Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет __Комп'ютерної інженерії та управління_____
(повна назва)

Кафедра Автоматизації проектування обчислювальної техніки
(повна назва)

Звіт
з передатестаційної практики

_____*БАКАЛАВР*_____
(освітній ступінь)

_____
(позначення документа)

Структурно-стеганографічне кодування з плаваючим базисом вбудовування для підвищення безпеки інформаційних ресурсів
(тема)

Виконав: студент IV курсу, групи КІ-14-7

спеціальності (напряму підготовки) _____

_____6.050102 – Комп'ютерна інженерія__

_____
(шифр і назва спеціальності, напряму)

_____ Бараннік Д.В.
(підпис) (прізвище, ініціали)

Керівник роботи_____ Літвінова Э.І.
(підпис) (прізвище, ініціали)

Керівник практики _____ Хаханова Г.В.
(підпис) (прізвище, ініціали)

2018 р.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ДКП – дискретне косинусне перетворення

ДНК – дезоксирибонуклеїнова кислота

ЗК – зображення-контейнер

НЗБ – найменш значимий біт

НПЧ – нерівновагове позиційне число

РС – розширення спектру

СКП – системи критичного призначення

ЗМІ – засоби масової інформації

СКІ – системи критичної інфраструктури

СІР – спеціальні інформаційні ресурси

ВСТУП

Досвід функціонування систем критичної інфраструктури в умовах активної протидії противника виявив гостру потребу забезпечення необхідного рівня безпеки спеціальних інформаційних ресурсів (СІР). З одного боку це диктується підвищеною значимістю СІР для інформаційної підтримки процесів ухвалення рішень, у тому числі в кризових ситуаціях. З іншого боку підвищуються загрози порушення конфіденційності і цілісності СІР. У значній мірі це обумовлено зростанням оперативно-програмних і інформаційно-технологічних можливостей протиборчої сторони. Тому підвищення безпеки спеціальних інформаційних ресурсів в інфокомунікаційних системах є актуальним напрямом науково-прикладних досліджень.

Звідси виникає інтерес розробки нових шляхів забезпечення безпеки СІР. Одним з напрямів є використання стеганографічних методів вбудовування інформації в зображення-контейнер. Базою для реалізації такого підходу є системи відеоконференцзв'язку, широке використання мультимедійних засобів, розвиток поля відеоінформації, наявність прив'язки службової інформації до конкретного відеоматеріалу.

Серед методів стеганографічних перетворень окремий інтерес представляють методи безпосереднього вбудовування інформації в зображення-контейнер.

Проте проведений аналіз існуючих методів виявив наступні проблемні недоліки:

- недостатнє значення відносної стеганографічної ємкості;

- недостатнє значення стійкості вбудовуваних даних до атак противника;

- значні візуальні спотворення стеганограми.

Такі недоліки обумовлені тим, що в процесі стеганографічних

перетворень в основному враховуються психовізуальні закономірності. При цьому вилучення вбудовуваної інформації здійснюється з використанням кореляційних залежностей, які порушуються в результаті нелінійної обробки стеганограми.

У цей же час підвищуються вимоги до інформаційного забезпечення систем критичної інфраструктури (СКІ). Такі вимоги обумовлені наступними чинниками:

- підвищення інформаційної інтенсивності донесень в умовах кризових ситуацій;
- використання в якості спеціальних донесень відеоматеріалів;
- підвищення значимості впливу спеціальних донесень на результативність функціонування СКІ;
- підвищення вимог відносно достовірності і наочності донесень;
- необхідність оперативної доставки прихованих повідомлень в обмежені тимчасові проміжки сеансу зв'язку;
- необхідність забезпечення і контролю використання пропагандистського поля протистояння.

Значить, в процесі використання існуючих стеганографічних систем для прихованої передачі спеціальної інформації виникає протиріччя, яке полягає в тому, що існуючі стеганографічні технології не забезпечують повною мірою системних вимог в кризових ситуаціях в умовах наявності активних протиборчих сторін.

Для вирішення протиріччя в процесі побудови стеганографічних систем пропонується додатково враховувати наявність структурних закономірностей відеоконтейнерів.

1 АСПЕКТИ АКТУАЛЬНОСТІ І ЗНАЧИМОСТІ СТЕГАНОГРАФІЧНИХ ПІДХОДІВ

Для обгрунтування підходу відносно підвищення безпеки спеціальних інформаційних ресурсів на основі стеганографічних методів необхідно розглянути аспекти, які визначають їх актуальність і значимість в кризових умовах. Тут слід виділити такі аспекти актуальності і значимості стеганографічних методів:

1. Необхідність підвищення рівня конфіденційності, цілісності і доступності спеціального інформаційного ресурсу. У сучасних умовах функціонування систем кризового призначення необхідною умовою є забезпечення заданого рівня складових інформаційної безпеки: конфіденційності, цілісності і доступності. Така необхідність обумовлена з одного боку підвищенням значимості інформації і необхідністю її захисту, а з іншого боку можливостями зловмисника відносно порушення конфіденційності, цілісності і доступності.

2. Обмеження при використанні криптографічних алгоритмів захисту спеціальних інформаційних ресурсів. Вони мають негативні наслідки і можуть завдати збитку політичному і економічному іміджу держави.

3. Формування умов для розвитку стеганографічних підходів забезпечення безпеки спеціальних інформаційних ресурсів обумовлюються наступними позиціями:

1) наявністю великої кількості різних стеганографічних методів приховуваного вбудовування і передачі інформації;

2) розвитком телекомунікаційних технологій, що використовують відкриті канали передачі даних широкого доступу;

3) відсутністю достатньої кількості методів стеганографічного аналізу для виявлення фактів наявності приховуваного вбудовування спеціальної інформації;

4) широким поширенням мультимедійних файлів в інфокомунікаційному просторі. Це створює базу для формування контейнерів, які використовуються при вбудовуванні інформації;

5) відсутністю обмежень в нормативно-правовій базі на використання стеганографічних методів захисту інформації.

Тому в системах комплексного захисту спеціальних інформаційних ресурсів потрібно також використовувати методи стеганографічних перетворень. Стеганографічні перетворення на відміну від криптографічної обробки дозволяють приховати сам факт наявності секретного повідомлення. Тут інформація у вигляді повідомлення перетвориться певним чином і вбудовується в деякий цифровий контейнер, який не привертає уваги. Функціональна схема реалізації прихованої передачі даних на основі використання стеганографічних підходів представлена на рис 1.6 і включає наступні етапи:

1. Стеганографічне вбудовування. На цьому етапі здійснюється стеганографічне вбудовування інформації в цифровий контейнер. Вбудовуване повідомлення може бути заздалегідь перетворене на основі алгоритмів шифрування, компресійного і завадостійкого кодування. У стеганографічному кодері перетворене повідомлення вбудовується в контейнер на основі стеганографічного правила і ключової інформації.

В результаті стеганографічного перетворення формується стеганограма.

