УДК 004.932.056.55 **doi: 10.32620/reks.2021.4.10**

В. В. БАРАННІК[1], Н. В. БАРАННІК[2], О. О. ІГНАТЬЄВ[2], В. В. ХІМЕНКО[2]

[1] ***Харківський національний університет імені В. Н. Каразіна, Україна***
[2] ***Харківський національний університет радіоелектроніки, Україна***

МЕТОД НЕПРЯМОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ПРОЦЕСІ СТИСНЕННЯ ВІДЕОЗОБРАЖЕНЬ

Обґрунтовується, те, що для забезпечення захисту спеціального інформаційного ресурсу в умовах його оперативної доставки, необхідно використовувати стеганографічні системи. В цьому випадку стеганографічні технології є складовою комплексних систем захисту інформації. В той же час для стеганографічних систем існує протиріччя між щільністю вбудованих даних та рівнем інформаційного ущільнення відеоконтейнеру (рівень зменшення бітового об'єму компактно представленого відеозображення відносно бітового об'єму початкового відеозображення). Це призводе до того, що в умовах потрібної якості (достовірності) цифрової відеоінформації,рівень бітової швидкості прихованого каналу є недостатнім. Отже науково-прикладна проблематика, що стосується необхідності підвищення цілісності (рівень відповідності прихованої інформації до її вбудовування у відеоконтейнер та після її вилучення) та бітової швидкості прихованого каналу передачі спеціальної інформації, є актуальною. Вирішення сформульованої задачі в області застосування стеганографічних перетворень можливо реалізовувати на основі застосування двох різних підходів. Перший підхід базується на методах безпосереднього вбудовування повідомлень. Але такий підхід характеризується внесенням спотворень до відеозображень, які використовуються в якості контейнеру. Тому трапляються зміни структурних та статистичних закономірностей в синтаксичному описі відеоконтейнеру. Це зменшує потенціальні можливості відносно ущільнення відеоконтейнерів. Другий підхід щодо створення методів стеганографічних перетворень базується на приховуванні інформації з використанням методів непрямого вбудовування. Тут в процесі вбудовування інформації використовується функціональна залежність між елементами відеоконтейнеру та елементами вбудованого повідомлення. Встановлення конкретної залежності між елементами в відеоконтейнері відповідає вбудовуванню елементу зі значенням «0» або «1». Однак для існуючих методів непрямого стеганографічного перетворення характерний недолік, який полягає у недостатньому значенні щільності вбудованих даних. Для усунення недоліків пропонується розробити підхід, який дозволить використовувати для приховування не тільки психовізуальну, але й структурну надмірність відеоконтейнеру. Тому мета досліджень статті полягає у розробці методу непрямого приховування інформації в процесі стиснення відеоконтейнеру для підвищення бітової швидкості каналу прихованих повідомлень. В процесі досліджень побудована стеганографічна мультіадична система, що дозволяє вбудовувати елементи прихованого повідомлення без втрат інформації на основі непрямого підходу шляхом модифікації активних основ мультіадичного базису з врахуванням їх невизначеності. Для відбору трансформант (масивів даних) в якості контейнерів для вбудовування інформації враховується вимога щодо існування базової системи зі всіма активними основами. Кількість вбудованих біт прихованого повідомлення дорівнює кількості активних основ в базовій системі мультіадичного простору. В результаті проведених експериментів отримано наступні результати : в процесі вбудовування повідомлень на базі створеного методу не вносяться спотворення в відеоконтейнер; для створеного методу досягається додаткове підвищення бітової швидкості прихованого каналу в середньому 5 … 7 разів.

Ключові слова: *стиснення відеозображень; конфіденційність інформації; стеганографічні перетворення; мультіадичний базис; модифікована система основ; кодування; компресія; відеозображення; найменш значущий біт, відносна заміна.*

Вступ

В процесі управління об'єктами критичної інфраструктури (ОКІФ) особливо в умовах ведення гібридних та інформаційних воєн актуальним є забезпечення своєчасної доставки телекомунікаційними мережами спеціальних інформаційних ресурсів з заданим рівнем повноти, цілісності та конфіденційності. В загальному випадку спеціальними інформаційними ресурсами можуть бути текстові документи; аудіо дані, статичні та динамічні відеоінформаційні ресурси [1, 2].

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Відповідно повнота цифрового відеозображення визначається як кількість пікселів, які застосовуються для представлення об'єктів на відеокадрі. Тобто необхідна повнота відеозображення повинна відповідати потрібному класу вирішення задач аналізу та ідентифікації об'єктів на відеокадрі. Повнота відеозображень визначається як розмір відеокадру в пікселях.

Достовірність цифрових відеозображень визначається показниками, що дозволяють оцінити якість відновлених цифрових відеозображень на приймальній стороні. Або у випадку їх стеганографічного перетворення – якість відеозображення (відеоконтейнеру) у разі вбудовування прихованих повідомлень. Отже кількісно рівень достовірності відеозображень оцінюється як рівень відхилення відновлених на приймальній стороні відеозображень відносно початкових. Одним з важливих кількісних показників, що визначають достовірність відновлених на приймальній стороні цифрових відеозображень є показник пікового відношення сигнал/шум (ПВСШ або PSNR). Цей показник визначає оцінку нормованого середньоквадратичного відхилення відновленого відеозображення відносно початкового в дБ.

Для забезпечення захисту спеціального інформаційного ресурсу в умовах його оперативної доставки, необхідно використовувати стеганографічні системи. При цьому потрібно враховувати можливість застосування розвиненої системи надання відеоінформаційних сервісів реального час. Тому стеганографічні технології, які використовують відеозображення в якості контейнерів, є важливою складовою комплексних систем захисту інформації [3, 5]. Це дозволяє :

- уникнути нормативно-правових обмежень та недоліків, які пов'язані зі збільшенням часу обробки, що можуть виникати в процесі додаткового застосування криптографічних перетворень [6, 8];

- створити умови для локалізації дисбалансу між своєчасністю доведення скритої інформації (спеціальної інформації) та показником її достовірності [9 – 11].

В той же час відеоконтейнер сам по собі може бути важливою інформацією, що використовується для прийняття рішень. Тоді для існуючих методів стеганографічних перетворень можуть виникати недоліки, а саме :

1) існує протиріччя між щільністю вбудованих даних та рівнем інформаційного ущільнення відеоконтейнеру (рівень зменшення бітового об'єму компактно представленого відеозображення відносно бітового об'єму початкового відеозображення) [12, 13]. Тут під щільністю вбудованих даних розуміється середня кількість біт вбудованого повідомлення, що приходиться на один біт початкового контейнеру (відеозображення);

2) для заданого рівня достовірності (якості цифрового відеозображення) відеоконтейнеру (величина ПВСШ сягає 40 дБ) у випадку використання 30 кадрів формату FullHD створюються умови для приховування повідомлень бітовим об'ємом лише 1,5 Мбіт. Це дозволяє приховувати відеозображення форматом CIF та SD. Але ж такий формат відеозображень, які приховуються, не задовольняє вимогам відносно повноти відеоінформації в системах управління ОКІФ. Отже ***науково-прикладна проблематика***, що стосується необхідності підвищенні цілісності *(рівень відповідності прихованої інформації до її вбудовування у відеоконтейнер та після її вилучення)* та бітової швидкості прихованого каналу передачі спеціальної інформації, ***є актуальною***.

