УКРАЇНА

(19) UA (11) 105942 (13) C2

(51) МПК (2014.01)
H04L 9/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2012 08110**

(22) Дата подання заявки: **02.07.2012**

(24) Дата, з якої є чинними права на винахід: **10.07.2014**

(41) Публікація відомостей про заявку: **10.01.2014, Бюл.№ 1**

(46) Публікація відомостей про видачу патенту: **10.07.2014, Бюл.№ 13**

(72) Винахідник(и):
Кузнецов Олександр Олександрович (UA),
Смірнов Олексій Анатолійович (UA)

(73) Власник(и):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ,
пр. Леніна, 14, м. Харків, 61166 (UA)

(56) Перелік документів, взятих до уваги експертизою:
US 6557103 B1, Apr. 29, 2003
Lisa M. Marvel, Charles G. Boncelet, Jr.and Charles T. Retter. Spread Spectrum Image Steganography. IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 1999. Знайдено в інтернеті 20.01.2014. < URL: http://ebookbrowsee.net/spread-spectrum-image-steganography-pdf-d307642487
CN 102063907 A, 18.05.2011
EA 007357 b1, 27.10.2006
UA 85189 C2, 12.01.2009
UA 81951 C2, 25.02.2008
RU 2288544 C2, 27.11.2006
RU 2262805 C2, 20.10.2005
RU 2407216 C1, 20.12.2010
Кузнецов А.А., Ботнов А.М., Лаптий П.А. Встраивание информационных данных в неподвижные изображения методом прямого расширения спектра. Прикладная радиоэлектроника, 2010, Том.9 , № 3, 470-478.
Смірнов О.А. Метод стеганографічного приховування та вилучення даних в просторовій області зображень із використанням прямого розширення спектру. Системи обробки інформації, 2012, вип. 3 (101), том. 1 Надійшла до редколегії 27.02.2012 Знайдено в інтернеті 20.01.2014. < URL: http://irbis-nbuv.gov.ua/.../cgiirbis_64.exe
Смирнов А.А. Метод стеганографического встраивания информации в неподвижные изображения с использованием сложных дискретных сигналов и прямого расширения спектра. Науково-технічний журнал «Захист інформації», №4, 2011. Надійшла: 17.12.2011. Знайдено в інтернеті 20.01.2014. < URL: http://ecobio.nau.edu.ua/index.php/ZI/article/viewFile/2051/2042
Смирнов А.А. Наука і техніка Повітряних Сил Збройних Сил України, 2011, № 2. Знайдено в інтернеті 20.01.2014. < URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe
US 6208735 B1, Mar. 27, 2001
Макарчук Ю.В. Система адаптивного стенографического скрытия данных методом замены младших значащих бит. Материалы Международной научно-практической конференции, 6-7 апреля 2010 г., Минск. Знайдено в інтернеті 21.01.2014. < URL: http://elib.bsu.by/handle/123456789/28605

UA 105942 C2

(54) СПОСІБ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ТА ВИЛУЧЕННЯ ДАНИХ В ПРОСТОРОВІЙ ОБЛАСТІ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА ТА ПРИСТРІЙ ДЛЯ ЙОГО РЕАЛІЗАЦІЇ (ВАРІАНТИ)

(57) Реферат:

Група винаходів належить до галузі прихованої передачі цифрової інформації. Спосіб стеганографічного приховування та вилучення даних в просторовій області зображень із використанням прямого розширення спектра, при якому застосовують адаптивне формування дискретних сигналів $\Phi_j = (\varphi_{j_0}, \varphi_{j_1}, ..., \varphi_{j_{n-1}})$, із врахуванням статистичних властивостей даних блоків контейнера C_i, тобто значення коефіцієнта кореляції $\rho(C_i, \Phi_j)$ для всіх $i = 0,...,N-1$ та для всіх

$j = 0,...,M-1$ за модулем не повинно перевищувати деякого наперед визначеного значення ρ_{max} (значення встановленого порога):

$$\left|\rho(C_i,\Phi_j)\right| = \left|\frac{1}{n}\sum_{z=0}^{n-1} C_{iz}\varphi_{j_z}\right| \le \rho_{max}.$$

Для його реалізації запропоновано два варіанти пристрою, а саме - пристрій стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра, який містить п'ять входів, вихід, блок введення інформаційних даних, блок введення ключів шифрування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів перемежування, блок введення контейнерів, блок шифрування, блок перешкодостійкого кодування, генератор псевдовипадкових послідовностей, модулятор, блок перемежування, блок додавання, блок квантування, блок формування та виводу стеганограми, в якому додатково введенний блок відбору псевдовипадкових послідовностей, причому його перший вхід з'єднаний з виходом генератора псевдовипадкових послідовностей, другий вхід з'єднаний з виходом блока введення контейнерів, а вихід з'єднаний з другим входом модулятора. А другий - пристрій для реалізації стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектра, який містить п'ять входів, вихід, блок введення інформаційних даних, блок введення ключів шифрування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів перемежування, блок введення контейнерів, блок шифрування, блок перешкодостійкого кодування, генератор псевдовипадкових послідовностей, модулятор, блок перемежування, блок додавання, блок квантування, блок формування та виводу стеганограми, в якому додатково введенний блок адаптації (запам'ятовуючого пристрою), причому його вхід з'єднаний з виходом блока введення ключів формування псевдовипадкових послідовностей, а вихід з'єднаний з другим входом генератора псевдовипадкових послідовностей. Група винаходів дозволяє значно підвищити достовірність вилучення вбудованих даних.

Фіг. 8

Запропонований винахід належить до галузі скритної передачі цифрової інформації і може бути використаний в засобах стеганографічного приховування даних для розширення їх можливостей.

Відомий спосіб стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра [J.R. Smith and B.O. Comisky. Modulation and information hiding in images. In R. Anderson, editor, Information Hiding, First International Workshop, volume 1174 °F Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996, pages 207-226], який ґрунтується на тому, що на передавальній стороні окремі блоки даних інформаційного повідомлення за допомогою відповідних пристроїв модулюються шумоподібними дискретними сигналами із великою базою. Модульоване інформаційне повідомлення за статистичними властивостями приймає вигляд випадкової послідовності, а за рахунок великої бази дискретних сигналів досягається розширення спектра частот. Отримане модульоване повідомлення за допомогою відповідного пристрою поелементно додається до даних контейнера (даних цифрового зображення в просторовій області) в результаті чого формується стеганограма (заповнений контейнер), яка передається приймальній стороні. На приймальній стороні вилучення блоків інформаційних даних виконується за допомогою кореляційного приймача, який обраховує значення коефіцієнта кореляції заповненого контейнера та відповідних дискретних сигналів, тотожних тим, що застосовувалися на передавальній стороні. Значення вилучених інформаційних даних приймається за допомогою порогового пристрою відповідно до обрахованого коефіцієнта кореляції. Секретний ключ задає правило формування псевдовипадкових послідовностей, які формуються відповідним генератором та використовуються як шумоподібні дискретні сигнали.

Недоліком цього способу є те, що в процесі стеганографічного приховування даних інформаційного повідомлення не враховуються статистичні властивості контейнера, тобто цифрові дані окремих фрагментів просторової області зображення можуть бути корельованими із застосовуваними дискретними сигналами, що призведе до виникнення помилки при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Відомий спосіб стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра [Marvel, L. M, C. G. Boncelet, Jr., and C. T. Retter. Spread Spectrum Image Steganography, IEEE Transactions on Image Processing, Vol 8, No 8, August 1999, pages 1075-1083], який ґрунтується на тому, що на передавальній стороні після шифрування та перешкодостійкого кодування окремі блоки даних Інформаційного повідомлення за допомогою відповідних пристроїв модулюються шумоподібними дискретними сигналами із великою базою. Модульоване інформаційне повідомлення за статистичними властивостями приймає вигляд випадкової послідовності, а за рахунок великої бази дискретних сигналів досягається розширення спектра частот. Отримане модульоване повідомлення подається на пристрій перемежування, на якому елементи за допомогою таємного ключа перемішуються за відповідним правилом. Отримані дані за допомогою відповідного пристрою поелементно додаються до даних контейнера (даних цифрового зображення в просторовій області). Отримані дані подаються на пристрій квантування, який виконує певне перетворення для зберігання початкового динамічного діапазону зображення-контейнера, в результаті чого формується стеганограма (заповнений контейнер), яка передається приймальній стороні. На приймальній стороні отримана стеганограма після фільтрації подається на пристрій зворотного перемежування, на якому елементи за допомогою таємного ключа перемішуються за правилом, яке інверсне правилу перемежування на передавальній стороні. Вилучення блоків інформаційних даних виконується за допомогою кореляційного приймача, який обраховує значення коефіцієнта кореляції отриманих після зворотного перемежування даних та відповідних дискретних сигналів, тотожних тим, що застосовувалися на передавальній стороні. Значення вилучених даних приймається за допомогою порогового пристрою відповідно до обрахованого коефіцієнта кореляції. В результаті чого після перешкодостійкого декодування та розшифрування формуються інформаційні повідомлення. Секретний ключ задає правило формування псевдовипадкових послідовностей, які формуються відповідним генератором та використовуються як шумоподібні дискретні сигнали.