2. Передача стеганографічно перетвореного контейнера (стеганограми) отримувачу по каналах передачі даних або розміщення стеганограми в сховищах. В процесі передачі в інфокомунікаціях стеганограма може піддаватися активним пасивним діям.

3. Стеганографічне вилучення. На цьому етапі авторизований користувач проводить стеганографічне декодування. В цьому випадку йому відома наступна інформація:

- факт наявності вбудованої інформації в стеганограмі;

- правило стеганографічного декодування;

- ключова інформація.

В результаті зворотнього стеганографічного перетворення авторизований користувач здійснює вилучення вбудованої інформації.

Процес стеганографічного вилучення здійснюється за наявності на приймальній стороні ключової інформації.

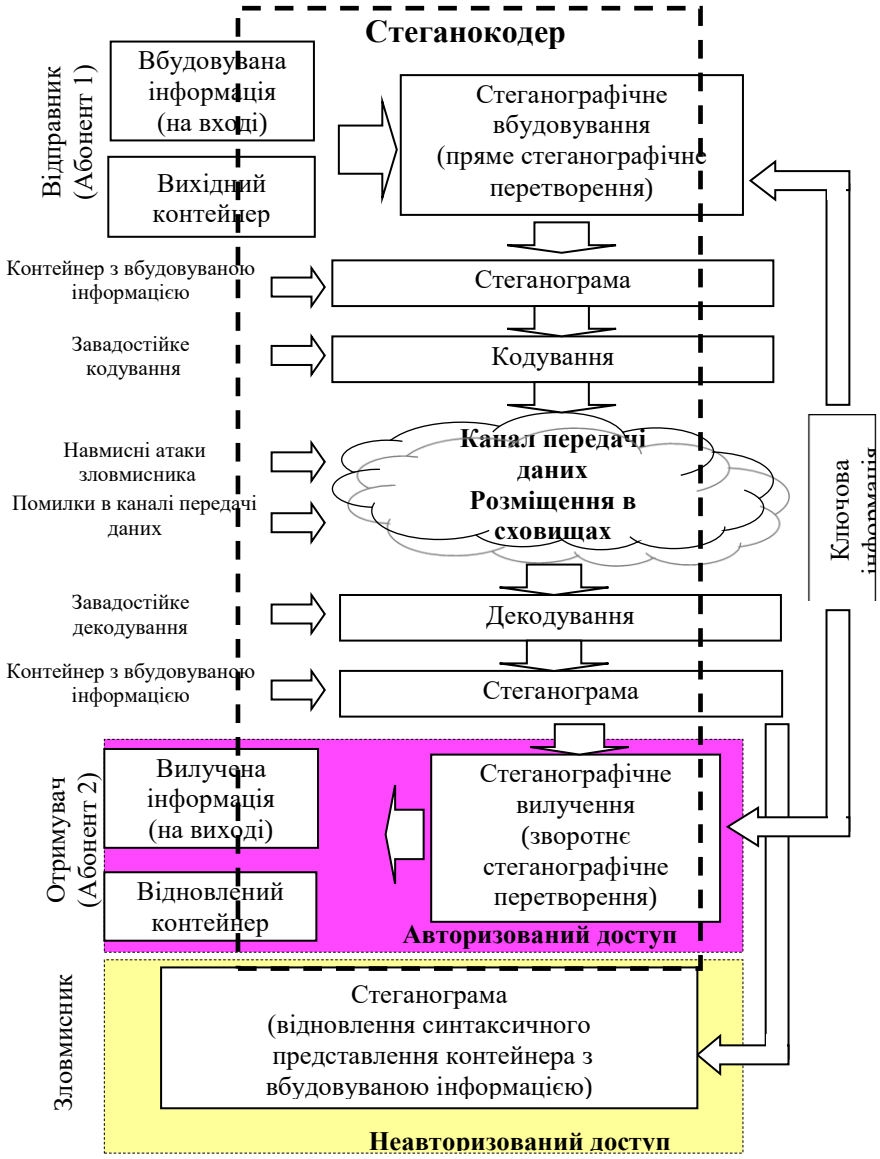

Рисунок. 1.1 - Функціональна схема реалізації прихованої передачі даних на основі стеганографічного підходу

Тепер розглянем випадок для неавторизованого доступу. Тут у зловмисника відсутня інформація про наявність скритного вбудовування повідомлення в конкретній стеганограмі. Навіть якщо зловмисник обізнаний про те, що в даній стеганограмі присутні вбудовані дані, він не здатний їх вилучити внаслідок відсутності у нього ключової інформації.

2 АСПЕКТИ ДОСЛІДЖЕНЬ

Задоволення вимог до інформаційного забезпечення кризових систем пов'язане з підвищенням ефективності функціонування існуючих стеганографічних методів для прихованої передачі спеціальних інформаційних ресурсів. В цьому випадку для існуючих стеганографічних перетворень висуваються наступні вимоги:

1.Необхідність підвищення відносної стеганографічної ємкості $w_{отн}$ методів вбудовування інформації. Дана вимога диктується постійним зростанням об'ємів і збільшенням змістовної значимості спеціальної інформації.

2. Необхідність підвищення ймовірності $P_{из}$ правильного вилучення вбудованих даних в умовах застосування активних атак. Наявність величезних можливостей зловмисника відносно реалізації атак, направлених на руйнування і модифікацію вбудованих даних. Це супроводжується підвищеними вимогами до стеганографічесних методів відносно безпомилкового вилучення вбудованих даних.

3. Необхідність збільшення чинника візуальної стійкості стеганограми. Для забезпечення стійкості зображення з вбудованими даними до візуальних атак, направлених на встановлення факту наявності стеганографічного вбудовування.

Отже, в процесі використання існуючих стеганографічних методів для прихованої передачі спеціальної інформації виникає протиріччя, яке полягає в тому, що існуючі технології стеганографічних перетворень не забезпечують повною мірою нових системних вимог в кризових умовах за наявності дестабілізуючих чинників і протиборчих сторін.

Для вдосконалення існуючих і розробки нових методів стеганографічних перетворень необхідно використовувати принципово нові підходи, які повинні базуватися на сучасних і перспективних досягненнях в області теорії інформації, кодування, теорії обробки цифрових відеопросторів,

технологій інтелектуального аналізу і методів криптографії. Одним з актуальних напрямів є використання структурних перетворень елементів просторового представлення зображення для виявлення структурно-комбінаторної надлишковості. Такий підхід дозволить підвищити стійкість вбудованих даних до активних атак противника.

Звідси, напрям дослідження полягає в розробці теоретичних основ і методів підвищення безпеки спеціальної інформації на основі стеганографічного перетворення.