Для оцінки цілісності прихованої інформації у цифровий відеоконтейнер найчастіше використовується такий показник, як ймовірність безпомилкового вилучення вбудованих даних авторизованим користувачем.

Метою дослідження є розробка методу непрямого вбудовування інформації в процесі стиснення відеоконтейнеру для підвищення бітової швидкості каналу прихованих повідомлень.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз підходів відносно забезпечення підвищення бітової швидкості прихованого каналу;

– розробити метод непрямого приховування повідомлень у відеоконтейнер без внесення спотворень на основі додаткового врахування структурних закономірностей ;

– провести експериментальну оцінку ефективності приховування повідомлень.

Аналіз підходів для забезпечення підвищення бітової швидкості прихованого каналу

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 до відеоконтейнеру [13, 14].

Вирішення сформульованої задачі в області застосування стеганографічних перетворень можливо реалізовувати на основі використання двох різних класів методів, а саме:

- класу методів, які забезпечують приховування повідомлень на основі безпосереднього вбудовування біту повідомлень [14, 15];

- класу методів, які використовують для вбудовування біту деяку умову або функціональну залежність між елементами відеоконтейнеру та бітами прихованого повідомлення [16 - 18].

Безпосереднє вбудовування здійснюється шляхом модифікації найменш значимого біту компоненти проміжного синтаксичного опису контейнеру в процесі його компактного представлення [19, 20]. Але для такого варіанту характерні недоліки :

- внесення спотворень в відеоінформаційний ресурс, який використовуються в якості контейнеру [21 - 23];

- те, що таке приховування інформації супроводжується впливом на процес стиснення відеоресурсу (відеозображення-контейнера). Вбудовування інформації витрачає деяку кількість психовізуальної надмірності, яка могла б використовуватись в процесі стиснення [24, 25]; модифікація бітів компонент поточного синтаксичного опису відеоконтейнеру призводе до зміни або руйнування структурних та статистичні закономірностей в послідовності елементів відеоконтейнеру [26, 27].

Навпаки непряме вбудовування проводиться в масив даних. Для вбудовування використовується деяка умова або функціональна залежність [28]. Встановлення конкретної залежності між елементами відеоконтейнеру відповідає вбудовуванню біту зі значенням «0» або «1».

Але в свою чергу для ***існуючих*** методів непрямого стеганографічного перетворення характерний недолік, який полягає у недостатньому значенні щільності вбудованих даних щодо сучасних вимог в системах управління ОКІФ [29, 30].

Для усунення недоліків непрямого стеганографічного вбудовування пропонується розробити підхід, який дозволить використовувати для приховування не тільки психовізуальну, але й структурну надмірність відеоконтейнеру. Такий підхід пропонується реалізовувати в процесі стиснення відеозображень на основі мультіадичного кодування [31, 32]. В цьому випадку створюються умови для виключення додаткових спотворень відеоконтейнеру.

Розробка непрямого методу приховування повідомлень в процесі стиснення відеозображень

Сформулюємо визначення стеганографічної мультіадичної системи.

Стеганографічна МАС – мультіадична система (МАС) в умовах *допустимих* модифікацій в просторі її структурних мета-ознак, для яких забезпечується вбудовування прихованої інформації в умовах підвищення стійкості щодо її несанкціонованого вилучення та/або можливості встановлення факту щодо її вбудовування.

В основі створення таких стеганографічних перетворень ***пропонується*** закладати властивість мультіадичних систем. Така властивість кроїться у можливості побудови множини допустимих модифікацій системи основ в умовах врахування структурно-комбінаторної надмірності. При цьому досягаються взаємно однозначні перетворення мультіадичних послідовностей [34 - 36].

Звідки стеганографічна МАС це модифікована МАС в допустимій множині варіантів систем основ.

Тоді якщо базова МАС описується функціоналом $F_{mads}(A_j; E_j; \Psi; \delta_j = 0)$, то варіант її модифікації з допустимою множиною $\Omega(\Psi)$ для стеганографічного вбудовування інформації - як $F_{mads}(A_j; E'_j; \Psi'; S; \delta_j = 0; \delta(s)_j = 0)$. Тут Ψ' - модифікована система основ; E'_j - кодове значення, яке знаходиться для початкової послідовності A_j; S - повідомлення, яке потрібно приховати шляхом стеганографічного вбудовування в контейнер; $\delta(s)_j$ - показник оцінки втрат інформації прихованого повідомлення після його вилучення з контейнеру.

Модифікація системи основ саме й визначає перетворення простору структурних мета-ознак в мультіадичному базисі для приховання інформації [37, 38]. Для модифікації можна використовувати тільки ті основи ψ_i, базові значення яких задовольняють вимогам

$$a_{i,j} \le \psi_i - 1 \le 255. \qquad (1),$$

В подальшому базові (опорні) основи, які задовольняють нерівності (1) будемо називати ***активними***.

Згідно виразу

$$1 \le {}_{\Delta}\psi_i^{(\theta)} \le 256 - \psi_i^{(\theta)}. \qquad (2)$$

динамічний діапазон величин ${}_{\Delta}\psi_i$ можливих модифікацій відносно значень базових основ ψ_i дорівнює $1 \le {}_{\Delta}\psi_i \le 256 - \psi_i$. Це дозволяє обирати модифіковане значення ψ'_i базової основи ψ_i в деякому діапазоні $[\psi_i + 1; 256]$, а саме :

$$\psi_i + 1 \le \psi'_i \le 256. \qquad (3)$$

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Отже наявність діапазону $[\psi_i + 1; 256]$ для вибору значень модифікованих основ ψ'_i визначає таку властивість активних базових основ ψ_i, як ***невизначеність***. Саме така невизначеність й використовується для прихованого вбудовування інформації в просторі структурних мета-ознак мультіадичної системи. Звідки невизначеність *активних* базових основ є *необхідною умовою* для модифікації їх значень, а отже й для реалізації стеганографічних перетворень. Схематично область невизначеності базової системи основ наведено на рис. 1. Навпаки, якщо основа базової системи не активна, то вона не використовується для приховування інформації в стеганографічних системах. Тому заздалегідь необхідно визначитись щодо кількості та позицій активних основ базової системи МАС. В іншому випадку не будуть створені умови для взаємно однозначного стеганографічного перетворення, тобто забезпечення ймовірності вилучення інформації на рівні одиниці (без втрат прихованої інформації). Для вирішення такої ситуації *пропонується* використовувати для стеганографічного перетворення тільки такі базові системи Ψ основ, для яких всі основи є активними.

Тобто

$$\Psi: a_{i,j} \le \psi_i - 1 \le 255 \quad \forall i = \overline{1, m}. \qquad (4)$$

Отже для реалізації стеганографічних перетворень потрібно обирати таку мультіадичну систему та прив'язану до неї трансформанту A (масив даних), для якої базова система основ задовольняє вимогам (4) відносно активності всіх основ.