Застосування пристроїв шифрування та перемежування у процесі приховування та вилучення даних дозволяє покращити статистичні властивості модульованого повідомлення, тобто наблизити його вигляд до випадкової послідовності. Застосування пристроїв перешкодостійкого кодування дозволяє підвищити достовірність передачі інформаційних повідомлень під час стегано графічних перетворень.

Недоліком цього способу є те, що в процесі стеганографічного приховування даних інформаційного повідомлення не враховуються статистичні властивості контейнера, тобто

цифрові дані окремих фрагментів просторової області зображення можуть бути корельованими із застосовуваними дискретними сигналами, що призведе до виникнення помилки при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Найбільш близьким до запропонованого технічного рішення є спосіб стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра [Patent No.: US 6,557,103 B1, Int.C1. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.C1. G06F 11/30. - № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003J, який ґрунтується на тому, що на передавальній стороні після шифрування та перешкодостійкого кодування окремі блоки $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{k-1}})$, $i = 0,...,N-1$ даних інформаційного повідомлення $m = (m_0, m_1, ..., m_{N-1})$ за допомогою відповідних пристроїв модулюються шумоподібними дискретними сигналами

$$\Phi_i = (\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}), \quad \Phi_i \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}, \; k \le M,$$

із базою $B = TF$, де T - тривалість елемента сигналу φ_{i_j}, F - смуга частот сигналу Φ_i. Оскільки $F = n\frac{1}{T}$ маємо $B = n >> 1$ і база сигналу задає кратність розширення смуги частот сигналу Φ_i по відношенню до елементарних сигналів φ_{i_j} та/або m_{i_j}.

В результаті для кожного інформаційного блока τ_i формується блок модульованого інформаційного сигналу

$$E_i = \sum_{j=0}^{k-1} m*_{i_j} \Phi_j = \left(\sum_{j=0}^{k-1} m*_{i_j} \varphi_{j_0}, \sum_{j=0}^{k-1} m*_{i_j} \varphi_{j_1}, ..., \sum_{j=0}^{k-1} m*_{i_j} \varphi_{j_{n-1}} \right), \quad (1)$$

де

$$m*_{i_j} = \begin{cases} +1, m_{i_j} = 1; \\ -1, m_{i_j} = 0; \end{cases};$$

який за статистичними властивостями приймає вигляд випадкової послідовності, а за рахунок великої бази дискретних сигналів досягається розширення спектра частот в $B = n$ разів.

Отримане модульоване повідомлення E_i подається на пристрій перемежування, на якому елементи E_i - за допомогою таємного ключа K_1 перемішуються за відповідним правилом f. Отримані дані $\overline{E_i} = f(E_i, K_1)$ за допомогою відповідного пристрою поелементно додаються до даних контейнера C_i (даних цифрового зображення в просторовій області) за правилом:

$$S_i = C_i + \overline{E_i} \cdot G,$$

де $G > 0$ - коефіцієнт підсилення розширювального сигналу, який задає "енергію" вбудованих блоків інформаційного повідомлення.

Отримані дані S_i подаються на пристрій квантування, який виконує певне перетворення для зберігання початкового динамічного діапазону зображення-контейнера, в результаті чого формуються окремі блоки стеганограма $\overline{S_i}$ та заповнений контейнер $\overline{S} = \overline{S_0} \cup \overline{S_1} \cup ... \cup \overline{S_{N-1}}$, який передається приймальній стороні.

На приймальній стороні отримані блоки стеганограми $\overline{S_i}$ після фільтрації подаються на пристрій зворотного перемежування, на якому елементи відфільтрованих блоків стегенограми $\overline{\overline{S_i}}$ за допомогою таємного ключа перемішуються за правилом f^{-1}, яке інверсне правилу перемежування f на передавальній стороні. Вилучення блоків інформаційних даних виконується за допомогою кореляційного приймача, який обраховує значення коефіцієнта кореляції отриманих після зворотного перемежування даних $S*_i = f^{-1}(\overline{\overline{S_i}}, K_1)$ та відповідних дискретних сигналів Φ_j тотожних тим, що застосовувалися на передавальній стороні:

$$\rho(S*_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} S*_{i_z} \varphi_{j_z} \approx G \cdot \frac{1}{n} \sum_{z=0}^{n-1} E_{i_z} \varphi_{j_z} + \frac{1}{n} \sum_{z=0}^{n-1} C_{i_z} \varphi_{j_z} \quad (2)$$

Припустимо, що масив даних блока контейнера C_i має випадкову статистичну структуру, тобто покладемо, що другий доданок в правій частині виразу (2) близький до нуля і ним можна знехтувати. Тоді маємо:

$$\rho(S*_i,\Phi_j)\approx G\cdot\frac{1}{n}\sum_{z=0}^{n-1}E_{iz}\varphi_{j_z}=G\cdot\frac{1}{n}\sum_{z=0}^{n-1}\left(\sum_{u=0}^{k-1}m*_{i_u}\varphi_{u_z}\right)\varphi_{j_z}= \quad (3)$$

$$G\cdot\sum_{u=0}^{k-1}m*_{i_u}\sum_{z=0}^{n-1}\varphi_{uz}\varphi_{j_z}=G\cdot\sum_{u=0}^{k-1}m*_{i_u}\rho(\Phi_u,\Phi_j).$$

Оскільки всі послідовності із множини Ф формуються за допомогою генератора псевдовипадкових послідовностей, Ініційованого таємним ключем K_2, відповідні дискретні сигнали є слабокорельованими, тобто при $u\neq j$ маємо $\rho(\Phi_u,\Phi_j)\approx 0$. Відповідно до цього всіма доданками, окрім випадку $u=j$, в правій частині рівняння (3) можна знехтувати. Звідки маємо:

$$\rho(S*_i,\Phi_j)\approx G\cdot m*_{i_j}\cdot\frac{1}{n}\sum_{z=0}^{n-1}(\varphi_{j_z})^2=G\cdot m*_{i_j}=\begin{cases}+G;\\-G.\end{cases} \quad (4)$$

Відповідне значення вилучених даних приймається за допомогою порогового пристрою відповідно до обрахованого коефіцієнта кореляції. Оскільки G>0 і n>0 знак $\rho(S*_i,\Phi_j)$ в (4) залежить тільки від $m*_{i_j}$, звідки маємо:

$$m*_{i_j}=\operatorname{sign}(\rho(S*_i,\Phi_j))=\begin{cases}-1,\rho(S_i,\Phi_j)<0;\\+1,\rho(S_i,\Phi_j)>0.\end{cases} \quad (5)$$

Якщо $\rho(S*_i,\Phi_j)=0$ в (5) будемо вважати, що вбудована інформація була втрачена (стерта).

З вилучених даних на приймальній стороні формуються окремі блоки даних $m_i=(m_{i_0},m_{i_1},...,m_{i_{k-1}})$, $i=0,...,N-1$ інформаційного повідомлення $m=(m_0,m_1,...,m_{N-1})$, де

$$m_{i_j}=\begin{cases}1,m*_{i_j}=+1;\\0,m*_{i_j}=-1;\end{cases};$$

з яких після перешкодостійкого декодування та розшифрування вилучених даних формуються інформаційні повідомлення. Секретний ключ K_2 задає правило формування псевдовипадкових послідовностей $\Phi_i=(\varphi_{i_0},\varphi_{i_1},...,\varphi_{i_{n-1}})$, які формуються відповідним генератором та використовуються як шумоподібні дискретні сигнали $\Phi_i\in\Phi=\{\Phi_0,\Phi_1,...,\Phi_{M-1}\}$ з ансамблю Ф потужності М. Правило шифрування та розшифрування на передавальній та приймальній стороні ініціюється секретним ключем K_3.

Застосування пристроїв шифрування та перемежування у процесі приховування та вилучення даних дозволяє покращити статистичні властивості модульованого повідомлення E_i тобто наблизити його вигляд до випадкової послідовності. Застосування пристроїв перешкодостійкого кодування дозволяє підвищити достовірність передачі інформаційних повідомлень $m=(m_0,m_1,...,m_{N-1})$ під час стеганографічних перетворень.