Структурно-комбінаторне стеганографічне кодування задається функціоналом $\mathrm{F}\{P_{из},\ w_{отн},\ h\}$ в умовах виконання наступних обмежень:

$$\begin{cases} P_{из} \geq P_{из}^{(тр)}; \\ w_{отн} \geq \mathrm{w}_{отн}^{(тр)}; \\ h \geq h^{(тр)}; \end{cases}$$

де $\mathrm{F}\{P_{из},\ w_{отн},\ h\}$ - функціонал, який реалізує стеганографічний метод вбудовування спеціальної інформації;

$\mathrm{w}_{отн}^{(тр)}$ - необхідне значення відносної стеганографічної ємкості системи;

$h^{(тр)}$ - необхідне значення пікового відношення сигнал-шум.

Таким чином, для досягнення поставленої необхідно вирішити наступні завдання:

- обгрунтувати підхід для вдосконалення методів безпосереднього вбудовування інформації в цифрове зображення-контейнер;

- розробити метод структурно-комбінаторного стеганографічного кодування для підвищення безпеки спеціальної інформації;

- створити метод для локалізації структурної стеганографічної надлишковості для підвищення стійкості відносно атак, направлених на виявлення факту вбудованої інформації;

- побудувати систему вбудовування інформації з маскуванням стеганографічної надлишковості.

3 РОЗРОБКА ТЕХНОЛОГІЇ ФУНКЦІОНАЛЬНОГО ПЕРЕТВОРЕННЯ ЧИСЕЛ З ІМПЛАНТОВАНИМИ ДАНИМИ НА ОСНОВІ НЕРІВНОВАГОВОГО ПОЗИЦІЙНОГО КОДУВАННЯ

В якості перетворюючого функціонала, що володіє властивостями у відповідності з вимогами відносно процесу приховання даних пропонується використовувати кодоутворюючу функцію для нерівновагового позиційного числа (НПЧ кодування), а як елемент-контейнер пропонується використовувати нерівновагове позиційне число.

В процесі нерівновагового позиційного кодування формуються кодові комбінації, що складаються з двох частин, а саме: інформаційна складова N і службова складова Ψ (рис. 3.1).

В цьому випадку вихідний елемент зображення розглядається як нерівновагове позиційне числа A, яке складається з m елементів, а саме

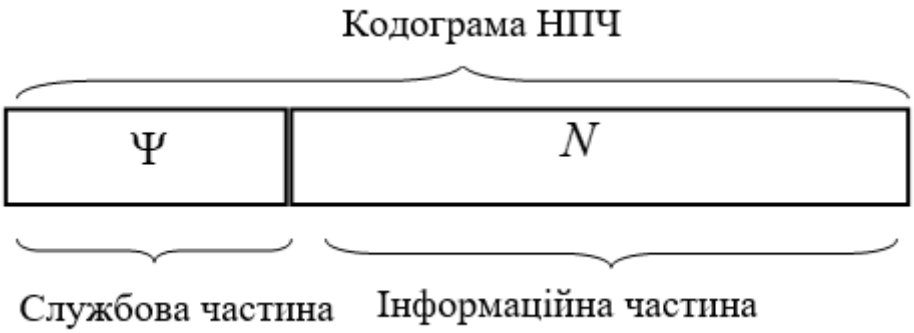

Рисунок. 3.1 -. Схема кодограми для нерівновагового позиційного числа

$$A = \{a_{1,j}; ...; a_{i,j}; ...; a_{m,j}\}.$$

Для вихідного НП числа (рис 3.2) A значення коду визначається по формулі:

$$N = f'(A),$$

де N - код вихідного нерівновагового позиційного числа A.

На другому етапі для сформованого значення коду N будується результуюче кодове представлення C_2 нерівновагового позиційного числа A:

$$C_2 = \varphi_c(N, \Psi).$$

Тут φ_c - оператор, що забезпечує побудову двійкової коду C_2 для кодового значення N і службових даних Ψ .

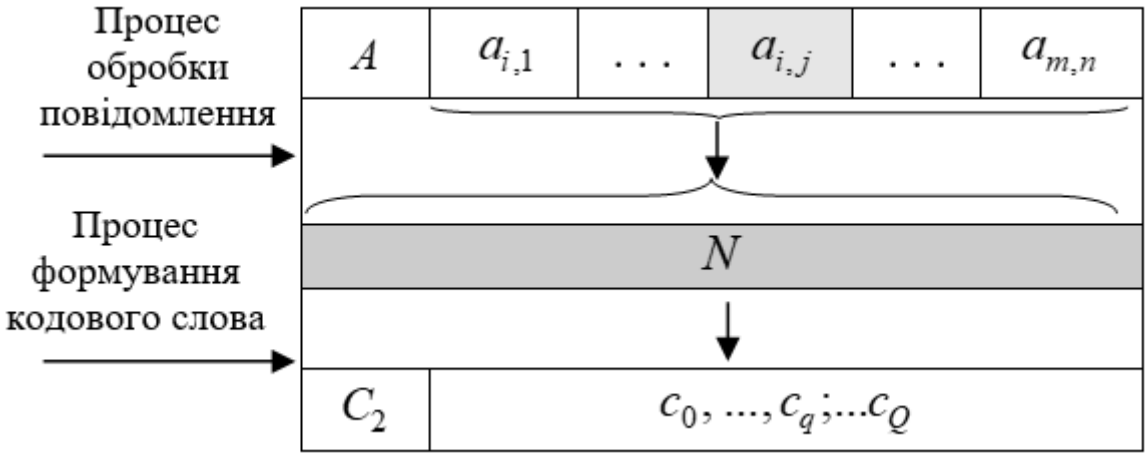

Рисунок. 3.2 - Структурна схема побудови кодових конструкцій для нерівновагового позиційного числа А

В цьому випадку отримаємо

$$C_2 = \{c_1; \ldots; c_q; \ldots; c_Q\}; \quad c_q \in \{0; 1\},$$

де Q - кількість біт на представлення НП числа C_2.

Службова складова включає інформацію про систему основ нерівновагового позиційного числа $\Psi = \{\psi_{i,j}\}$.

В разі такого підходу для формування кодового представлення C_2

нерівновагового позиційного числа A, оператор зворотнього функціонального перетворення $f^{(-1)'}(\bullet)$ дозволить отримати вихідне НП число A за наявності службової інформації Ψ . Вираз, який описує зворотнє функціональне перетворення має вигляд:

$$A = f^{(-1)'}(C_2; \Psi).$$

Для такого підходу принцип вбудовування пропонується вибирати таким чином (рис 3.3).