Тоді для прихованого вбудовування повідомлення S шляхом модифікації активних основ базової системи з використанням її невизначеності *пропонується* наступне *правило* :

- якщо значення γ -го біту двійкового представлення прихованого повідомлення S дорівнює 0, $[s_\gamma]_2 = 0$, то значення поточної основи ψ_i базової системи Ψ залишається незмінним. Відповідно модифіковане значення основи визначається як : якщо $[s_\gamma]_2 = 0$, то $\psi'_i = \psi_i$;

- якщо величина $[s_\gamma]_2$ дорівнює 1, $[s_\gamma]_2 = 1$, то значення базової основи модифікується, тобто : якщо $[s_\gamma]_2 = 1$, то $\psi'_i = \psi_i + {}_\Delta\psi_i$.

Узагальнюючі наведені вирази отримуємо наступне співвідношення для модифікації значень базових основ ψ_i в залежності від двійкового елементу $[s_\gamma]_2$ прихованого повідомлення S :

$$\psi'_i = \psi_i + {}_\Delta\psi_i \cdot [s_\gamma]_2, \; i = \overline{1, m}. \qquad (5)$$

Тут $[s_\gamma]_2$ - значення відповідно γ -го біту двійкового представлення прихованого повідомлення S :

$$[S]_2 = ([s_1]_2; \ldots; [s_\gamma]_2; \ldots; [s_\ell]_2),$$

де ℓ - кількість біт в двійковому представлені $[S]_2$ прихованого повідомлення S

Співвідношення (5) описує оператор $\varphi_{ise}(\Psi; S)$ непрямого стеганографічного перетворення (непрямого стеганографічного кодування) шляхом модифікації активної базової системи основ, $\Psi' = \varphi_{ise}(\Psi; S)$.

В цьому випадку оператор кодування $\varphi'_{emad}(A_j; \Psi')$ в модифікованому базисі Ψ' основ мультіадичного простору буде мати такий вигляд :

$$\varphi'_{emad}(A_j; \Psi') = \varphi_{emad}(A_j; \varphi_{ise}(\Psi; S)).$$

Відповідно кодове значення E'_j для послідовності A_j в модифікованому мультіадичному базисі Ψ' основ з врахуванням непрямого вбудовування

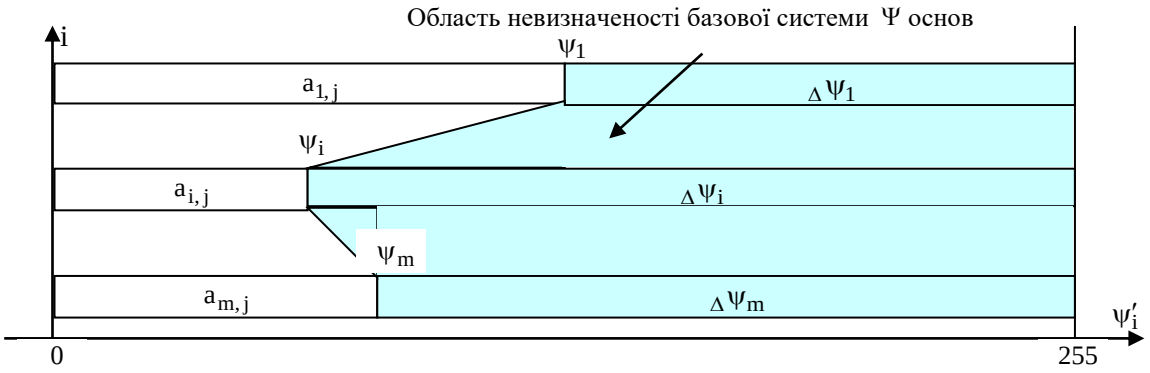

Рис. 1. Схема утворення області невизначеності базової системи основ

елементу $[s_\gamma]_2$ знаходиться за допомогою наступного виразу [38 - 40] :

$$E'_j = \sum_{i=1}^{m} a_{i,j} \prod_{\xi=i+1}^{m} (\psi_\xi + {}_\Delta\psi_\xi \cdot [s_\gamma]_2). \quad (6)$$

Дане співвідношення дозволяє організовувати одночасне кодування мультіадичної послідовності A_j та вбудовування прихованої інформації S в модифікованому базисі Ψ' основ.

Для програмної реалізації такого процесу більш ефективнішим з позиції скорочення часу на обробку є використання рекурентного виразу для співвідношення (6). Тоді кодове значення $E'^{(i)}_j$ на i-му кроці процесу кодування з приховуванням інформації через кодове значення $E'^{(i-1)}_j$ для попереднього $(i-1)$-го кроку знаходиться за допомогою формули [40 - 42] :

$$E'^{(i)}_j = (E'^{(i-1)}_j) \cdot \psi'_i + a_{i,j}. \quad (7)$$

Структурно-функціональна схема мультіадичного кодування з непрямим вбудовуванням прихованої інформації в модифікованій системі основ наведено на рис. 2.

Оскільки розмір системи основ мультіадичної системи обмежено m основами, тобто $|\Psi'| = m$, то кількість двійкових елементів, що вбудовуються буде дорівнювати m біт. Звідки в одній мультіадичний системі на основі непрямого вбудовування в модифіковану систему основ можна приховати двійкове повідомлення $[S^{(m)}]_2$ довжиною m біт :

$$[S^{(m)}]_2 = ([s_1]_2;...;[s_\gamma]_2;...;[s_m]_2).$$

У разі, якщо $\ell > m$, то для вбудовування елементів, які залишилися, потрібно використовувати іншу МАС, тобто іншу трансформанту (масив даних).

Порівняльна оцінка ефективності різних методів стеганографічних перетворень

Розглянемо оцінку ефективності створеного та існуючих методів непрямого стеганографічного приховування інформації. Для порівняльної оцінки проводиться моделювання у вигляді натурного експерименту. Для цього розроблений програмний комплекс, який виконується на операційних системах сімейства Microsoft. Додаткових бібліотек сторонніх розробників для коректної роботи програмного комплексу не вимагається. Додаткових вимог

Рис. 2. Структурно-функціональна схема кодування в стеганографічний мультіадичний системі непрямого вбудовування інформації

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

до персональної обчислювальної техніки не висувається. Для порівняння використовується модифікований метод Coch and Zhao [14, 15]. Він є найбільш поширеним представником методів відносної заміни величин дискретного косинусного перетворення. Тут приховування інформації організується в спектральному просторі. Для чого початкові фрагменти відеозображень трансформуються за допомогою дискретного косинусного перетворення (ДКП). Метод забезпечує непряме приховування інформації з щільністю η_{cbi} вбудованих даних, $\eta_{cbi} = 2 \cdot 10^{-3}$ відносно бітового об'єму початкових відеозображень [16, 17].