Недоліком способу-прототипу є те, що в процесі стеганографічного приховування даних інформаційного повідомлення не враховуються статистичні властивості блоків контейнера C_i, тобто цифрові дані окремих фрагментів просторової області зображення можуть бути корельованими із застосовуваними дискретними сигналами, що призведе до виникнення помилки при вилученні відповідних блоків інформаційних даних на приймальній стороні. Так, наприклад, якщо коефіцієнт кореляції і-го блока C_i контейнера буде вищий за модулем та протилежний за знаком значенню $G\cdot m*_{i_j}$, тобто, коли другий доданок в правій частині виразу (2) буде перевищувати за модулем та протилежним за знаком першому доданку (та виконуватиметься умова взаємної ортогональності застосовуваних дискретних сигналів), гарантовано відбудеться помилка при вилученні даних за правилом (5). На практиці, як довели проведені авторами дослідження, такі випадки відбуваються дуже часто. Це пов'язане з тим, що цифрові дані просторової області реальних зображень, використовуваних під час стеганографічного приховування інформаційних повідомлень, не мають випадкової статистичної структури, тобто застосовуване припущення при переході від формули (2) до

формули (3) на практиці не виконується і є хибним. Зазвичай при стеганографічному приховуванні застосовуються реалістичні зображення і відповідні цифрові дані у просторовій області зображень не є реалізацією випадкового процесу і навіть за своїми статистичними властивостями не подібні до псевдовипадкових послідовностей. Відповідні значення коефіцієнта кореляції

$$\rho(C_i,\Phi_j)=\frac{1}{n}\sum_{z=0}^{n-1}C_{iz}\varphi_{j_z}\neq 0$$

і можуть приймати великі за амплітудою ($\left|\rho\left(C_i,\Phi_j\right)\right|>>1$) та випадкові за знаком величини. Збільшити у цьому випадку достовірність вилучених даних можливо тільки застосувавши низькошвидкісні перешкодостійкі коди (як у розглянутому способі-прототипі), що призводить до зниження відносної швидкості передачі інформації, або підвищивши коефіцієнт підсилення G, що призводить до збільшення внесених похибок.

Для підтвердження цього факту на фіг. 1 наведено емпіричні оцінки залежності ймовірності помилкового вилучення окремих бітів даних із просторової області зображень за допомогою розглянутого способу-прототипу (переривчата лінія). При цьому застосовувався коефіцієнт підсилення G=4, а кількість бітів k, вбудованих в один блок C_i контейнера змінювалася від 1 до 255. На фіг. 2 наведено емпіричні оцінки залежності середньої долі внесених похибок (відносно до динамічного діапазону в 256 рівнів) в просторову область контейнера-зображення відносно від кількості бітів, вбудованих в один елемент контейнера. З наведених залежностей (фіг 1, 2 переривчаста лінія) видно, що при внесенні похибок в просторову область контейнера-зображення нижчу за зоровий поріг чуттєвості людини (2-3 %) вдається вбудувати не більше 10 бітів даних в один блок контейнера C_i. Але навіть при такій незначній кількості вбудованих даних ймовірність помилкового вилучення приймає значення 0,05…0,25 що вимагає застосування низькошвидкісних перешкодостійких кодів із здатністю виправляти багатократні помилки.

На фіг. 3, 4 наведено, відповідно, емпіричні оцінки залежності ймовірності помилкового вилучення окремих бітів даних та залежності середньої долі внесених похибок від значень коефіцієнта підсилення G за допомогою розглянутого способу-прототипу (переривчата лінія). При цьому в один блок C_i контейнера вбудовувалося k=4 бітів інформаційних даних, а коефіцієнт підсилення G змінювався від 1 до 8. З наведених залежностей (фіг 3, 4, переривчаста лінія) видно, що при значені коефіцієнта підсилення G>6 вбудовування інформаційних даних в просторову область контейнера-зображення призводить до внесення похибок, доля яких (відносно до динамічного діапазону) перевищує зоровий поріг чуттєвості людини (2-3 %). Тобто факт приховування даних в зображенні виявляється зоровим спостереженням і стеганографічне вбудовування з цими параметрами є недоцільним. Але при значенні коефіцієнта підсилення G≤6 спостерігається велика кількість помилок при вилученні окремих бітів даних із просторової області зображень, відповідна ймовірність помилкового вилучення $P_{ош\geq 0,2}$.

Емпіричні оцінки залежності ймовірності помилкового вилучення окремих бітів даних від середньої долі внесених похибок в контейнер-зображення при зміні кількості бітів, вбудованих в один елемент контейнера (від 1 до 255) або зміні значень коефіцієнта підсилення розширювального сигналу (від 1 до 8) наведено, відповідно на фіг. 5, 6. У першому випадку (фіг. 5) наведені залежності побудовані відповідно до фіксованого значення коефіцієнта підсилення G-4, в другому випадку (фіг. 6) - відповідно до фіксованого значення k=4. З наведених залежностей (переривчата лінія) видно, що практично у всіх випадках при вбудовуванні даних за допомогою способу прототипу спостерігається велика кількість помилок при вилученні окремих бітів даних із просторової області зображень. Навіть при малих значеннях k=12 ймовірність помилкового вилучення даних приймає значення 0,05…0,25 (див. фіг. 7). При k=4 і внесенні похибок в контейнер-зображення, що лежать нижче порога чуттєвості зорової системи людини ймовірність помилкового вилучення даних лежить вище за 0,2.

На фіг. 7 наведено приклади зображень, які застосовувалися при проведенні досліджень: фіг. 7а - вихідне зображення (пустий контейнер); фіг. 7б - зображення із вбудованими повідомленнями за допомогою способу-прототипу (заповнений контейнер); фіг. 7в - зображення із вбудованими повідомленнями за допомогою запропонованого способу (заповнений контейнер). Вбудовування даних виконано з параметрами: G=4, k=4.

В основу винаходу поставлена задача створити спосіб стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра який, за

рахунок врахування статистичних властивостей контейнера C_i дозволить значно підвищити достовірність вилучення вбудованих даних, тобто шляхом введення додаткових обмежень на значення коефіцієнта кореляції використовуваних дискретних сигналів та окремих фрагментів просторової області зображення реалізація винаходу дозволить значно зменшити кількість виникаючих помилок при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Поставлена задача вирішується за рахунок адаптивного формування псевдовипадкових послідовностей $\Phi_j = (\varphi_{j_0}, \varphi_{j_1}, ..., \varphi_{j_{n-1}})$, із врахуванням статистичних властивостей даних блоків контейнера C_i, тобто значення коефіцієнта кореляції $\rho(C_i, \Phi_j)$ для всіх $i = 0,...,N-1$ та для всіх $j = 0,...,M-1$ за модулем не повинно перевищувати деякого наперед визначеного значення ρ_{max} (значення встановленого порога):

$$\left|\rho(C_i, \Phi_j)\right| = \left|\frac{1}{n}\sum_{z=0}^{n-1} C_{iz}\varphi_{j_z}\right| \le \rho_{max}. \qquad (6)$$

Таким чином, формування послідовностей $\Phi_i \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ виконується за псевдовипадковим правилом, яке ініційоване секретним ключем K_2, та із врахуванням накладеної системи обмежень (6) для всіх $i = 0,...,N-1$ та для всіх $j = 0,...,M-1$.

При такому формуванні дискретних сигналів кожна послідовність з ансамблю $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ не буде корельовано (до встановленої межі) з жодним блоком контейнера, і відповідно, коефіцієнт кореляції і-го блока C_i контейнера за модулем ніколи не буде вищий за модулем та протилежним за знаком значенню ρ_{max}. Відповідно до цього (та при виконанні умови взаємної ортогональності застосовуваних дискретних сигналів) другий доданок в правій частині виразу (2) може перевищити за модулем та бути протилежним за знаком першому доданку тільки у випадку, коли $\left|G \cdot m^*_{i_j}\right| < \rho_{max}$. Саме у цьому випадку відбудеться помилка вилучення інформаційних даних, але ймовірність такої події буде значно менша за ймовірність випадку виникнення помилки вилучення даних у способі-прототипі. Якщо значення порога ρ_{max} задати менше, ніж значення коефіцієнта підсилення G, тобто, у випадку, коли виконується нерівність $\left|G \cdot m^*_{i_j}\right| < \rho_{max}$ помилка не відбудеться зовсім, тобто буде досягнута безпомилкова передача прихованої інформації.