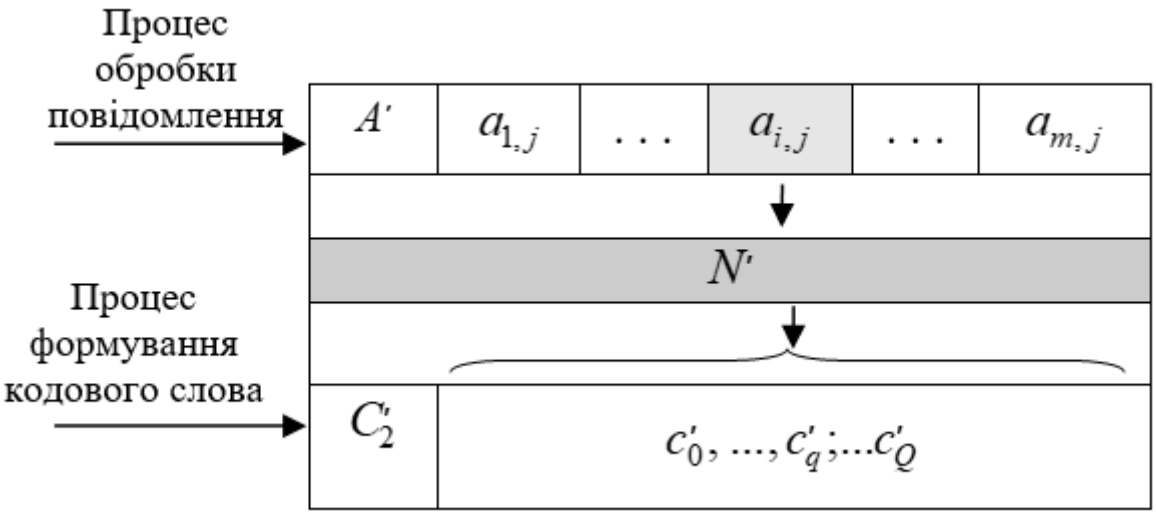

Рисунок 3.3 - Структурна схема побудови кодових конструкцій НП числа A' з вбудованими даними

У вихідне нерівновагове позиційне число A за допомогою оператора φ' вбудовується біт b_ξ приховуваного повідомлення В таким чином, що

$$A' = \varphi'(A; b_\xi).$$

Тут A' - нерівновагове позиційне число з вбудованим бітом b_ξ (НПЧ з вбудовуванням).

Після чого, визначається код N' для числа A':

$$N' = f'(A').$$

На третьому етапі для сформованого значення коду N' будується результуюче кодове представлення C_2' нерівновагового позиційного числа A' з вбудовуванням:

$$C_2' = \varphi_c(N', \Psi^{(1)}).$$

Тут φ_c - оператор, що забезпечує побудову двійкового коду C_2'.

Зворотнє стеганографічне перетворення виконуватиметься за біполярним принципом для авторизованого (за наявності ключа $\Psi^{(2)}$) і неавторизованого користувача (зловмисника) за стандартних умов.

Перший спосіб використовується неавторизованим користувачем. Відновлення зображення відбувається за наявності відкритої службової інформації $\Psi^{(1)}$, що є системою основ НП числа A'. Таке зворотнє перетворення дозволяє достовірно реконструювати елемент $A''(1)$ по формулі:

$$A(1)'' = f'^{(-1)}(C_2; \Psi^{(1)})$$

так, щоб значення кількісної метрики $\varepsilon(A; A(1)'')$ було найменшим

$$\varepsilon(A; A(1)'') \to 0.$$

Тут $A''(1)$ - елемент, реконструйований за стандартних умов.

Другий спосіб існує для авторизованого користувача. Тут зворотнє функціональне перетворення здійснюється з використанням відкритої службової інформації $\Psi^{(1)}$ і ключа $\Psi^{(2)}$. В даному випадку значення ключа $\Psi^{(2)}$

є заздалегідь відомим значенням основи вбудованого елементу так, щоб $\Psi^{(2)} \neq \Psi^{(1)}$. Зворотнє функціональне перетворення дозволить авторизованому користувачеві безпомилково реконструювати число з вбудованими даними, тобто:

$$A(2)'' = f'^{(-1)}(C_2; \Psi^{(1)}; \Psi^{(2)}) \quad \text{і} \quad A(2)'' = A',$$

де $A(2)''$ - нерівновагове позиційне число з вбудованими даними, отримане при зворотньому функціональному перетворенні авторизованим користувачем.

Вилучення вбудованої інформації відбувається без внесення помилок внаслідок застосування оператора вилучення $\varphi_c'^{(1)}$ до нерівновагового позиційного числа $A(2)''$, що реконструюється, при якому також можливе безпомилкове відновлення числа A''' як елементу вихідного зображення, так що:

$$\varphi'^{(-1)}(A''(2)) = \begin{cases} b'_\xi, & b'_\xi = b_\xi; \\ A''', & A''' = A. \end{cases}$$

Тут b'_ξ - вилучений елемент приховуваного повідомлення B'_2.

На рис. 3.4. представлена схема стеганографічного методу на основі нерівновагового позиційного кодування. Пряме стеганографічне перетворення реалізується в три етапи. На першому етапі за допомогою оператора вбудовування φ біт b_ξ приховуваного повідомлення B_2 вбудовується на різну позицію НП числа A. Отримане внаслідок завантаження біту b_ξ нерівновгове позиційне число A' визначається виразом

$$A' = \varphi(b_\xi; A).$$

На другому етапі для стеганочисла A' за правилом $f(A')$ формується код N', а саме:

$$N' = f'(A').$$

Формування коду відбувається з врахуванням ключової інформації $\Psi^{(2)}$, що уявляє собою основу вбудованого елементу.

На третьому етапі будується результуюче кодове представлення C_2' числа A' з вбудованими даними. Це описується виразом:

$$C_2' = \varphi_c(N'; \Psi^{(1)}).$$

Отримана стеганограма C, що містить в собі інформаційну складову N' і службову складову $\Psi^{(1)}$, піддається атакуючим діям.