Для оцінки бітової швидкості прихованого в відеоінформаційному потоці каналу передачі вбудованих повідомлень з використанням телекомунікаційних мереж розглянемо :

1) телекомунікаційні технології передачі даних Wi-Fi; LTE-A, відповідно швидкість передачі даних в мережі 100 Мбіт/с – 1 Гбіт/с;

2) для ущільнення відеоінформаційного ресурсу використовується інформаційна платформа сімейства JPEG [10, 14, 22, 23, 25];

3) в якості контейнеру обріється відеозображення. Розмір формату відеоконтейнерів відповідає форматам FullHD, 4K та 8K. Частота кадрів від 15 до 30 кадрів/с. При цьому використовувалися три групи заздалегідь класифікованих відеозображень залежно від ступеня насиченості дрібними деталями, а саме слабонасичені, середньонасичені та сильнонасичені. Відеозображення бралися із стандартизованих баз, які використовуються для тестування методів кодування і обробки відеоінформації. У експериментах використовувалося по 100 зображень кожного з трьох класів.

4) в залежності від структурно-семантичної інформативності відеоконтейнерів потрібний рівень ПВСШ приймається на рівні 20 … 40 дБ.

5) корекція параметрів процесу стиснення здійснюється таким чином, щоб для варіанту вбудовування повідомлень забезпечити умову, коли локалізується зниження величини k_{id} інформаційного ущільнення, тобто $k'_{id} \approx k_{id}$ та $_{\Delta}k \to 1$ (рис. 3);

6) часові затримки на процеси вбудовування та вилучення повідомлення не повинні перевищувати лінійну складність;

7) для вбудовування використовувались повідомлення, що представляють собою відеозображення, які насичені об'єктами різного рівня роздрібної здатності.

Оцінка величини $_{\Delta}U(K; h''; k_{id})_{real}$ бітової швидкості прихованого каналу для різних методів наведена у вигляді діаграм на рис. 4. Тут в якості відеоконтейнеру використовувались середньо насичені за своїм змістом відеозображення. В залежності від величин ПВСШ реконструйованого відеозображення, інформаційного ущільнення, та щільності η_{cbi} вбудованих даних величина $_{\Delta}U(K; h''; k_{id})_{real}$ визначається наступною формулою. У разі зміни стандартних параметрів процесу стиснення для досягнення умови $k'_{id} \approx k_{id}$ відносно рівня інформаційного ущільнення відеозображень :

$$_{\Delta}U(K; h''; k_{id})_{real} = \eta_{cbi} \cdot k_{id} \cdot U_c = \eta'_{cbi} \cdot U_c \,.$$
$$\text{для} \quad h'' \le h' \,.$$

Тут h - пікове відношення сигнал-шум для відеозображення з вбудованою інформацією, яке реконструйоване після стиснення на приймальній стороні неавторизованим користувачем; η_{cbi} - відносна ємкість стеганографічної системи (СГС), що визначається як щільність вбудованої інформації в контейнер; h_{nes} - необхідна величина ПВСШ, що визначає достатній рівень достовірності відеозображення після його реконструкції; δ_0 - потрібний рівень повноти відеозображення, який визначається величиною роздрібної здатності; U_c - швидкість передачі даних з використанням бездротових ТКС.

По результатам аналізу діаграм на рис. 4 можна заключити наступне :

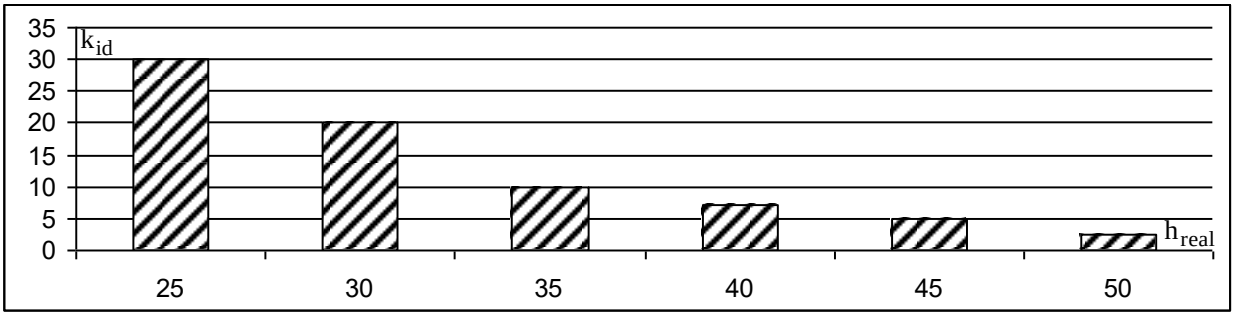

Рис. 3. Діаграма залежності значень коефіцієнту k_{id} від рівня h_{real} ПВСШ з вилученням механізмів компенсації руху міжкадрових об'єктів

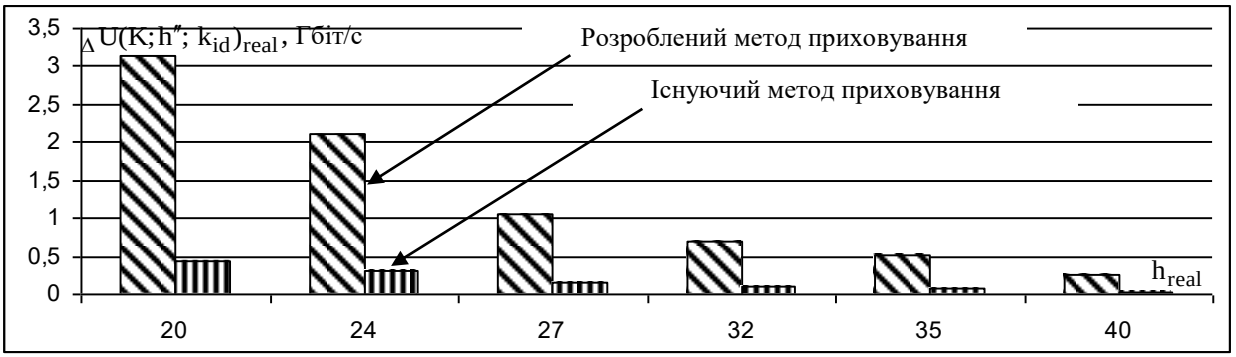

Рис. 4. Діаграма порівняння величини $_{\Delta}U(K;h'';k_{id})_{real}$ від h_{real} для різних методів непрямого вбудовування повідомлень в умовах $k'_{id} \approx k_{id}$ у разі використання телекомунікаційних технологій з продуктивністю 1 Гбіт/с

- рівень щільності вбудованих повідомлень для створеного методу перевищує в 9 разів відповідний рівень для існуючих методів непрямого приховування інформації;

- в процесі вбудовування повідомлень на базі створеного методу не вносяться спотворення у відеоконтейнер. Отже в цьому випадку бітова швидкість прихованого каналу визначається об'ємом прихованих даних, рівнем інформаційного ущільнення відеоконтейнеру, швидкістю передачі даних в телекомунікаційній мережі;

- з врахуванням додаткових затрат часу на приховування інформації для створеного методу досягається додаткове підвищення бітової швидкості прихованого каналу в середньому 5 … 7 разів.

