynskyy, O. Kulitsa // 1st International Conference on Advanced Information and Communication Technologies (AICT'2015). - 2015. P. 80–83.

[42] Wu, Y. NPCR and UACI Randomness Tests for Image Encryption / Y. Wu, J. P. Noonan, S. Agaian // Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT). 2011. Vol. 2. P. 31–38. DOI: 10.4236/jss.2015.33005.

[43] 43.Бараннік, В. В., Сідченко, С. О., Баран нік, Н. В., Хіменко, А. М. (2021). Метод маскувального ущільнення службових даних в системах компресії відеозображень. Радіо-електронні і комп'ютерні системи, 2, 51–63. DOI: https://doi.org/10.32620/reks.2021.2.05.

Бараннік Н. В.

МЕТОДОЛОГІЯ СТВОРЕННЯ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ НЕПРЯМОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ МУЛЬТІАДИЧНИХ ПЕРЕТВОРЕНЬ

Показано, що актуальним напрямком підвищення безпеки інформаційних ресурсів при передачі в інфокомунікаційних системах є використання методів стеганографічного вбудовування інформації в відеозображення. Ефективність таких методів значно підвищується у разі використання в комплексі методів приховування, які засновані на принципах безпосереднього та непрямого вбудовування повідомлень. В той же час існуючи методи стеганографії використовують в процесі вбудовування інформації в основному лише закономірності, що породжуються особливостями візуального сприйняття відеозображень. Отже обґрунтовано, що науково-прикладна задача, яка полягає в підвищені щільності вбудованих в відеоконтейнер повідомлень з заданим рівнем їх достовірності, є актуальною. В основі вирішення цієї задачі знаходиться вирішення протиріччя, яке стосується того, що підвищення щільності вбудованих даних призводить до зниження бітової швидкості відеоконтейнеру, стійкості до стеганоаналізу, достовірності спеціальної інформації та відеоконтейнеру. Тому метою дослідження є розробка методології стеганографічного вбудовування інформації з врахуванням закономірностей відеоконтейнеру, які породжені його структурними та структурно-статистичними особливостями. Вирішення сформульованої задачі в області застосування стеганографічних перетворень пропонується реалізовувати з використанням методів непрямого вбудовування біту повідомлення, що приховується, деяку умову або функціональну залежність. Для побудови стеганографічної системи в умовах виконання необхідних вимог пропонується використовувати мультіадичні перетворення. В цьому випадку досягається наступне. Доведено можливість створення стеганографічних перетворень щодо непрямого вбудовування та вилучення прихованої інформації в мультіадичному базисі шляхом модифікації базової системи основ у межах допустимої множини. Доведено наявність множини допустимих мультіадичних систем для однієї послідовності так, що досягається взаємно однозначне пряме та зворотне кодове перетворення. Обґрунтовано, що мультіадичній системі, яка створюється в спектральному просторі трансформант ДКП, притаманний потенціал відносно формування множини допустимих модифікацій систем основ. У свою чергу, така характерна особливість створює можливість для побудови непрямих стеганографічних перетворень в мультіадичному базисі на основі модифікації структурних мета-ознак.

Ключові слова: стеганографічні перетворення, відеоконтейнер, стиснення відеозображень, непряме вбудовування, щільність вбудовування.

Barannik N.

METHODOLOGY OF INDIRECT INFORMATION HIDDENING STEGANOGRAPHIC SYSTEM CREATION ON THE MULTIADIC TRANSFORMATIONS BASIS

It is shown that the current direction of information resources security increasing during transmission through infocommunication systems is using the methods of steganographic embedding information in video images. The effectiveness of such methods is significantly increased when using a set of concealment methods, which are based on the principles of messages direct and indirect embedding. At the same time, the existing steganographic methods use in the information embedding process mainly only patterns generated by the peculiarities of the video images visual perception. Therefore, it is substantiated that the scientific and applied task, which consists in increasing the density of messages embedded in the video container with a given level of their reliability, is relevant. The solution to this problem is based on the elimination the contradiction that the increase in the embedded data density leads to a decrease in the video container bit rate, resistance to steganoanalysis, the special information and the video container reliability. Therefore, the aim of the research is developing a methodology for steganographic information embedding, taking into account the video container features, which are generated by its structural and structural-statistical features. The solution of the formulated problem in the field of steganographic transformations application is offered to be realized with using a bit of the hidden message some condition or functional dependence indirect embedding methods. To construct a steganographic system in terms of compliance with the necessary requirements are encouraged to use multi-stage conversion. In this case, the following is achieved. The possibility of creating steganographic transformations of indirect embedding and retrieval of hidden information in the multiadic basis by modifying the basic system of bases within the allowable set is proved. The existence of an admissible multiadic systems set for one sequence is proved so that mutually unambiguous direct and inverse code transformation is achieved. It is substantiated that the multiadic system, which is created in the DCT transformant spectral space, has the potential to form a set of the base systems permissible modifications. In turn, this characteristic feature creates an opportunity to construct indirect steganographic transformations in the multiadic basis, which based on the structural meta-features modification.

Keywords: steganographic transformations, video container, video image compression, indirect embedding, embedding density.

Стаття надійшла до редакції 01.09.2021 р.
Прийнято до друку 04.10.2021 р.