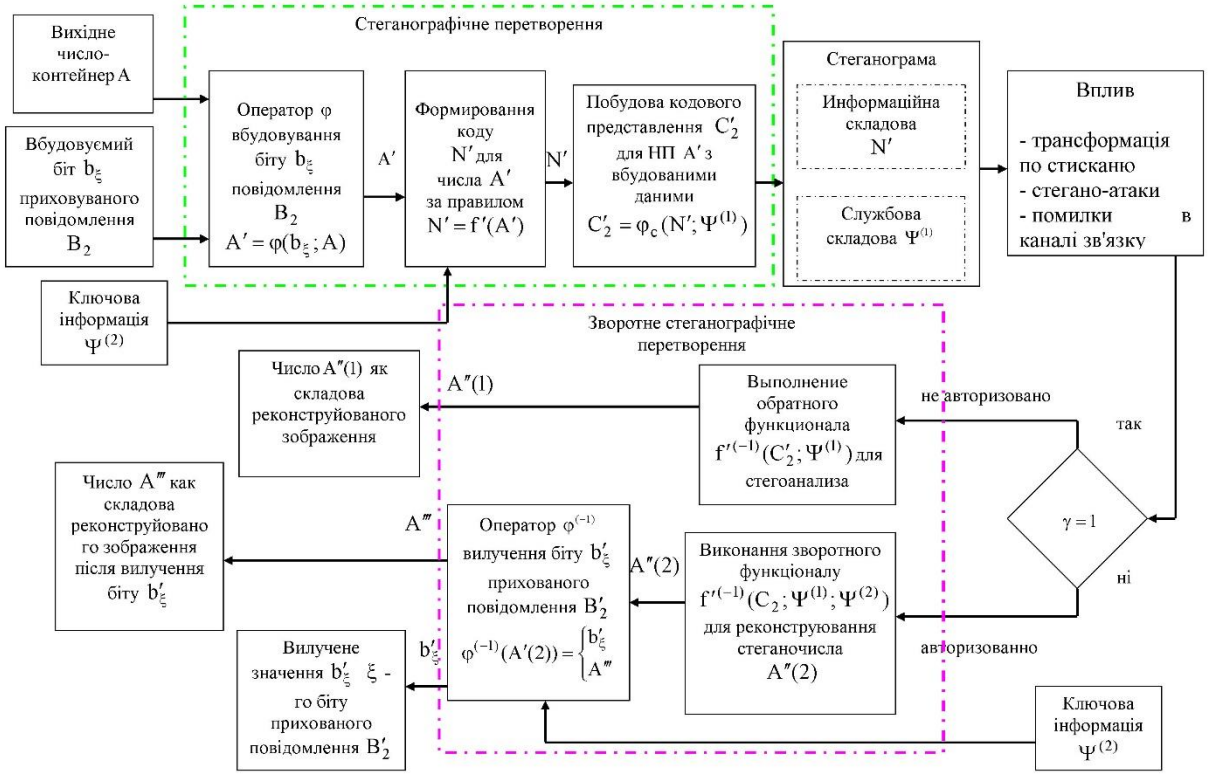

Рисунок 3.4 - Схема стеганографічного перетворення на основі нерівновагового позиційного кодування

Зворотнє стеганографічне перетворення включає випадок для неавторизованого користувача (стеганографічний аналіз) за умови, що йому відомий зворотній функціонал $f'^{(-1)}$. При стеганографічному аналізі, за правилом $f'^{(-1)}(\bullet)$ формується число, записуване як:

$$A''(1) = f'^{(-1)}(C_2'; \Psi^{(1)}).$$

Тут $A''(1)$ - число, як складова зображення, що реконструюється, отримане в результаті стегоаналізу.

Для авторизованого користувача зворотнє стеганографічне перетворення відбувається в два етапи. На першому етапі за правилом $f'^{(-1)}(\bullet)$ і з врахуванням ключової інформації $\Psi^{(2)}$ відбувається реконструкція числа з вбудованими даними. Це задається таким співвідношенням:

$$A''(2) = f'^{(-1)}(C_2'; \Psi^{(1)}; \Psi^{(2)}).$$

На другому етапі з реконструйованого числа $A''(2)$ відбувається вилучення b_ξ' приховуваного повідомлення B_2. Внаслідок застосування оператора вилучення $\varphi'^{(1)}$ також відбувається реконструкція числа A'', як складового вихідного зображення, що описується виразом

$$\varphi'^{(1)}(A'(2)) = \begin{cases} b_\xi', & \Psi = \Psi^{(2)}; \\ A''', & \Psi = \Psi^{(2)}. \end{cases}.$$

Таким чином, розроблений підхід для проектування стенографічної системи заснований на використанні функціонального перетворення для чисел з вбудованою інформацією.

4 РОЗРОБКА МЕТОДУ СТРУКТУРНО-КОМБІНАТОРНОГО СТЕГАНОГРАФІЧНОГО КОДУВАННЯ

4.1 Розробка концепції стеганографічного кодування нерівновагового числа з імплантованим елементом

Для реалізації виявленої потенційної можливості відносно вбудовування інформації на основі структурно-комбінаторних характеристик пропонується підхід у вигляді формування стеганокоду для числа з імплантованими даними в нерівноваговому позиційному базисі.

Імплантацію в число $A(j)$ пропонується проводити поелементно, тобто один елемент b_ξ на позицію γ-го розряду числа $A(j)$. Тут b_ξ - ξ-й елемент вбудовуваної послідовності $B = \{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0; 255]$, $\xi = \overline{1, \nu}$. В цьому випадку імплантація визначається по наступній формулі :

$A(j)' = A(j)$ Y b_ξ, у разі коли $b_\xi = a'_{\gamma, j}$.

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

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

де $A(j)'$ - число з імплантованим елементом $a'_{\gamma, j}$ в γ -й розряд числа;

$(m+1)$ - кількість елементів в числі з імплантацією.

На наступному етапі число $A(j)'$ з імплантованим елементом кодується. На цьому етапі проводиться вбудовування приховуваної інформації в код-контейнер. У зв'язку з чим, сформулюємо наступне визначення.

Визначення. Процес одночасного вбудовування інформації і побудови

кода-контейнера, тобто коли вбудовування інформації здійснюється в процесі формування кода-контейнера, називається стеганографічним кодуванням.

Визначення. Значення кода-контейнера, що містить приховувану інформацію, називається стеганокодом.

Визначення. Формування стеганокоду на основі кодування нерівновагового позиційного числа з імплантованим елементом приховуваного повідомлення називається структурно-комбінаторним стеганографічним кодуванням в нерівноваговому позиційному базисі.

Значення стеганокода $N(j)'$ для нерівновагового позиційного числа з імплантацією визначається по наступній формулі:

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}) .$$

Тут $V^{(2)}$ - ваговий коефіцієнт імплантованого елементу $a'_{\gamma,j}$.

В разі такого вбудовування фрагмент вихідної відеопослідовності розглядається, як позиційне число $A(j)' = \{ a_{1,j}; ...; a'_{\gamma,j}; ...; a_{i,j}; ...; a_{m+1,j} \}$ з імплантованим елементом $a'_{\gamma,j}$, $i = \overline{1, m+1}$. Для числа $A(j)'$ кодове представлення $C(A(j)')$ його стеганокоду $N(j)'$ в нерівноваговому позиційному базисі формується в два етапи (рис 4.1).

Перший етап включає обчислення значення стеганокода $N(j)'$, як зваженого сумування величин $a_{i,j} V'_{i,j}$ і величини $a'_{\gamma,j} V'_{\gamma,j}$. Кодограма $C(A(j)')$ стеганокода формується на другому етапі для значення величини $N(j)'$:

$$C(A(j))' = \{c_1, ..., c_\tau, ..., c_{q(j)'}\},$$

де $q(j)'$ - довжина кодограми $C(A(j)')$.