Оцінки величин інформаційного ущільнення k_{id} та щільності η_{cbi} вбудованих даних представлялись як усереднені дані по кожному класу відеоконтейнерів. Розмір вибірки складає 100 відеозображень. При цьому довірчий інтервал складає ±3 %. Для оцінки довірчого інтервалу використовувалося правило трьох сигм (3-sigma rule). Достовірність отриманих результатів підтверджується тим, що :

- в процесі стеганографічних перетворень не вносяться додаткові спотворення у відеоконтейнер;

- забезпечується вилучення прихованих повідомлень без втрат інформації. Тобто величина ймовірності безпомилкового вилучення вбудованих даних авторизованим користувачем дорівнює одиниці.

Висновки

По викладеному матеріалу можна заключити :

1. Побудована стеганографічна мультіадична система, що дозволяє вбудовувати елементи прихованого повідомлення без втрат інформації на основі непрямого підходу шляхом модифікації активних основ мультіадичного базису з врахуванням їх невизначеності. Для відбору трансформант (масивів даних) в якості контейнерів для вбудовування інформації враховується вимога щодо існування базової системи зі всіма активними основами. Кількість вбудованих біт прихованого повідомлення дорівнює кількості активних основ в базовий системі мультіадичного простору.

Отже, наукова новизна полягає у тому, що вперше створено стеганографічну мультіадичну систему на основі непрямого приховування інформації. Основні її відмінності:

- вбудовування інформації здійснюється в процесі стиснення даних на основі мультіадичного кодування;

- непряме приховання інформації здійснюється в мультіадичному просторі структурних мета-ознак базової системи з активними основами;

- модифікація основ здійснюється з врахуванням структурно-комбінаторної надмірності, що породжена закономірностями відносно обмеженості динамічних діапазонів елементів мультіадичних чисел.

Це дозволяє створити умови для одночасного стійкого відносно стегано-атак приховування інформації та зменшення бітового об'єму відеоданих.

2. Розроблений метод забезпечує:

- те, що рівень щільності вбудованих повідомлень перевищує в 9 разів відповідний рівень для існуючих методів непрямого приховування інформації;

- виключення спотворень у відеоконтейнер в процесі вбудовування повідомлень. Отже в цьому випадку бітова швидкість прихованого каналу визначається об'ємом прихованих даних, рівнем інформаційного ущільнення відеоконтейнеру, швидкістю передачі даних в телекомунікаційній мережі;

- додаткове підвищення бітової швидкості прихованого каналу в середньому 5 … 7 разів.

3. Розвиток цього дослідження можливий за двома напрямками. По-перше, це вдосконалення

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

існуючих методів стиснення без втрат якості відеозображень. По-друге, це вдосконалення методу непрямого приховування інформації на основі додаткового врахування ключової послідовності.

Література

1. *JPEG Privacy & Security Abstract and Executive Summary [Electronic resource]. – 2015. – Access mode: https://jpeg.org/items/20150910_privacy_security_summary.html. – 7.06.2021.*

2. *Sharma, R. Data Security using Compression and Cryptography Techniques [Text] / R. Sharma, S. Bollavarapu // International Journal of Computer Applications. – 2015. – Vol. 117, No. 14. – P. 15–18. DOI: 10.5120/20621-3342.*

3. *Announcing the ADVANCED ENCRYPTION STANDARD (AES) [Text]. – Federal Information Processing Standards Publication 197, 2001. – 51 p.*

4. *Utility Driven Adaptive Preprocessing for Screen Content Video Compression [Text] / S. Wang, X. Zhang, X. Liu, J. Zhang, S. Ma, W. Gao // IEEE Transactions on Multimedia. – 2017. – Vol. 19, No. 3. – P. 660–667.*

5. *Gonzales, R. C. Digital image processing. [Text] / R. C. Gonzales, R. E. Woods // Prentice Inc. Upper Saddle River. – 2002. –779 p.*

6. *Dong, W. JPEG Compression Forensics against Resizing [Text] / W. Dong, J. Wang // IEEE Trustcom/ BigDataSE/IɞSPA. – 2016. – P. 1001 –1007. DOI: 10.1109/TrustCom.2016.0168.*

7. *Richter, T. Error Bounds for HDR Image Coding with JPEG XT [Text] / T. Richter // Data Compression Conference (DCC). – 2017. – P. 122–130. DOI: 10.1109/DCC.2017.7.*

8. *A Fast JPEG Image Compression Algorithm Based on DCT [Text] / W. Xiao, N. Wan, A. Hong, X. Chen // IEEE International Conference on Smart Cloud (SmartCloud). – 2020. – P. 106–110. DOI: 10.1109/SmartCloud49737.2020.00028.*

9. *Learned Video Compression [Text] / O. Rippel et al. // IEEE/CVF International Conference on Computer Vision (ICCV). – 2019. – P. 3453–3462. DOI: 10.1109/ICCV.2019.00355.*

10. *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.*

11. *Cruise UAV Video Compression Based on Long-Term Wide-Range Background [Text] / X. Wang, J. Xiao, R. Hu, Z. Wang // Data Compression Conference (DCC). – 2017. – P. 466–467. DOI: 10.1109/DCC.2017.71*

12. *Naor, M. Visual Cryptography [Text] / M. Naor, A. Shamir // Proceedings of the Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science. – 1995. – Vol. 950. – P. 1–12. DOI: 10.1007/bfb0053419.*

13. *Neural Inter-Frame Compression for Video Coding [Text] / A. Djelouah, J. Campos, S. Schaub-Meyer, C. Schroers // IEEE/CVF International Conference on Computer Vision (ICCV). – 2019. – P. 6420–6428. DOI: 10.1109/ICCV.2019.00652.*

14. *Narmatha, C. A LS-compression scheme for grayscale images using pixel based technique [Text] / C. Narmatha, P. Manimegalai, S. Manimurugan // International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT). – 2017. – P. 1–5. DOI: 10.1109/IGEHT.2017.8093980.*

15. *Alam, M. A. Faster Image Compression Technique Based on LZW Algorithm Using GPU Parallel Processing [Text] / M. A. Alam // Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2nd International Conference on Imaging, Vision & Pattern Recognition (icIVPR). – 2018. – P. 272–275, DOI: 10.1109/ICIEV.2018.8640956.*

16. *Chen, Ch.-Ch. A secure Boolean-based multi-secret image sharing scheme [Text] / Ch.-Ch. Chen, W.-J. Wu // Journal of Systems and Software. – 2014. – Vol. 92. – P. 107–114. DOI: 10.1016/j.jss.2014.01.001.*

17. *Deshmukh, M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic [Text] / M. Deshmukh, N. Nain, M. Ahmed // IEEE 30 th International Conference on Advanced Information Networking and Applications (AINA). – 2016. – P. 690–697. DOI: 10.1109/aina.2016.56.*

18. *Comparison of lossless video and image compression codecs for medical computed tomography datasets [Text] / V. Bui, L. Chang, D. Li, L. Hsu, M. Chen // IEEE International Conference on Big Data (Big Data). – 2016. – P. 3960–3962. DOI: 10.1109/BigData.2016.7841075.*

19. *Yang, Ch.-N. Enhanced Boolean-based multi secret image sharing scheme [Text] / Ch.-N. Yang, Ch.-H. Chen, S.-R. Cai // Journal of Systems and Software. – 2016. – Vol. 116. – P. 22–34. DOI: 10.1016/j.jss.2015.01.031.*

20. *An Encryption-then-Compression system for JPEG 2000 standard [Text] / O. Watanabe, A. Uchida, T. Fukuhara, H. Kiya // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – 2015. – P. 1226–1230. DOI: 10.1109/ICASSP.2015.7178165.*

21. *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.*

22. *Method of Increasing the Capacity of Information Threat Detection Filters in Modern Information and Communication Systems [Text] / T. Belikova, A. Lekakh, O. Dovbenko, O. Dodukh // IEEE 3rd International Conference on Advanced Information and Communications Technologies (AICT 2019). – 2019. – P. 426–429. DOI: 10.1109/AIACT.2019.8847754.*

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

24. 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.