Для підтвердження зробленого висновку на фіг. 3-6 суцільною лінією наведено емпіричні оцінки ймовірнісних властивостей стеганографічного приховування даних за допомогою запропонованого способу:

- на фіг. 1 наведено емпіричні оцінки залежності ймовірності помилкового вилучення окремих бітів даних із просторової області зображень при фіксованому коефіцієнті підсилення $G = 4$, та змінній кількості бітів, вбудованих в один елемент контейнера $k = 1,\ldots,255$, які вбудовувалися в один блок C_i контейнера;

- на фіг. 2 наведено емпіричні оцінки залежності середньої долі внесених похибок (відносно до динамічного діапазону в 256 рівнів) в просторову область контейнера-зображення відносно від кількості бітів, вбудованих в один елемент контейнера;

- на фіг. 3 емпіричні оцінки залежності ймовірності помилкового вилучення окремих бітів даних від значень коефіцієнта підсилення, який змінювався в діапазоні $G = 1,\ldots,8$, та при фіксованому значенні кількості бітів, вбудованих в один елемент контейнера $k = 4$;

- на фіг. 4 наведено емпіричні оцінки залежності середньої долі внесених похибок від значень коефіцієнта підсилення, який змінювався в діапазоні $G = 1$, …,8, та при фіксованому значенні кількості бітів, вбудованих в один елемент контейнера $k = 4$;

- на фіг. 5 наведено емпіричні оцінки залежності ймовірності помилкового вилучення окремих бітів даних від середньої долі внесених похибок в контейнер-зображення при зміні кількості бітів, вбудованих в один елемент контейнера $k = 1,\ldots,255$ та при фіксованому коефіцієнті підсилення $G = 4$;

- на фіг. 6 наведено емпіричні оцінки залежності ймовірності помилкового вилучення окремих бітів даних від середньої долі внесених похибок в контейнер-зображення при зміні

коефіцієнта підсилення, який змінювався в діапазоні G=1,…,8, та при фіксованому значенні кількості бітів, вбудованих в один елемент контейнера $k = 4$.

Залежності, які наведено на фіг. 1-6 (суцільна лінія) отримано із використанням адаптованого (до статистичних властивостей контейнера) формування дискретних сигналів, значення встановленого порога дорівнювало $\rho_{max} = 3{,}9$.

З наведених залежностей на фіг. 1, 2 (суцільна лінія) видно, що при внесенні похибок в просторову область контейнера-зображення, нижчу за зоровий поріг чутливості людини (2-3 %) вдається вбудувати не більше 10 бітів даних в один блок контейнера C_i (як і у способі-прототипі). Але при такій кількості вбудованих даних ймовірність помилкового вилучення значно менша за 0,1 та в декілька десятків разів менша, ніж у способі-прототипі.

З наведених залежностей на фіг. 3, 4 (суцільна лінія) видно, що при значені коефіцієнта підсилення G>6 вбудовування інформаційних даних в просторову область контейнера-зображення призводить до внесення похибок, доля яких (відносно до динамічного діапазону) перевищує зоровий поріг чуттєвості людини (2-3 %) так само як і у способі-прототипі. При таких значеннях коефіцієнта С приховування даних в зображенні є недоцільним. При значеннях G≤6 похибки, що вносяться в контейнер-зображення лежать нижче порога зорової чутливості людини, тобто є непомітними. При цьому в порівнянні за способом-прототипом спостерігається суттєве зниження кількості помилок при вилученні окремих бітів даних із просторової області зображень. Крім того, при значенні коефіцієнта підсилення G>4 спостерігається повна відсутність помилок в вилучених даних, що підтверджує зроблений вийде висновок стосовно безпомилкової передачі прихованої інформації.

Дійсно, вже при G=4 виконується нерівність $\left|G \cdot m*_{i_j}\right| > \rho_{max.}$, тобто за умови дійсності припущення щодо взаємної ортогональності застосовуваних дискретних сигналів помилки зовсім не відбуваються і досягається безпомилкова передача прихованої інформації.

З наведених залежностей на фіг. 5, 6 (суцільна лінія) видно, що практично у всіх випадках при вбудовуванні даних запропонованим способом є виграш відносно до способу-прототипу (переривчаста лінія). Так, при збільшенні кількості k бітів, вбудованих в один елемент контейнера, так само як і у способі-прототипі, спостерігається збільшення ймовірності помилкового вилучення даних на приймальні стороні. Одна це збільшення йде значно повільніше, ніж у способі-прототипі. При збільшенні значень коефіцієнта підсилення G спостерігається зменшення ймовірності помилкового вилучення даних, однак запропонований спосіб (суцільна лінія) має значно покращенні ймовірнісні властивості, ніж спосіб-прототип (переривчаста лінія).

Таким чином досягається конкретний технічний результат, а саме: за рахунок врахування статистичних властивостей цифрових даних окремих фрагментів просторової області контейнера-зображення при адаптивному формуванні псевдовипадкових послідовностей (дискретних сигналів) вдається значно зменшити кількість виникнення помилок при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Суть запропонованого способу стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра полягає в тому, що на передавальній стороні після шифрування та перешкодостійкого кодування окремі блоки даних інформаційного повідомлення за допомогою відповідних пристроїв модулюються шумоподібними дискретними сигналами із великою базою. При цьому застосовується адаптивне формування дискретних сигналів із врахуванням статистичних властивостей даних контейнера, тобто значення за модулем коефіцієнта кореляції формованих псевдовипадкових послідовностей та даних контейнера не повинно перевищувати деякого наперед визначеного значення (встановленого порога). Модульоване інформаційне повідомлення за статистичними властивостями приймає, вигляд випадкової послідовності, а за рахунок великої бази дискретних сигналів досягається розширення спектра частот. Отримане модульоване повідомлення подається на пристрій перемежування, на якому елементи за допомогою таємного ключа перемішуються за відповідним правилом. Отримані дані за допомогою відповідного пристрою поелементно додаються до даних контейнера (даних цифрового зображення в просторовій області). Отримані дані подаються на пристрій квантування, який виконує певне перетворення для зберігання початкового динамічного діапазону зображення-контейнера, в результаті чого формується стеганограма (заповнений контейнер), яка передається приймальній стороні. На приймальній стороні отримана стеганограма після фільтрації подається на пристрій зворотного перемежування, на якому елементи за допомогою таємного ключа перемішуються за правилом, яке інверсне правилу перемежування на передавальній стороні. Вилучення блоків інформаційних даних виконується за допомогою кореляційного приймача, який обраховує

значення коефіцієнта кореляції отриманих після зворотного перемежування даних та відповідних дискретних сигналів, тотожних тим, що застосовувалися на передавальній стороні. Значення вилучених даних приймається за допомогою порогового пристрою відповідно до обрахованого коефіцієнта кореляції. В результаті чого після перешкодостійкого декодування та розшифрування формуються інформаційні повідомлення. Секретний ключ задає правило адаптивного формування псевдовипадкових послідовностей, які формуються відповідним генератором та використовуються як шумоподібні дискретні сигнали.

Застосування пристроїв шифрування та перемежування у процесі приховування та вилучення даних дозволяє покращити статистичні властивості модульованого повідомлення, тобто наблизити його вигляд до випадкової послідовності. Застосування пристроїв перешкодостійкого кодування дозволяє підвищити достовірність передачі інформаційних повідомлень під час стеганографічних перетворень. За рахунок адаптивного формування псевдовипадкових послідовностей із врахуванням статистичних властивостей даних контейнера вдається значно зменшити кількість виникнення помилок при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Таким чином, за рахунок адаптивного формування псевдовипадкових послідовностей із врахуванням статистичних властивостей даних контейнера, тобто шляхом введення додаткових обмежень на значення коефіцієнта кореляції використовуваних дискретних сигналів та окремих фрагментів просторової області зображення реалізація винаходу дозволяє значно зменшити кількість виникаючих помилок при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Відомий пристрій для реалізації стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра, який містить п'ять входів, вихід, блок введення інформаційних даних, блок введення ключів шифрування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів перемежування, блок введення контейнерів, блок шифрування, блок перешкодостійкого кодування, генератор псевдовипадкових послідовностей, модулятор, блок перемежування, блок додавання, блок квантування, блок формування та виводу стеганограми [Patent No.: US 6,557,103 B1, Int.C1. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.C1. G06F 11/30. - № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003].

Перший вхід пристрою з'єднаний з входом блока введення інформаційних даних, вихід якого з'єднаний з першим входом блока шифрування. Другий вхід пристрою з'єднаний з входом блока введення ключів шифрування, вихід якого з'єднаний з другим входом блока шифрування. Вихід блока шифрування з'єднаний з входом блока перешкодостійкого кодування, вихід якого з'єднаний з першим входом модулятора. Третій вхід пристрою з'єднаний з входом блока введення ключів формування псевдовипадкових послідовностей, вихід якого з'єднаний з входом генератора псевдовипадкових послідовностей. Вихід генератора псевдовипадкових послідовностей з'єднаний з другим входом модулятора, вихід якого з'єднаний з першим входом блока перемежування. Четвертий вхід пристрою з'єднаний з входом блока введення ключів перемежування, вихід якого з'єднаний з другим входом блока перемежування. Вихід блока перемежування з'єднаний з першим входом блока додавання. П'ятий вхід пристрою з'єднаний з входом блока введення контейнерів, вихід якого з'єднаний з блоком додавання. Вихід блока додавання з'єднаний з входом блока квантування. Вихід блока квантування з'єднаний з входом блока формування та виводу стеганограми, вихід якого з'єднаний з виходом пристрою.