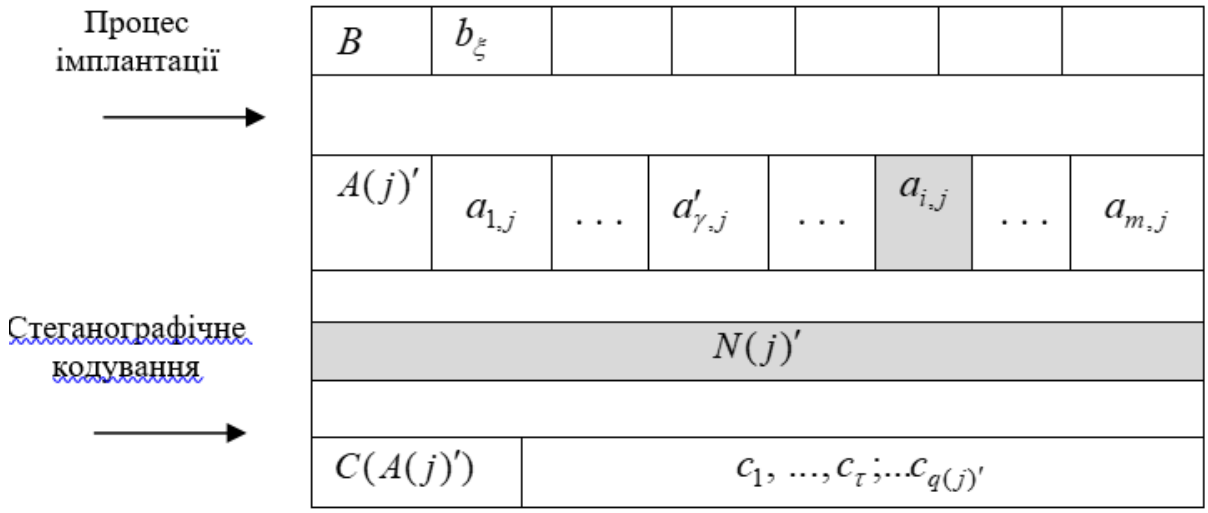

Рисунок. 4.1 - Структурна схема побудови кодограми стеганокоду для числа $A'(j)$ з імплантацією

В результаті стеганографічного кодування формуються кодові комбінації, що складаються з двох частин: службової $\Psi^{(1)}$ і інформаційної $N(j)'$ (значення стеганокоду). У зв'язку з чим сформулюємо наступне визначення:

Визначення. Кодову комбінацію, яка містить службову частину $\Psi^{(1)}$ (система основ) і інформаційну частину (кодове представлення стеганокоду $N(j)'$) називатимемо стеганограмою.

Значить, вбудовування елементу в нерівновагове позиційне число здійснюється внаслідок кодування в два етапи. На першому етапі для НПЧ з імплантацією формується стеганокод. Другий етап передбачає формування кодограми для значення стеганокоду. В результаті стеганографічного перетворення формується стеганограма, що містить службову і інформаційну частини.

4.2 Розробка стеганографічної системи з маскуванням структурної стеганографічної надлишковості

Розглянемо процес стеганографічного кодування. Даний етап включає наступні дії:

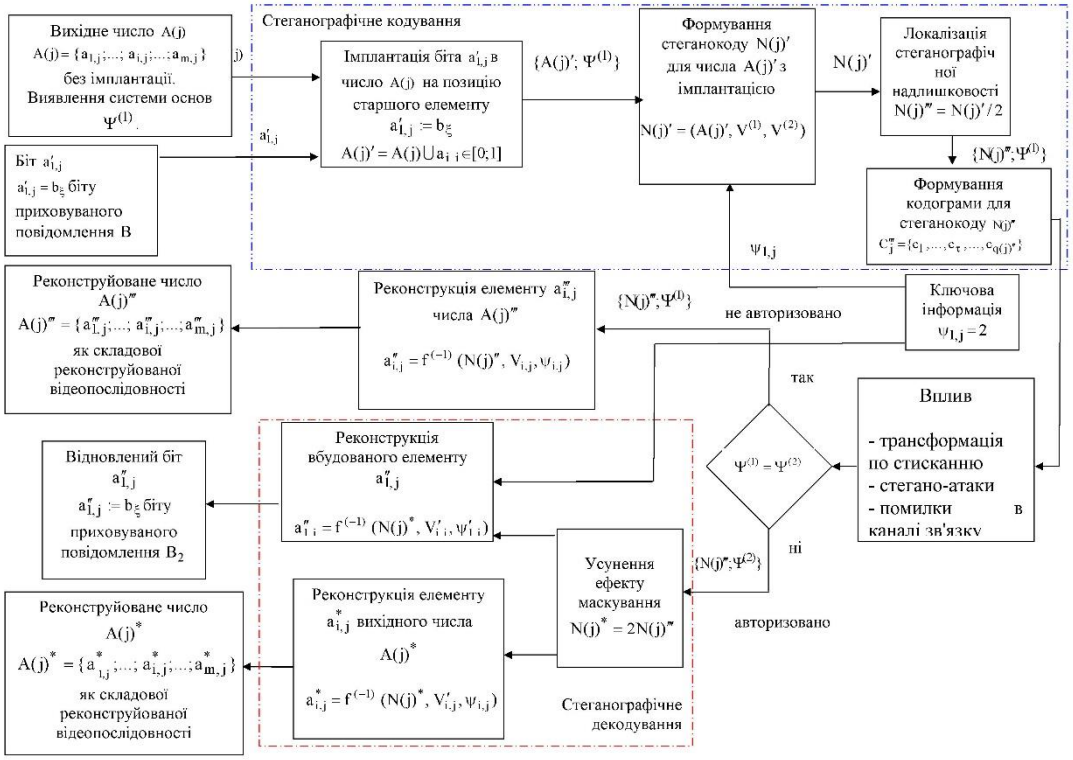

Рисунок 4.2 - Структурна схема стеганографічної системи на основі імплантації приховуваного двійкового елементу на старшу позицію НПЧ з подальшим кодуванням і маскуванням

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

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

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

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

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

2. Формування стеганокоду $N(j)'$ для числа $A(j)'$ з імплантованим елементом $a'_{1,j}$. Враховуючи механізм локалізації кількості структурної стеганографічної надлишковості, вираз для формування стеганокоду $N(j)'$ матиме вигляд:

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}).$$

3. Маскування структурної стеганографічної надлишковості. Здійснення такого маскування відбувається шляхом корекції стеганокоду $N'(j)$, а саме зменшенням довжини його двійкового представлення на один біт. Для отримання значення скоректованого стеганокоду $N(j)''$ використовується наступний вираз:

$$N(j)'' = N(j)'/2.$$

На рис 4.3 схематично відображені етапи стеганографічного кодування.