25. Encode when necessary: Correlated network coding under unreliable wireless links [Text] / S. Wang, M. Kim, Z. Yin, T. He // ACM Transactions on Sensor Networks.– 2017. – Vol. 13, Iss. 1. DOI: 10.1145/3023953.

26. Hierarchical image-scrambling method with scramble-level controllability for privacy protection [Text] / T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki, T. Fujino // IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS). – 2013. – P. 1371–1374. DOI: 10.1109/MWSCAS.2013.6674911.

27. Lossless Compression of JPEG Coded Photo Collections [Text] / H. Wu, X. Sun, J. Yang, W. Zeng, F. Wu // IEEE Transactions on Image Processing. – 2016. – Vol. 25. – No. 6. – P. 2684–2696. DOI: 10.1109/TIP.2016.2551366.

28. Yuan, L. Secure JPEG Scrambling enabling Privacy in Photo Sharing [Text] / L. Yuan, P. Korshunov, T. Ebrahimi, // 11 th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG). – 2015. – P. 1–6. DOI: 10.1109/FG.2015.7285022.

29. Decoding Method of Information-Psychological Destructions in the Phonetic Space of Information Resources [Text] / T. Belikova // 2nd IEEE International Conference on Advanced Trends in Information Theory (ATIT). – 2020. – P 87–91. DOI: 10.1109/ATIT50783.2020.9349300.

30. Kobayashi, H. Bitstream-Based JPEG Image Encryption with File-Size Preserving [Text] / H. Kobayashi, H. Kiya // IEEE 7 th Global Conference on Consumer Electronics (GCCE). – 2018. – P. 1–4. DOI: 10.1109/gcce.2018.8574605.

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

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

33. The technology of the video stream intensity controlling based on the bit-planes recombination [Text] / 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.

34. The method of crypto-semantic presentation of images based on the floating scheme in the basis of the upper boundaries [Text] / V. Barannik, I. Tupitsya, S. Sidchenko, R. Tarnopolov // IEEE Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (IEEE PIC S&T 2015). – 2015. – P. 248–250. DOI: 10.1109/INFOCOMMST.2015.7357326.

35. 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.

36. A Integration the non-equilibrium position encoding into the compression technology of the transformed images [Text] / V. Barannik, Yu. Ryabukha, V. Tverdokhlib, A. Dodukh, O. Suprun, D. Tarasenko // IEEE 14th International Conference on East-West Design & Test Symposium (EWDTS, 2017). – 2017. – P. 1–5. DOI: 10.1109/EWDTS.2017.8110030.

37. Development Second and Third Phase of the Selective Frame Processing Method [Text] / Vladimir Barannik, Valeriy 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.

38. Model intelligent processing of aerial photographs with a dedicated key features interpretation [Text] / V. Barannik, A. Krasnorutskiy, Yu. Ryabukha, D. Okladnoy // 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). – 2016. - P. 736-738. DOI: 10.1109/TCSET.2016.7452167.

39. Coding tangible component of transforms to provide accessibility and integrity of video data [Text] / 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.

40. 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.

41. The video stream encoding method in infocommunication systems [Text] / V. Barannik, D. Barannik, S. Podlesny, , D. Tarasenko, O. Kulitsa // 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET). – 2018. - P. 538-541. DOI: 10.1109/TCSET.2018.8336259.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

42. 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.

43. Метод маскувального ущільнення службових даних в системах компресії відеозображень [Текст] / В. В. Бараннік, С. О. Сідченко, Н. В. Бараннік, А. М. Хіменко // Радіоелектронні і комп'ютерні системи. – 2021. – № 2(98). – Р. 51–63. DOI: 10.32620/reks.2021.2.05.

References

1. *JPEG Privacy & Security Abstract and Executive Summary*, 2015. Available at: https://jpeg.org/items/20150910_privacy_security_summary.html. (accessed 7.06.2021).

2. Sharma, R., Bollavarapu, S. Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*, 2015, vol. 117, no. 14, pp. 15-18. DOI: 10.5120/20621-3342.

3. *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards Publication 197, 2001. 51 p.

4. Wang, S., Zhang, X., Liu, X., Zhang, J., Ma, S., Gao, W. Utility Driven Adaptive Preprocessing for Screen Content Video Compression. *IEEE Transactions on Multimedia*, 2017, vol. 19, no. 3, pp. 660-667.

5. Gonzales, R. C., Woods, R. E. Digital image processing. *Prentice Inc. Upper Saddle River*, 2002. 779 p.

6. Dong, W., Wang, J. *JPEG Compression Forensics against Resizing. IEEE Trustcom/ BigDataSE/IʙSPA,* Tianjin, China, 2016, pp. 1001-1007. DOI: 10.1109/TrustCom.2016.0168.

7. Richter, T. Error Bounds for HDR Image Coding with JPEG XT. *Data Compression Conference (DCC)*, 2017, pp. 122-130. DOI: 10.1109/DCC.2017.7.

8. Xiao, W., Wan, N.A., Hong and Chen, X. A Fast JPEG Image Compression Algorithm Based on DCT. *IEEE International Conference on Smart Cloud (SmartCloud)*, 2020, pp. 106-110. DOI: 10.1109/ SmartCloud49737. 2020.00028.

9. Rippel, O. et al. Learned Video Compression. *IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019, pp. 3453-3462. DOI: 10.1109/ICCV. 2019.00355.

10. Rivest, R. L., Shamir, A., Adleman, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, iss. 2, pp. 120-126. DOI: 10.1145/359340.359342.

11. Wang, X., Xiao, J., Hu, R., Wang, Z. Cruise UAV Video Compression Based on Long-Term Wide-Range Background. *Data Compression Conference (DCC)*, 2017, pp. 466-467. DOI: 10.1109/DCC.2017.71.

12. Naor, M., Shamir, A. Visual Cryptography. *Proceedings of the Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science*, 1995, vol. 950, pp. 1-12. DOI: 10.1007/bfb0053419.

13. Djelouah, A., Campos, J., Schaub-Meyer, S., Schroers, C. Neural Inter-Frame Compression for Video Coding. *IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019, pp. 6420-6428. DOI: 10.1109/ICCV.2019.00652.