Робота відомого пристрою полягає в наступному. Па перший вхід пристрою вводиться послідовність інформаційних даних, яка за допомогою блока вводу інформаційних даних подається на перший вхід блока шифрування. На другий вхід пристрою подається ключ шифрування, який через блок блока введення ключів шифрування подається на другий вхід блока шифрування. В блока шифрування за правилом, яке Ініційоване введеним ключем шифрування, виконується шифрування для підвищення конфіденційності інформаційних даних. Зашифровані інформаційні дані з виходу блока шифрування подаються на вхід блока перешкодостійкого кодування, в якому виконується внесення спеціально формованої надмірності для підвищення достовірності зашифрованих даних. Отримані дані з виходу блока перешкодостійкого кодування подаються на перший вхід модулятора. На третій вхід пристрою подається ключ формування псевдовипадкових послідовностей, який через блок введення ключів формування псевдовипадкових послідовностей подається на вхід генератора псевдовипадкових послідовностей. Генератор псевдовипадкових послідовностей за правилом, яке ініційоване введеним ключем формування псевдовипадкових послідовностей, формує дискретні сигнали, тобто дискретні послідовності, елементи яких сформовано

псевдовипадковим чином. Сформовані псевдовипадкові послідовності подаються на другий вхід модулятора, в якому подані на перший вхід інформаційні дані модулюються за правилом (1). Сформоване таким чином модульоване повідомлення подається на перший вхід блока перемежування. На четвертий вхід пристрою подається ключ перемежування, який через блок введення ключів перемежування подається на другий вхід блока перемежування та ініціює відповідне правило перемежування. В блока перемежування виконується перемежування поданого на його перший вхід модульованого повідомлення. Отримані дані подаються на блок додавання, у якому виконується поелементне додавання з даними контейнера, які через блок введення контейнерів з п'ятого входу пристрою подаються на другий вхід блока додавання. Отримані дані з виходу блока додавання подаються на вхід блока квантування, який виконує перетворення для зберігання початкового динамічного діапазону зображення-контейнера, в результаті чого формуються окремі блоки стеганограми, що подаються на вхід блока формування та виводу стеганограми. В блока формування та виводу стеганограми завершуються стеганографічна обробка даних шляхом об'єднання окремих блоків стеганограми, формується заповнений контейнер (стеганограма) та подасться на вихід пристрою.

Недоліком відомого пристрою-прототипу є те, що в процесі стеганографічного приховування даних інформаційного повідомлення не враховуються статистичні властивості контейнера, тобто цифрові дан ні окремих фрагментів просторової області зображення можуть бути корельованими із застосовуваними дискретними сигналами, що може призвести до виникнення помилки при вилученні відповідних блоків інформаційних даних на приймальній стороні.

В основу винаходу поставлена задача створити пристрій стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра, який, за рахунок врахування статистичних властивостей контейнера, дозволить значно підвищити достовірність вилучення вбудованих даних, тобто шляхом введення додаткових обмежень на значення коефіцієнта кореляції використовуваних дискретних сигналів та окремих фрагментів просторової області зображення реалізація винаходу дозволить значно зменшити кількість виникаючих помилок при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Поставлена задача вирішується за рахунок того, що в пристрій стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра, який містить п'ять входів, вихід, блок введення інформаційних даних, блок введення ключів шифрування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів перемежування, блок введення контейнерів, блок шифрування, блок перешкодостійкого кодування, генератор псевдовипадкових послідовностей, модулятор, блок перемежування, блок додавання, блок квантування, блок формування та виводу стеган о грами додатково вводиться блок відбору псевдовипадкових послідовностей, причому його перший вхід з'єднаний з виходом генератора псевдовипадкових послідовностей, другий вхід з'єднаний з виходом блока введення контейнерів, а вихід з'єднаний з другим входом модулятора.

Додатково введений блок відбору псевдовипадкових послідовностей реалізується таким чином, щоб значення коефіцієнта кореляції псевдовипадкових послідовностей та блоків даних контейнера не перевищували значення наперед встановленого порога, тобто у цьому блока реалізується правило відбору псевдовипадкових послідовностей за критерієм (6).

Структурна схема запропонованого пристрою стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра зображено на фіг. 8.

Запропонований пристрій містить п'ять входів, вихід, блок введення інформаційних даних, блок введення ключів шифрування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів перемежування, блок введення контейнерів, блок шифрування, блок перешкодостійкого кодування, генератор псевдовипадкових послідовностей, модулятор, блок перемежування, блок додавання, блок квантування, блок формування та виводу стеганограми та додатково введений блок відбору псевдовипадкових послідовностей.

Елементи запропонованого пристрою з'єднанні наступним чином. Перший вхід пристрою з'єднаний з входом блока введення інформаційних даних, вихід якого з'єднаний з першим входом блока шифрування. Другий вхід пристрою з'єднаний з входом блока введення ключів шифрування, вихід якого з'єднаний з другим входом блока шифрування. Вихід блока шифрування з'єднаний з входом блока перешкодостійкого кодування, вихід якого з'єднаний з першим входом модулятора. Третій вхід пристрою з'єднаний з входом блока введення ключів формування псевдовипадкових послідовностей, вихід якого з'єднаний з входом генератора псевдовипадкових послідовностей. Вихід генератора псевдовипадкових послідовностей

з'єднаний з першим входом додатково введеного блока відбору псевдовипадкових послідовностей, вихід якого з'єднаний з другим входом модулятора. Вихід модулятора з'єднаний з першим входом блока перемежування. Четвертий вхід пристрою з'єднаний з входом блока введення ключів перемежування, вихід якого з'єднаний з другим входом блока перемежування. Вихід блока перемежування з'єднаний з першим входом блока додавання. П'ятий вхід пристрою з'єднаний з входом блока введення контейнерів, вихід якого з'єднаний з блоком додавання та другим входом додатково введеного блока відбору псевдовипадкових послідовностей. Вихід блока додавання з'єднаний з входом блока квантування. Вихід блока квантування з'єднаний з входом блока формування та виводу стеганограми, вихід якого з'єднаний з виходом пристрою.

Робота запропонованого пристрою полягає в наступному. На перший вхід пристрою вводиться послідовність інформаційних даних, яка за допомогою блока вводу інформаційних даних подається на перший вхід блока шифрування. На другий вхід пристрою подається ключ K_1 шифрування, який через блок блока введення ключів шифрування подається на другий вхід блока шифрування. В блока шифрування за правилом, яке ініційоване введеним ключем шифрування, виконується шифрування для підвищення конфіденційності Інформаційних даних. Зашифровані інформаційні дані з виходу блока шифрування подаються на вхід блока перешкодостійкого кодування, в якому виконується внесення спеціально формованої надмірності для підвищення достовірності зашифрованих даних. Отримані дані $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{k-1}})$ з виходу блока перешкодостійкого кодування подаються на перший вхід модулятора. На третій вхід пристрою подається ключ K_2 формування псевдовипадкових послідовностей, який через блок введення ключів формування псевдовипадкових послідовностей подається на вхід генератора псевдовипадкових послідовностей. Генератор псевдовипадкових послідовностей за правилом, яке ініційоване введеним ключем K_2 формування псевдовипадкових послідовностей, формує дискретні сигнали Φ_j, тобто дискретні послідовності, елементи яких сформовано псевдовипадковим чином. Сформовані псевдовипадкові послідовності Φ_j подаються на перший вхід додатково введеного блока відбору послідовностей, на другий вхід якого з п'ятого входу пристрою через блок введення контейнерів подаються фрагменти контейнера C_i. В блока відбору послідовностей за правилом (6) для всіх фрагментів контейнера C_i, $i = 0,...,N-1$ розраховується значення коефіцієнта кореляції

$$\rho(C_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} C_{iz} \varphi_{j_z}$$

та порівнюється із наперед визначеним значенням $\rho_{max.}$.

У випадку, коли хоча б для одного $i \in \{0,...,N-1\}$ розраховане значення $\rho(C_i, \Phi_j)$ перевищить значення порога $\rho_{max.}$, сформована псевдовипадкова послідовність бракується, тобто дискретні сигнали Φ_j із $\rho(G \cdot m *_{i_j}) > \rho_{max.}$ хоча б для одного $i \in \{0,...,N-1\}$ для стеганографічного приховування інформаційних даних не застосовуються.

Якщо для сформованого дискретного сигналу Φ_j та для всіх $i = 0,...,N-1$ розраховані значення коефіцієнта кореляції $\rho(C_i, \Phi_j)$ менші або дорівнюють встановленому порогу $\rho_{max.}$, тобто, якщо виконується умова (6) для всіх блоків даних контейнера, відповідне значення Φ_j приймається до подальшого стеганографічного приховування інформаційних даних.

Сформовані таким чином псевдовипадкові послідовності складають ансамбль дискретних сигналів $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$, вони враховують статистичні властивості контейнера та подаються до модулятора. На модулятор подається також блоки інформаційних даних $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{k-1}})$, $k \le M$, в якому вони модулюються за правилом (1).