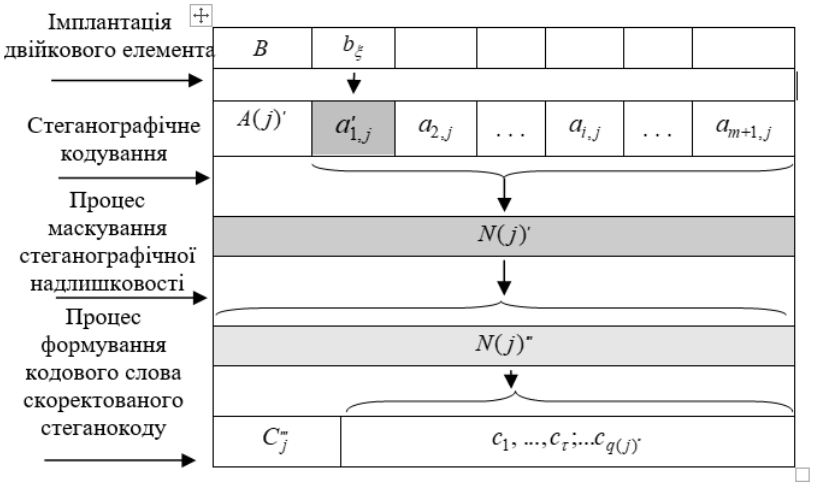

Рисунок 4.3 - Структурна схема побудови кодограми скоректованого

стеганокоду для числа $A'(j)$ з імплантацією

4. Формування кодограми C_j''' для кодового представлення скоректованого стеганокоду $N(j)'''$:

$$C_j''' = \{c_1, ..., c_\tau, ..., c_{q(j)''}\},$$

де $q(j)''$ - довжина кодограми C_j''' рівна $q(j)'' = [(\lambda og_2 \psi'_{\gamma,j} + \lambda og_2 (f_{осн}(\Psi^{(1)})))/2] + 1$.

Тепер необхідно розглянути другу базову складову розробленої стеганографічної системи - стеганографічне декодування.

4.3 Розробка структурно-комбінаторного демаскуючого декодування

Розглянемо процес вилучення даних, що містяться в стеганограмі. Для цього введемо наступне визначення.

Визначення. Процес вилучення приховуваної інформації, здійснюваний одночасно з процесом реконструкції кода-контейнера, називається стеганографічним декодуванням.

Визначення. Процес одночасного вилучення приховуваної інформації і відновлення нерівновагового позиційного числа на основі реконструкції стеганокоду називається структурно-комбінаторним стеганографічним декодуванням в нерівноваговому позиційному базисі.

Процес стеганографічного декодування в даному випадку здійснюється за біполярним принципом для авторизованого користувача і зловмисника (неавторизований користувач).

В разі неавторизованого доступу, коли у зловмисника немає інформації про позицію стеганокоду в стислому представленні зображення і позиції вбудованого елементу, процес декодування здійснюється на основі наступних

етапів:

1. Вилучення з кодограми C_j''' скоректованого стеганокоду $N(j)''$ за допомогою системи основ $\Psi^{(1)}$.

2. Відновлення елементів вихідної відеопослідовності по формулі:

$$a_{i,j}''' = f^{(-1)}(N(j)''', V_{i,j}, \psi_{i.j}),$$

де $a_{i,j}'''$ - i-й елемент реконструйованого числа $A(j)''$, як складової реконструйованої j-ій відеопослідовності, при неавторизованому доступі.

3. Оцінка якості візуального сприйняття зображення, що реконструюється, тобто проведення атаки відносно факту наявності вбудованої інформації.

Навпаки, коли проводиться стеганографічне декодування авторизованим користувачем, то йому доступна наступна інформація:

1) позиція стеганокоду в стисненому представленні зображення;

2) позиція вбудованого елементу $a'_{1,j}$;

3) основа вбудованого елементу $a'_{1,j}$.

В цьому випадку стеганографічне декодування буде містити наступні етапи:

1. Витягання з кодограми C_j''' скоректованого стеганокоду $N(j)''$. Таке витягання здійснюється на основі системи основ $\Psi^{(1)}$, яка міститься в службовій частині стеганограми.

2. Проведення демаскування стеганокоду (усунення ефекту маскування). Для цього введемо наступне визначення.

Визначення. Стеганографічне декодування з врахуванням демаскованої структурної стеганографічної надлишковості називатимемо демаскуючим стеганографічним декодуванням.

Для цього до двійкового представлення стеганокоду $N(j)''$, вилученого з кодограми C_j''' добавляється один біт, рівний нулю. Значення відновленого

стеганокоду $N(j)^*$ визначається по формулі:

$$N(j)^* = N(j)''' * 2$$

3. Відновлення вбудованого елементу $a'_{1,j}$. Даний етап реалізується на основі інформації про позицію стеганокоду в стисненому зображенні, про позицію вбудованого елементу і його основи $\psi'_{1,j} = 2$. Для цього використовується наступна формула:

$$a''_{1,j} = f^{(-1)}(N(j)^*, V_{1,j}, \psi'_{1,j}).$$

Тут $a''_{1,j}$ - значення вилученого біта вбудованої інформації $b_\xi := a''_{i,j}$.

4. Відновлення інших елементів $a^*_{i,j}$ вихідної відеопослідовності проводиться на основі використання системи основ $\Psi_j^{(1)}$. При цьому застосовується вираз:

$$a^*_{i,j} = [N(j)^* / V'_{i,j}] - [N(j)^* / (\psi_{i,j} V'_{i,j})] \psi_{i,j},$$

де $a^*_{i,j}$ - i-й елемент числа $A(j)^*$, як складової реконструйованої вихідної j - ої відеопослідовності, при авторизованому доступі.

ВИСНОВКИ

1. Обгрунтований підхід на основі нерівновагового позиційного кодування, де як елемент-контейнер пропонується використовувати нерівновагове позиційне число, а як функціональне перетворення використовується кодоутворююча функція для нерівновагового позиційного числа. При такому підході передбачається вбудовування біта секретного повідомлення у вихідне нерівновагове позиційне число. В результаті застосування прямого функціонального перетворення для вихідного числа з вбудованою інформацією формується результуюче кодове представлення. Зворотнє функціональне перетворення здійснюватиметься для зловмисника (неавторизований доступ) і для авторизованого користувача. При першому способі реконструкція елементу вихідного зображення реалізується неавторизованим користувачем з врахуванням відкритої службової інформації. Другий спосіб дозволяє, за наявності службової інформації і закритого ключа, вилучити біт вбудованих даних і безпомилково реконструювати вихідний елемент зображення-контейнера.

2. Розроблена стеганографічна система на основі прямого і зворотнього функціонального перетворення для нерівновагового позиційного числа з імплантованим елементом, що забезпечує вбудовування і вилучення приховуваної інформації на основі відповідного структурно-комбінаторного стеганографічного кодування і декодування.

3. Розроблено структурно-комбінаторне стеганографічне кодування з маскуванням, що базується на наступних етапах:

- формування нерівновагового позиційного базису для фрагмента зображення;

- структурно-комбінаторне стеганографічне кодування в нерівноваговому базисі основ;

- маскування структурної стеганографічної надлишковості шляхом її

локалізації на основі корекції довжини стеганограми.

4. Створено правило вбудовування інформації для структурно-комбінаторного стеганографічного кодування, яке полягає в тому, що:

1) один біт приховуваного повідомлення вбудовується на старшу позицію нерівновагового позиційного числа;

2) локалізація стеганографічної надлишковості досягається на основі відсікання молодшого біта стеганограми.

На основі правила побудовано маскуюче стеганографічне кодування для вбудовування одного біта на старшу позицію нерівновагового позиційного числа. Це забезпечує вбудовування приховуваної інформації в умовах:

1) підвищення стійкості приховуваної інформації;

2) забезпечення відновлення елементів вихідної відеопослідовності незалежно від наявності вбудованої інформації;

3) зниження кількості структурної стеганографічної надлишковості.