14. Narmatha, C., Manimegalai, P., Manimurugan, S. A LS-compression scheme for grayscale images using pixel based technique. *International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)*, 2017, pp. 1-5. DOI: 10.1109/ IGEHT.2017.8093980.

15. Alam, M. A., Faster Image Compression Technique Based on LZW Algorithm Using GPU Parallel Processing. *Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2nd International Conference on Imaging, Vision & Pattern Recognition (icIVPR)*, 2018, pp. 272-275, DOI: 10.1109/ICIEV.2018.8640956.

16. Chen, T.-H., Wu, Ch.-S. Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*, 2011, vol. 91, iss. 1, pp. 90-97. DOI: 10.1016/j.sigpro.2010.06.012.

17. Deshmukh, M., Nain, N., Ahmed, M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic. *IEEE 30 th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 690-697. DOI: 10.1109/aina.2016.56.

18. Bui, V., Chang, L., Li, D., Hsu, L., Chen, M. Comparison of lossless video and image compression codecs for medical computed tomography datasets. *IEEE International Conference on Big Data (Big Data)*, 2016, pp. 3960-3962. DOI: 10.1109/BigData. 2016.7841075.

19. Yang, Ch.-N., Chen, Ch.-H., Cai, S.-R. Enhanced Boolean-based multi secret image sharing scheme. *Journal of Systems and Software*, 2016, vol. 116, pp. 22-34. DOI: 10.1016/j.jss.2015.01.031.

20. Watanabe, O., Uchida, A., Fukuhara, T., Kiya, H. An Encryption-then-Compression system for JPEG 2000 standard. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 1226-1230, DOI: 10.1109/ICASSP.2015. 7178165.

21. Zhou, J., Liu, X., Au, O. C., Tang, Y. Y. Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation. *IEEE Transactions on Information* Forensics and Security, 2014, vol. 9, no. 1, pp. 39-50. DOI: 10.1109/TIFS.2013.2291625.

22. Lekakh, A., Belikova, T., Dovbenko, O., Dodukh, O. Method of Increasing the Capacity of Information Threat Detection Filters in Modern Information and Communication Systems. *IEEE 3rd Interna-*

tional Conference on Advanced Information and Communications Technologies (AICT 2019), 2019, pp. 426-429. DOI: 10.1109/AIACT.2019.8847754.

23. Barannik, Valeriy. Fast Coding of Irregular Binary Binomial Numbers with a Set Number of Units Series. *IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 2020, pp. 29-33. DOI: 10.1109/ATIT50783.2020.9349356.

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

25. Wang, S., Kim, S. M., Yin, Z., & He, T. Encode when necessary: Correlated network coding under unreliable wireless links. *ACM Transactions on Sensor Networks*, 2017, vol. 13(1). DOI: 10.1145/3023953.

26. Honda, T., Murakami, Y., Yanagihara, Y., Kumaki, T., Fujino, T. Hierarchical image-scrambling method with scramble-level controllability for privacy protection. *IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013, pp. 1371-1374. DOI: 10.1109/MWSCAS.2013.6674911.

27. Wu, H., Sun, X., Yang, J., Zeng, W., Wu, F. Lossless Compression of JPEG Coded Photo Collections. *IEEE Transactions on Image Processing*, 2016, vol. 25, no. 6, pp. 2684-2696. DOI: 10.1109/TIP.2016.2551366.

28. Yuan, L., Korshunov, P., Ebrahimi, T. Secure JPEG Scrambling enabling Privacy in Photo Sharing. *11 th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, 2015, pp. 1-6. DOI: 10.1109/FG.2015.7285022.

29. Belikova, T. Decoding Method of Information-Psychological Destructions in the Phonetic Space of Information Resources. *2nd IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 2020, pp. 87–91. DOI: 10.1109/ATIT50783.2020.9349300.

30. Kobayashi, H., Kiya, H. Bitstream-Based JPEG Image Encryption with File-Size Preserving. *IEEE 7 th Global Conference on Consumer Electronics (GCCE)*, 2018, pp. 1-4. DOI: 10.1109/gcce.2018.8574605.

31. Li, F., Krivenko, S., Lukin, V. Two-step providing of desired quality in lossy image compression by SPIHT. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 2, pp. 22-32. DOI: 10.32620/reks.2020.2.02.

32. Ieremeiev, O., Lukin, V., Okarma, K. *Kombinovana metryka vizual'noyi yakosti zobrazhen' dystantsiynoho zonduvannya na osnovi neyronnoyi merezhi* [Combined visual quality metric of remote sensing images based on neural network]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 4(96), pp. 4-15. DOI: 10.32620/reks.2020.4.01.

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

34. Barannik, V., Tupitsya, I., Sidchenko, S., Tarnopolov, R. *The method of crypto-semantic presentation of images based on the floating scheme in the basis of the upper boundaries*. *IEEE Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (IEEE PIC S&T 2015)*, 2015, pp. 248-250. DOI: 10.1109/INFOCOMMST.2015.7357326.

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

36. Barannik, V., Ryabukha, Yu., Tverdokhlib, V., Dodukh, A., Suprun, O., Tarasenko, D. Integration the non-equilibrium position encoding into the compression technology of the transformed images. *IEEE 14th International Conference on East-West Design & Test Symposium (EWDTS, 2017)*, 2017, pp. 1-5. DOI: 10.1109/EWDTS.2017.8110030.

37. Barannik, Vladimir, Barannik, Valeriy, Havrylov, D., Sorokun, A. Development Second and Third Phase of the Selective Frame Processing Method. *3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 54-57. DOI: 10.1109/AIACT.2019.8847897.

38. Barannik, V., Krasnorutskiy, A., Ryabukha, Yu., Okladnoy, D. Model intelligent processing of aerial photographs with a dedicated key features interpretation. *IEEE 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2016, pp. 736-738. DOI: 10.1109/TCSET.2016.7452167.

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

40. Barannik, V. V., Ryabukha, Yu. N., Kulitsa, O. S. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems. *Telecommunications and Radio Engineering*, 2017, vol. 76, no. 9, pp. 785-797. DOI: 10.1615/TelecomRadEng.v76.i9.40.

41. Barannik, V. V., Barannik, D., Podlesny, S., Tarasenko, D., Kulitsa, O. The video stream encoding method in infocommunication systems. *14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineer-*

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ing (TCSET), 2018, pp. 538-541. DOI: 10.1109/TCSET.2018.8336259.

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

43. Barannik, V., Sidchenko, S., Barannik, N., Khimenko, A. Metod maskuval'noho ushchil'nennya sluzhbovykh danykh v systemakh kompresiyi videozobrazhen' [The method of masking overhead compaction in video compression systems]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2021, no. 2, pp. 51–63. DOI: 10.32620/reks.2021.2.05.