Сформоване таким чином модульоване повідомлення E_i подається на перший вхід блока перемежування. На четвертий вхід пристрою подається ключ K_3 перемежування, який через блок введення ключів перемежування подається на другий вхід блока перемежування та ініціює відповідне правило перемежування. В блоці перемежування виконується перемежування

поданого на його перший вхід модульованого повідомлення E_i, тобто за правилом f, яке задає таємний ключ K_3, псевдовипадковим чином переставляються місцями елементи E_i.

Отримані дані $\overline{E_i} = f(E_i, K_1)$ подаються на блок додавання, у якому виконується поелементне додавання з фрагментами контейнера C_i (з даними цифрового зображення в просторовій області): $S_i = C_i + \overline{E_i} \cdot G$, де $G > 0$ - коефіцієнт підсилення розширювального сигналу, який задає "енергію" вбудованих блоків інформаційного повідомлення. Окремі фрагменти контейнера C_i через блок введення контейнерів з п'ятого входу пристрою подаються на другий вхід блока додавання.

Отримані дані S_i з виходу блока додавання подаються на вхід блока квантування, який виконує перетворення для зберігання початкового динамічного діапазону зображення-контейнера, в результаті чого формуються окремі блоки стеганограми $\overline{S_i}$, що подається на вхід блока формування та виводу стеганограми. В блока формування та виводу стеганограми завершуються стеганографічна обробка даних шляхом об'єднання окремих блоків стеганограми та заповнений контейнер $\overline{S} = \overline{S_0} \cup \overline{S_1} \cup ... \cup \overline{S_{N-1}}$, формується заповнений контейнер (стеганограма) $\overline{S}$ та подається на вихід пристрою.

Таким чином, в результаті роботи запропонованого пристрою за рахунок додаткового введення блока відбору псевдовипадкових послідовностей, що реалізує правило відбору послідовностей за критерієм (6) Із врахуванням статистичних властивостей контейнера, вдається значно підвищити достовірність вилучення вбудованих даних.

Відомий пристрій для реалізації стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектра, який містить чотири входи, вихід, блок введення та форматування стеганограм, блок введення ключів деперемежування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів розшифрування, блок фільтрації, блок деперемежування, генератор псевдовипадкових послідовностей, демодулятор, блок перешкодостійкого декодування, блок розшифрування, блок формування та виводу інформаційних даних [Patent No.: US 6,557,103 B1, Int.C1. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.C1. G06F 11/30. - № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003].

Перший вхід пристрою з'єднаний з входом блока введення та форматування стеганограми, вихід якого з'єднаний з першим входом блока фільтрації. Вихід блока фільтрації з'єднаний з першим входом блока деперемежування. Другий вхід пристрою з'єднаний з входом блока введення ключів деперемежування, вихід якого з'єднаний з другим входом блока деперемежування. Вихід блока деперемежування з'єднаний з першим входом демодулятора. Третій вхід пристрою з'єднаний з входом блока введення ключів формування псевдовипадкових послідовностей, вихід якого з'єднаний з входом генератора псевдовипадкових послідовностей. Вихід генератора псевдовипадкових послідовностей з'єднаний з другим входом демодулятора, вихід якого з'єднаний з входом блока перешкодостійкого декодування. Вихід блока перешкодостійкого декодування з'єднаний з першим входом блока розшифрування. Четвертий вхід пристрою з'єднаний з входом блока введення ключів розшифрування, вихід якого з'єднаний з другим входом блока розшифрування. Вихід блока розшифрування з'єднаний з входом блока формування та виводу інформаційних даних.

Робота відомого пристрою полягає в наступному. На перший вхід пристрою вводиться стеганограма, яка подається на вхід блока введення та форматування стеганограми, в якому формуються окремі фрагменти (блоки) просторової області стеганозображення, що подаються на вхід пристрою фільтрації. Після фільтрації отримані дані подаються на перший вхід блока де-перемежування, на якому виконується дія, інверсна перемежуванню на передавальній стороні. Блок деперемежування ініційовано ключем деперемежування, який подається на другий вхід пристрою та через блок введення ключів деперемежування подається на другий вхід блока деперемежування. Отримані після деперемежування дані подаються на перший вхід демодулятора, який виконує функцію кореляційного приймача дискретних сигналів за розглянутим вище правилом.

На третій вхід пристрою подається ключ формування псевдовипадкових послідовностей, який через блок введення ключів формування псевдовипадкових послідовностей подається на вхід генератора псевдовипадкових чисел. Генератор псевдовипадкових чисел, що ініційований введеним ключем формування псевдовипадкових послідовностей, формує ансамбль

дискретних сигналів (псевдовипадкових послідовностей), які подаються на другий вхід демодулятора. Послідовності, які надходять до демодулятора з виходу генератора псевдовипадкових послідовностей є тотожними тим, які застосовуються на передавальній стороні при вбудовуванні інформаційних повідомлень.

В демодуляторі обчислюється значення коефіцієнта кореляції між поданими на його перший вхід даними (з виходу блока деперемежування) та послідовностями, які подані на його другий вхід (з виходу генератора псевдовипадкових послідовностей). Рішення, стосовно значення вбудованих даних, приймається відповідно до значення обрахованого коефіцієнта кореляції за правилом (5).

Вилучені дані подаються на вхід блока перешкодостійкого декодування, в якому за визначеним правилом із використанням внесеної надмірності виправляються деякі помилки, відповідно до корегуючої здатності коду. Це призводить до деякого підвищення достовірності переданих даних. Отримані після декодування дані подаються на перший вхід блока розшифрування, ініційованого ключем розшифрування. Ключ розшифрування подається на четвертий вхід пристрою та через блок введення ключів розшифрування подається на другий вхід блока розшифрування. Розшифровані повідомлення подаються на вхід блока форматування та виводу інформаційних даних, в якому завершується формування інформаційних повідомлень, що подаються на вихід пристрою.

Недоліком відомого пристрою-прототипу є те, що в процесі стеганографічного приховування даних інформаційного повідомлення не враховуються статистичні властивості контейнера, тобто цифрові дані окремих фрагментів просторової області зображення можуть бути корельованими із застосовуваними дискретними сигналами, що може призвести до виникнення помилки при вилученні відповідних блоків інформаційних даних на приймальній стороні.

В основу винаходу поставлена задача створити пристрій для реалізації стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектра який, за рахунок врахування статистичних властивостей контейнера дозволить значно підвищити достовірність вилучення вбудованих даних, тобто шляхом введення додаткових обмежень на значення коефіцієнта кореляції використовуваних дискретних сигналів та окремих фрагментів просторової області зображення реалізація винаходу дозволить значно зменшити кількість виникаючих помилок при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Поставлена задача вирішується за рахунок того, що в пристрій для реалізації стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектра, який містить чотири входи, вихід, блок введення та форматування стеганограмм, блок введення ключів де-перемежування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів розшифрування, блок фільтрації, блок де-перемежування, генератор псевдовипадкових послідовностей, демодулятор, блок перешкодостійкого декодування, блок розшифрування, блок формування та виводу інформаційних даних додатково вводиться блок адаптації (запам'ятовуючий пристрій), причому його вхід з'єднаний з виходом блока введення ключів формування псевдовипадкових послідовностей, а вихід з'єднаний з другим входом генератора псевдовипадкових послідовностей.

Додатково введений блок адаптації (запам'ятовуючий пристрій) реалізується таким чином, щоб значення коефіцієнта кореляції застосовуваних псевдовипадкових послідовностей (дискретних сигналів) та блоків даних контейнера не перевищували значення наперед встановленого порога, тобто у цьому блока реалізується правило відбору псевдовипадкових послідовностей за критерієм (6). Блок адаптації може бути реалізований у вигляді запам'ятовуючого пристрою, коли в ньому зберігаються псевдовипадкові послідовності, тотожні тим, які застосовуються на передавальній стороні при вбудовуванні інформаційних повідомлень.

Структурна схема запропонованого пристрою для реалізації стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектра зображено на фіг. 9.

Запропонований пристрій містить чотири входи, вихід, блок введення та форматування стеганограмм, блок введення ключів деперемежування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів розшифрування, блок фільтрації, блок деперемежування, генератор псевдовипадкових послідовностей, демодулятор, блок перешкодостійкого декодування, блок розшифрування, блок формування та виводу інформаційних даних та додатково введений блок адаптації (запам'ятовуючий пристрій).