5. Розроблено демаскуюче стеганографічне декодування для витягання імплантованого на старшу позицію біта з одночасною реконструкцією елементів вихідного нерівновагового позиційного числа. Механізм демаскуючого стеганографічного декодування передбачає:

1) відновлення вихідної довжини для скоректованого в процесі маскування стеганокоду;

2) структурно-комбінаторне стеганографічне декодування, що забезпечує відновлення нерівновагового позиційного числа з імплантованим елементом;

3) вилучення елементу приховуваного повідомлення із старшої позиції нерівновагового позиційного числа.

Наукова новизна обумовлена рішенням науково-прикладного завдання підвищення безпеки спеціальних інформаційних ресурсів на основі використання технології структурно-комбінаторного стеганографічного кодування.

Наукова новизна результатів досліджень полягає в тому, що:

1. Вперше розроблена стеганографічна система на основі безпосереднього вбудовування приховуваної інформації у відеопослідовність. На відміну від інших стеганосистем забезпечується одночасне вбудовування і витягання прихованої інформації відповідно в процесі формування і реконструкції кода-контейнера в базисі основ нерівновагового позиційного числа. Це забезпечує вбудовування прихованої інформації на основі обліку кількості структурно-комбінаторної надлишковості фрагментів відеозображень.

2. Вперше розроблений метод структурно-комбінаторного стеганографічного кодування з маскуванням. На відміну від інших методів забезпечується вбудовування приховуваної інформації в процесі нерівновагового позиційного кодування з подальшою локалізацією стеганографічної надлишковості. Це дозволяє знизити можливість виявлення зловмисником факту наявності вбудованої інформації.

3. Вперше розроблено метод демаскуючого стеганографічного декодування. На відміну від існуючих методів витягання прихованої інформації і відновлення нерівновагового позиційного числа проводиться на основі реконструкції стеганокоду за біполярним принципом з демаскуванням стеганографічної надлишковості. Це дозволяє підвищити ефективність витягання приховуваної інформації і локалізувати атаки зловмисника на виявлення факту наявності прихованої інформації.

4. Отримали подальше удосконалення методів підвищення безпеки державної інформації на основі застосування стеганографічних систем. На відміну від інших систем використовується структурно-комбінаторне стеганографічне маскуюче і демаскуюче перетворення. Це дозволяє підвищити скритність і цілісність вбудованої інформації.

Новизна отриманих результатів підтверджується відсутністю розроблених методів в існуючих стандартах цифрової обробки зображень і стеганографічного кодування.

Основні практичні результати полягають в тому, що:

Розроблений метод підвищення безпеки спеціальних інформаційних ресурсів в системах кризового призначення на основі структурно-комбінаторного стеганографічного кодування, доведений до програмно – апаратних реалізацій. На основі чого отримані такі результати:

1. Проведений порівняльний аналіз значень відносної стеганографічної ємкості розробленого методу відносно методів найменш значимого біта і розширення спектру показав, що:

1) при однакових значення стеганографічної ємкості виграш для розробленого методу відносно методу НЗБ по величині пікового відношення сигнал шум складає в середньому від 8 до 20 дБ.

2) для розробленого методу виграш в значенні стеганографічної ємкості відносно методу РС складає від 1,22 до 5,47 %.

2. Оцінка характеристик приховання вбудованих повідомлень в разі неавторизованого доступу дозволяє зробити висновок, що величина ПВСШ для всіх типів зображення набуває максимального значення в разі вбудовування в нерівновагове позиційне число довжиною $m = 2$. При цьому виграш в значенні ПВСШ відносно вбудовування в НПЧ з довжиною $m = 2; 3; 4; 6$ буде рівний:

- для сильно насиченого зображення «Знімок аеропорту» від 2,725 дБ до 4,86 дБ;

- для середньо насиченого зображення «Фотознімок» від 2,71 до 4,79 дБ;

- для слабо насиченого зображення «Літак на фоні неба» від 2,85 до 4,79дБ.

3. Проведений порівняльний аналіз розробленого методу відносно методів НЗБ і РС по ймовірності безпомилкового вилучення вбудованих даних показав, що виграш в значенні ймовірності безпомилкового вилучення відносно методів найменш значимого біта і розширення спектру складає:

- для методу НЗБ - 40 %;

- для методу РС - 50 %.

4. Оцінка стійкості приховуваних повідомлень до атак зловмисника дозволяє зробити висновок, що для різних значень коефіцієнта квантування найбільшою стійкістю володіють дані, стеганографічно вбудовані в нерівновагове позиційне число довжиною $m = 6$. Навпаки найменшою стійкістю володіють дані стеганографічно вбудовані в НПЧ довжиною $m = 2$. При цьому виграш для розробленого методу відносно методів РС і НЗБ по кількості безпомилково вилучених даних складає:

- відносно методу НЗБ- 40 %;
- відносно методу РС – 40%.

5.Оцінка стеганографічного бітрейта розробленого методу вбудовування дозволяє зробити висновок, що найбільшого значення стеганографічний бітрейт набуває в разі формування нерівновагових позиційних чисел довжиною $m = 2$ - 1,5 біта на піксель, і навпаки найменше значення пропускної спроможності спостерігається для нерівновагових позиційних чисел довжиною $m = 6$ - 0,5 біта на піксель. При цьому виграш для розробленого методу відносно існуючих методів складає:

- для методу НЗБ – до 25 %;
- для методу РС – до 25 %.

Отримані наукові результати є внеском у розвиток теорії інформаційної безпеки відносно забезпечення безпеки спеціальних інформаційних ресурсів в кризових системах.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Аграновски А.В. Стеганография, цифровые водяные знаки и стегоанализ [Тест]: учеб. пособие для вузов / А.В. Аграновски, А.В. Балакин, В.Г. Грибунин. – М.:Вузовская книга, 2009. – 220 с.

2. Алфёров А. П. Основы криптографии: учебное пособие / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

3. Андреев А. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 7. – С.19 – 25.

4. Андреев А.. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 8. – С.16 – 22.

5. Анин Б. Защита компьютерной информации / Б.Анин. - СПб.: БХВ-Петербург, 2000. - 384 с.

6. Артехин Б.В. Стеганография / Артехин Б.В. // Журнал «Защита информации. Конфидент». – 1996. - № 4 -

7. Бабенко В. Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький // Системи обробки інформації : зб. наук. праць. – № 9 (107). – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 163–168.

8. Баранник Д.В. Концепция структурного стеганографического кодирования с маскированием / Д.В. Баранник, А.Э. Бекиров // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 4 - 11.

9. Баранник Д.В. Стеганографическая система на основе неравновесного позиционного кодирования / Д.В. Баранник, В.В. Баранник, А.Э. Бекиров // Радіоелектроніка та інформатика. - 2014. - №4. - С. 37 – 46.