Надійшла до редакції 27.09.2021, розглянута на редколегії 26.11.2021

МЕТОД КОСВЕННОГО СКРЫТИЯ ИНФОРМАЦИИ В ПРОЦЕССЕ СЖАТИЯ ВИДЕОИЗОБРАЖЕНИЙ

В. В. Баранник, Н. В. Баранник, А. А. Игнатьев, В. В. Хименко

Обосновывается, то, что для обеспечения защиты специального информационного ресурса в условиях его оперативной доставки, необходимо использовать стеганографические системы. В этом случае стеганографические технологии являются составляющей комплексных систем защиты информации. В то же время для стеганографических систем существует противоречие между плотностью встроенных данных и уровнем информационного уплотнения видеоконтейнера (уровень уменьшения битового объема компактно представленного видеоизображения относительно битового объема начального видеоизображения). Это является причиной того, что в условиях требуемого качества (достоверности) цифровой видеоинформации, уровень битовой скорости скрытого канала будет недостаточным. Следовательно, научно прикладная проблематика, состоящая в необходимости повышения целостности (уровень соответствия скрытой информации до ее встраивания в видеоконтейнер и после ее изъятия) и битовой скорости скрытого канала передачи специальной информации, является актуальной. Решение сформулированной задачи в области применения стеганографических преобразований реализуется на основе применения двух разных подходов. Первый подход базируется на методах непосредственного встраивания сообщений. Но такой подход характеризуется внесением искажений в видеоизображения, которые используются в качестве контейнера. Поэтому происходят изменения структурных и статистических закономерностей в синтаксическом описании видеоконтейнеров. Это снижает потенциальные возможности относительно сжатия видеоконтейнеров. Второй подход в направлении создания методов стеганографических преобразований базируется на скрытии информации с использованием методов косвенного встраивания. Здесь в процессе встраивания информации используется функциональная зависимость между элементами видеоконтейнера и элементами встроенного сообщения. Установление конкретной зависимости между элементами видеоконтейнера соответствует встраиванию элемента со значением «0» или «1». Однако для существующих методов косвенного стеганографического преобразования характерный недостаток, который заключается в низком значении плотности встроенных данных. Для устранения недостатков предлагается разработать подход, который позволит использовать для скрытия не только психовизуальную, но и структурную избыточность видеоконтейнера. Поэтому цель исследований статьи заключается в разработке метода косвенного скрытия информации в процессе сжатия видеоконтейнера для повышения битовой скорости канала скрытых сообщений. В процессе исследований построена стеганографическая мультиадическая система. Это позволяет встраивать элементы скрытого сообщения без потерь информации на основе косвенного подхода путем модификации активных оснований мультиадического базиса с учетом их неопределенности. Для отбора трансформант (массивов данных) в качестве контейнеров для встраивания информации учитывается требование относительно существования базовой системы со всеми активными основаниями. Количество встроенных бит скрытого сообщения соответствует количеству активных оснований в базовой системе мультиадического пространства. В результате проведенных экспериментов получены следующие результаты: в процессе встраивания сообщений на базе созданного метода не вносятся искажения в видеоконтейнер; для созданного метода достигается дополнительное повышение битовой скорости скрытого канала в среднем 5 … 7 раз.

Ключевые слова: сжатие видеоизображений; конфиденциальность информации; стеганографические преобразования; мультиадический базис; модифицированная система оснований; кодирование; компрессия; видеоизображения; наименее значимый бит, относительная замена.

METHOD OF INDIRECT INFORMATION HIDING IN THE PROCESS OF VIDEO COMPRESSION

V. Barannik, N. Barannik, O. Ignatyev, V. Himenko

It is substantiated that steganographic systems should be used to ensure the protection of special information resources in conditions of its prompt delivery. Here, steganographic technologies are an integral part of complex

information protection systems. Simultaneously, for steganographic systems, there is a contradiction between the density of embedded data and level of information compaction of video container (level of reduction of volume bit volume of compact presented video image concerning bit volume of an initial video image). It leads to the fact that under the conditions of the required quality (reliability) of digital video information, the bit rate level of the covert channel is insufficient. Consequently, the scientific-applied problem concerns the necessity to increase the integrity (the level of correspondence of the hidden information before its embedding in a video container and after its extraction) and bit rate of the hidden channel of special information transmission. It is relevant. The solution of the described problem in the field of application of steganographic transformations can be realized based on the application of two different approaches. The first approach is based on methods of direct message embedding. But this approach is characterized by introducing distortions in the video images used as a container. Therefore, changes in structural and statistical patterns in the syntactic description of the video container happen. It reduces the potential for video container compaction. The second approach to creating steganographic transformation methods is based on information hiding using indirect embedding technique. Here, the embedding process exploits the functional dependency between the elements of the video container and the elements of the embedded message. Setting a specific dependency between the elements in the video container corresponds to the embedded element with a value of "0" or "1". However, the existing indirect steganographic transformation methods have a disadvantage. It consists of an insufficient value of embedded data density. To eliminate these disadvantages, it is proposed to develop an approach that allows using not only psychovisual but also structural redundancy of video container for concealment. Therefore, the research objective of this paper is to develop a method for indirect information withholding in the video container compression process to increase the bit rate of the hidden message channel. In the process of research, a steganographic multiagent system is constructed, which allows embedding hidden message elements without loss of information based on the indirect approach by modifying the active bases of the multiagent basis considering their uncertainty. To select transformants (data sets) as containers for information embedding, the requirement of the existence of a base system with all active bases is taken into account. The number of embedded bits of the hidden message is equal to the number of active bases in the base system of the multiadic space. Because of the made experiments, the following results have been received: in the process of embedding messages based on the created method distortions in a video container is not brought; for the created method the additional increase in the hidden channel bit rate in average 5 … 7 times are reached.

Keywords: image compressing; information security; steganographic transformation; multiadic basis; modification of basis system; coding; compression; video image; the least significant bit; relative replacement.

Бараннік Володимир Вікторович – д-р техн. наук, проф., проф. кафедри штучного інтелекту та програмного забезпечення, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

Бараннік Наталія Вячеславівна – здобувач, Харківський національний університет радіоелектроніки, Харків, Україна.

Ігнатьєв Олександр Олексійович – студент Харківського національного університету радіоелектроніки, Харків, Україна.

Хіменко Вікторія Вікторівна – аспірант Харківського національного університету радіоелектроніки, Харків, Україна.

Vladimir Barannik – Doctor of Technical Sciences, Professor, Professor of the Department of Artificial Intelligence and Software, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: vvbar.off@gmail.com, ORCID: 0000-0002-2848-4524, Scopus Author ID: 27867503300,
https://scholar.google.com/citations?&user=3xZFPUQAAAAJ&hl.

Natalia Barannik – PhD student, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine,
e-mail: barannik11121972@gmail.com, ORCID: 0000-0001-6420-1838, Scopus Author ID: 57207757558,
https://scholar.google.com.ua/citations?&user=6rGhQ5EAAAAJ.

Oleksandr Ignatyev – Student, Kharkiv National University of Radio Electronics, Kharkiv,
e-mail: oleksandr.ignatyev10@gmail.com, ORCID: 0000-0003-1227-6840.

Victoriya Himenko – PhD student, Kharkiv National University of Radio Electronics, Kharkiv,
e-mail: vika.iv55@gmail.com.