Елементи запропонованого пристрою з'єднанні наступним чином. Перший вхід пристрою з'єднаний з входом блока введення та форматування стеганограми, вихід якого з'єднаний з першим входом блока фільтрації. Вихід блока фільтрації з'єднаний з першим входом блока деперемежування. Другий вхід пристрою з'єднаний з входом блока введення ключів деперемежування, вихід якого з'єднаний з другим входом блока деперемежування. Вихід „ блока деперемежування з'єднаний з першим входом демодулятора. Третій вхід пристрою з'єднаний з входом блока введення ключів формування псевдовипадкових послідовностей, вихід якого з'єднаний з першим входом генератора псевдовипадкових послідовностей та входом додатково введеного блока адаптації (запам'ятовуючого пристрою). Вихід блока адаптації з'єднаний з другим входом генератора псевдовипадкових послідовностей. Вихід генератора псевдовипадкових послідовностей з'єднаний з другим входом демодулятора, вихід якого з'єднаний з входом блока перешкодостійкого декодування. Вихід блока перешкодостійкого декодування з'єднаний з першим входом блока розшифрування. Четвертий вхід пристрою з'єднаний з входом блока введення ключів розшифрування, вихід якого з'єднаний з другим входом блока розшифрування. Вихід блока розшифрування з'єднаний з входом блока формування та виводу інформаційних даних.

Робота запропонованого пристрою полягає в наступному. На перший вхід пристрою вводиться стеганограма $\bar{S}$, яка подається на вхід блока введення та форматування стеганограми, в якому формуються окремі фрагменти (блоки) $\overline{S_i}$ просторової області стеганозображення, що подаються на вхід пристрою фільтрації. Після фільтрації отримані дані $\overline{\overline{S_i}}$ подаються на перший вхід блока деперемежування, на якому виконується дія, інверсна перемежуванню на передавальній стороні.

Блок деперемежування ініційовано ключем деперемежування K_1, який подається на другий вхід пристрою та через блок введення ключів деперемежування подається на другий вхід блока деперемежування. Отримані після деперемежування дані $S*_i$ подаються на перший вхід демодулятора, який виконує функцію кореляційного приймача дискретних сигналів за розглянутим вище правилом.

На третій вхід пристрою подається ключ формування псевдовипадкових послідовностей K_1, який через блок введення ключів формування псевдовипадкових послідовностей подається на вхід генератора псевдовипадкових чисел та на вхід додатково введеного блока адаптації (запам'ятовуючого пристрою). Блок адаптації виконує корегування роботи генератора псевдовипадкових послідовностей таким чином, щоб коефіцієнт кореляції формованих дискретних сигналів та блоків даних контейнера не перевищував значення наперед встановленого порога, тобто у цьому блока реалізується правило відбору псевдовипадкових послідовностей за критерієм (6). У найпростішому випадку блок адаптації може бути реалізований у вигляді запам'ятовуючого пристрою, коли в ньому зберігаються псевдовипадкові послідовності, тотожні тим, які застосовуються на передавальній стороні при вбудовуванні інформаційних повідомлень.

Вихідна дія додатково введеного блока адаптації подається на другий вхід генератора псевдовипадкових чисел, який ініційовано введеним ключем формування псевдовипадкових послідовностей. Генератор формує ансамбль дискретних сигналів $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ (псевдовипадкових послідовностей). Сформовані дискретні сигнали Φ_j подаються на другий вхід демодулятора. Послідовності, які надходять до демодулятора з виходу генератора псевдовипадкових послідовностей, є тотожними тим, які застосовуються на передавальній стороні при вбудовуванні інформаційних повідомлень.

В демодуляторі обчислюється значення коефіцієнта кореляції між поданими на його перший вхід даними $S*_i$ (з виходу блока деперемежування) та послідовностями Φ_j, які подані на його другий вхід (з виходу генератора псевдовипадкових послідовностей). Рішення, стосовно значення вбудованих даних, приймається відповідно до значення обрахованого коефіцієнта кореляції за правилом (5).

Вилучені дані m_i подаються на вхід блока перешкодостійкого декодування, в якому за визначеним правилом із використанням внесеної надмірності виправляються деякі помилки, відповідно до корегуючої здатності коду. Це призводить до деякого підвищення достовірності переданих даних. Отримані після декодування дані подаються на перший вхід блока розшифрування, ініційованого ключем розшифрування K_3. Ключ розшифрування KA_3 подається на четвертий вхід пристрою та через блок введення ключів розшифрування подається на другий вхід блока розшифрування. Розшифровані повідомлення подаються на вхід блока

форматування та виводу інформаційних даних, в якому завершується формування інформаційних повідомлень, що подаються на вихід пристрою.

Таким чином, в результаті роботи запропонованого пристрою за рахунок додаткового введення блока адаптації (запам'ятовуючого пристрою), що реалізує правило відбору послідовностей за критерієм (6) із врахуванням статистичних властивостей контейнера, вдається значно підвищити достовірність вилучення вбудованих даних.

ФОРМУЛА ВИНАХОДУ

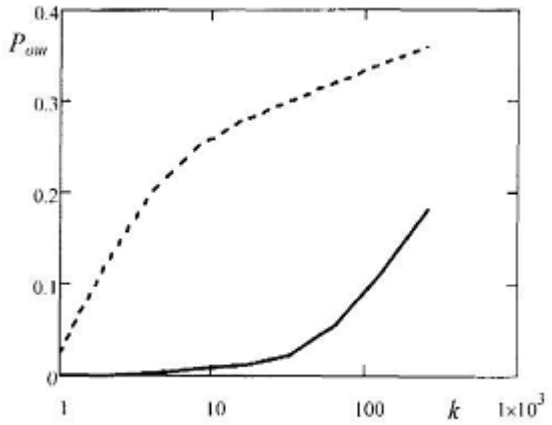
1. Спосіб стеганографічного приховування та вилучення даних в просторовій області зображень із використанням прямого розширення спектра, який полягає в тому, що на передавальній стороні після шифрування та перешкодостійкого кодування окремі блоки даних інформаційного повідомлення за допомогою відповідних пристроїв модулюються шумоподібними дискретними сигналами із великою базою, модульоване інформаційне повідомлення за статистичними властивостями приймає вигляд випадкової послідовності, а за рахунок великої бази дискретних сигналів досягається розширення спектра частот, отримане модульоване повідомлення подається на пристрій перемежування, на якому елементи за допомогою таємного ключа перемішуються за відповідним правилом, отримані данні за допомогою відповідного пристрою поелементно додаються до даних контейнера, а саме - даних цифрового зображення в просторовій області, потім ці дані подаються на пристрій квантування, який виконує певне перетворення для зберігання початкового динамічного діапазону зображення-контейнера, в результаті чого формується стеганограма та заповнений контейнер, стеганограма передається приймальній стороні, на приймальній стороні отримана стеганограма після фільтрації подається на пристрій зворотного перемежування, на якому елементи за допомогою таємного ключа перемішуються за правилом, яке інверсне правилу перемежування на передавальній стороні, вилучення блоків інформаційних даних виконується за допомогою кореляційного приймача, який обраховує значення коефіцієнта кореляції отримані після зворотного перемежування даних та відповідних дискретних сигналів, тотожних тим, що застосовувалися на передавальній стороні, значення вилучених даних приймається за допомогою порогового пристрою відповідно до обрахованого коефіцієнта кореляції, в результаті чого після перешкодостійкого декодування та розшифрування формуються інформаційні повідомлення, секретний ключ задає правило адаптивного формування псевдовипадкових послідовностей, які формуються відповідним генератором та використовуються як шумоподібні дискретні сигнали, який **відрізняється** тим, що застосовують адаптивне формування дискретних сигналів $\Phi_j = \left(\varphi_{j_0}, \varphi_{j_1}, ..., \varphi_{j_{n-1}}\right)$ із врахуванням статистичних властивостей даних блоків контейнера C_i, тобто значення коефіцієнта кореляції $\rho(C_i, \Phi_j)$ для всіх $i = 0,...,N-1$ та для всіх $j = 0,...,M-1$ за модулем не повинно перевищувати деякого наперед визначеного значення ρ_{max} (значення встановленого порога):

$$\left|\rho(C_i, \Phi_j)\right| = \left|\frac{1}{n}\sum_{z=0}^{n-1} C_{iz}\varphi_{j_z}\right| \le \rho_{max}.$$

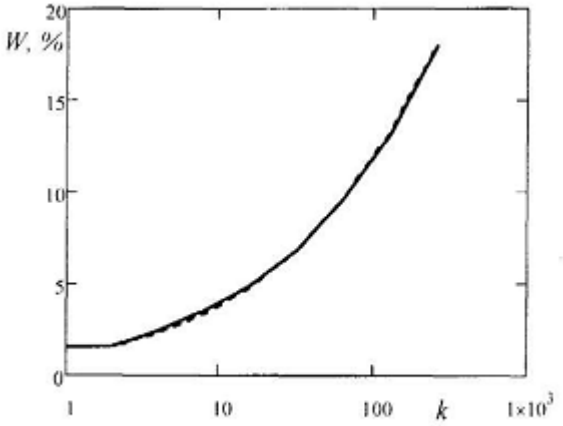
2. Пристрій для реалізації стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектра, який містить п'ять входів, вихід, блок введення інформаційних даних, блок введення ключів шифрування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів перемежування, блок введення контейнерів, блок шифрування, блок перешкодостійкого кодування, генератор псевдовипадкових послідовностей, модулятор, блок перемежування, блок додавання, блок квантування, блок формування та виводу стеганограми, який **відрізняється** тим, що додатково введений блок відбору псевдовипадкових послідовностей, причому його перший вхід з'єднаний з виходом генератора псевдовипадкових послідовностей, другий вхід з'єднаний з виходом блока введення контейнерів, а вихід з'єднаний з другим входом модулятора.

3. Пристрій для реалізації стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектра, який містить п'ять входів, вихід, блок введення інформаційних даних, блок введення ключів шифрування, блок введення ключів формування псевдовипадкових послідовностей, блок введення ключів перемежування, блок введення контейнерів, блок шифрування, блок перешкодостійкого кодування, генератор псевдовипадкових послідовностей, модулятор, блок перемежування, блок додавання, блок квантування, блок формування та виводу стеганограми, який **відрізняється** тим, що додатково введений блок адаптації (запам'ятовуючий пристрій), причому його вхід з'єднаний з виходом

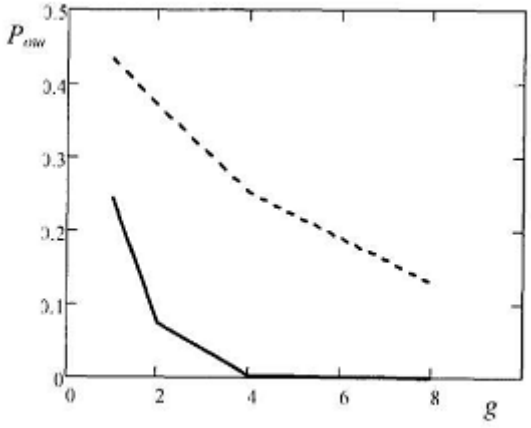
блока введення ключів формування псевдовипадкових послідовностей, а вихід з'єднаний з другим входом генератора псевдовипадкових послідовностей.



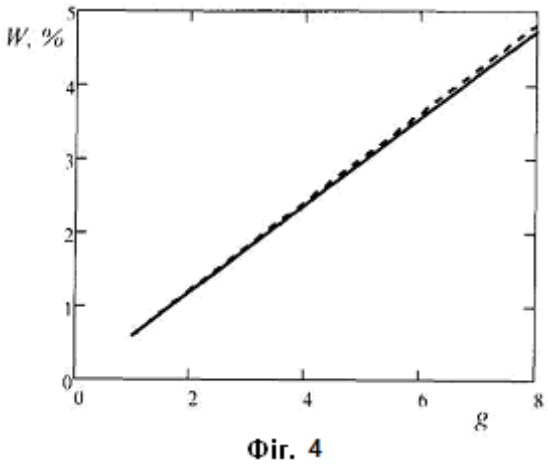
Фіг. 1



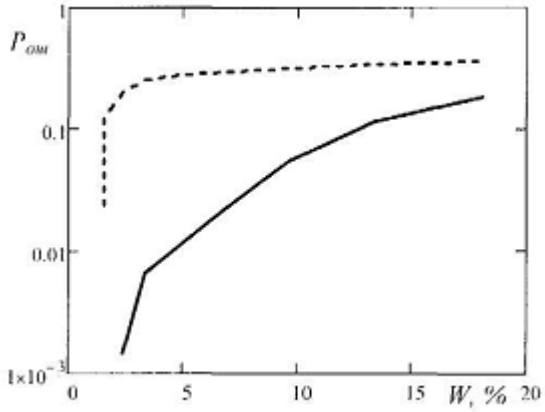
Фіг. 2



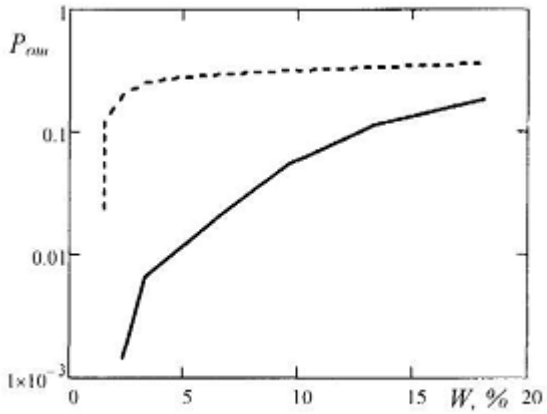
Фіг. 3



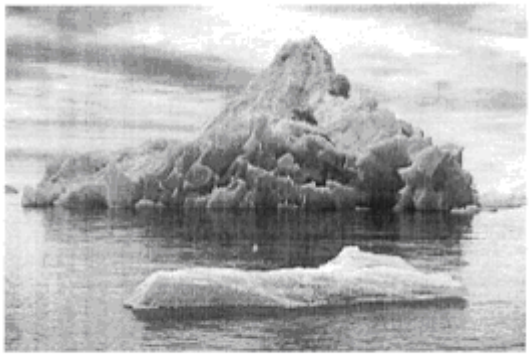
Фіг. 4



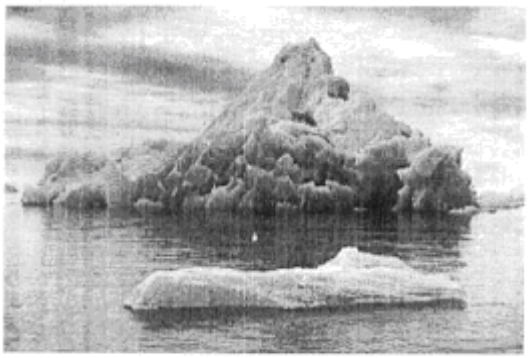
Фіг. 5



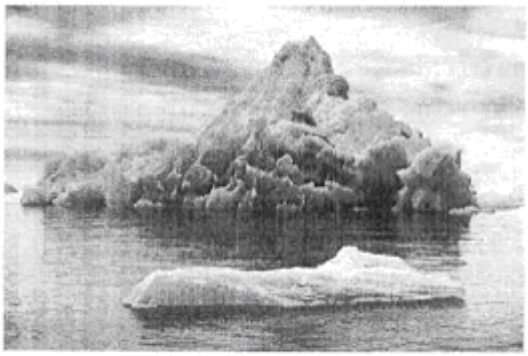
Фіг. 6



Фіг. 7а

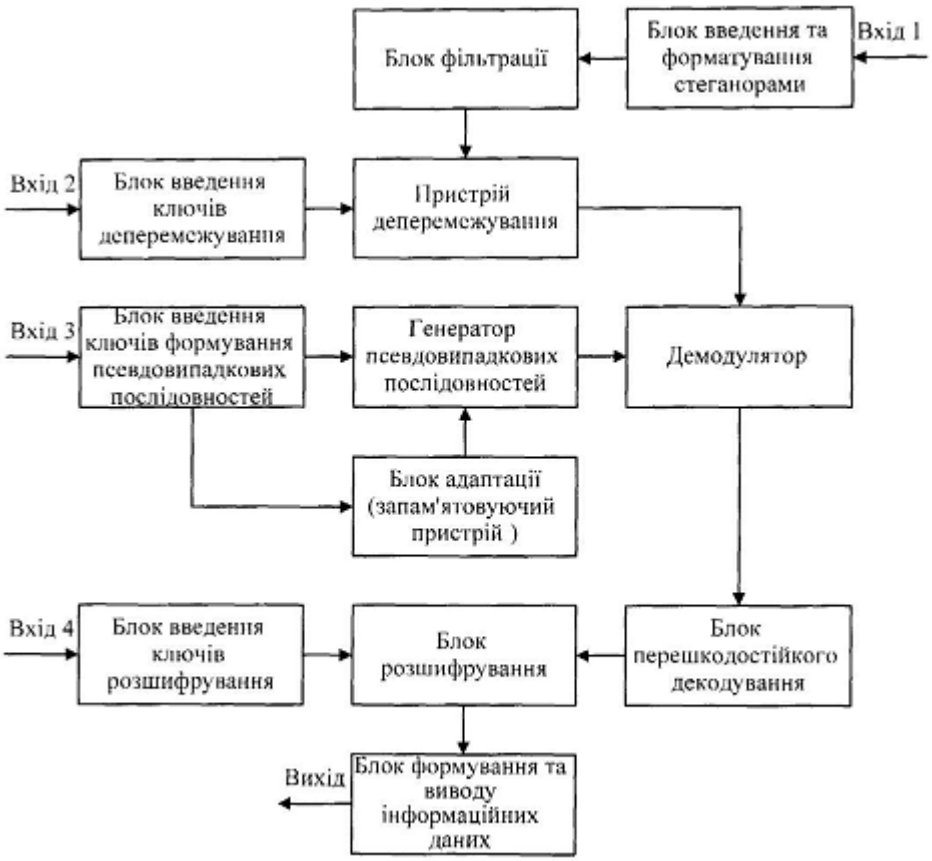


Фіг. 7б



Фіг. 7в

Фіг. 8



Фіг. 9

Комп'ютерна верстка С. Чулій

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601