УДК 621.396

О.А. Смірнов

Кіровоградський національний технічний університет, Кіровоград

МЕТОД СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ТА ВИЛУЧЕННЯ ДАНИХ В ПРОСТОРОВІЙ ОБЛАСТІ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРУ

Розглядаються стеганографічні системи захисту інформації, в яких приховується не тільки смисловий зміст інформаційних даних, але й сам факту організації таємної передачі повідомлень. Пропонується метод стеганографічного приховування та вилучення даних в просторовій області зображень із використанням прямого розширення спектру. Запропонований метод відрізняється від відомих врахуванням статистичних властивостей контейнера-зображення, що дозволяє значно підвищити достовірність вилучення вбудованих даних, тобто за рахунок введення додаткових обмежень на значення коефіцієнту кореляції використовуваних дискретних сигналів та даних просторової області зображення вдається значно зменшити кількість виникаючих помилок при вилученні інформаційних даних на приймальній стороні.

Ключові слова: *стеганографія, захист інформації, пряме розширення спектру*

Вступ

Перспективним напрямком у розвитку стеганографічних методів приховування та вилучення інформаційних повідомлень з просторової області нерухомих зображень є застосування прямого розширення спектру. У роботах [1 – 3] було запропоновано використання дискретних сигналів з великою базою для вбудовування інформаційних повідомлень в контейнери-зображення. При цьому стеганографічна система здобуває переваги широкосмугової системи зв'язку, а саме: високу перешкодостійкість, імітостійкість та скритність передачі інформаційних повідомлень. Однак, як було з'ясовано в роботі [4], застосування псевдовипадкових послідовностей у якості дискретних сигналів при прямому розширенні спектру не гарантує правильного вилучення інформаційних повідомлень на приймальній стороні. Річ у тім, що при стеганографічному перетворенні зазвичай у якості контейнерів застосовуються реалістичні зображення, відповідно, при реалізації корреляційного прийому дискретних сигналів на приймальній стороні може виникнути помилка. Ймовірність цієї події, як показано у [4], може бути зменшена за рахунок врахування статистичних властивостей контейнерів-зображень при псевдовипадковому формуванні дискретних сигналів.

Метою цієї статті є розробка методу стеганографічного приховування та вилучення даних в просторовій області зображень із використанням прямого розширення спектру, який враховує статистичні властивості контейнера-зображення, що дозволяє значно підвищити достовірність вилучення вбудованих даних, тобто за рахунок введення додаткових обмежень на значення коефіцієнту кореляції використовуваних дискретних сигналів та даних просторової області зображення вдається значно зменшити кількість виникаючих помилок при вилученні інформаційних даних на приймальній стороні.

1. Відомий метод стеганографічного приховування даних

Відомий метод стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектру [1 – 3] ґрунтується на тому, що на передавальній стороні після шифрування та перешкодостійкого кодування окремі блоки $m_i = \left(m_{i_0}, m_{i_1}, ..., m_{i_{k-1}}\right)$, $i = 0,..., N-1$ даних інформаційного повідомлення $m = \left(m_0, m_1, ..., m_{N-1}\right)$ за допомогою відповідних пристроїв модулюються шумоподібними дискретними сигналами:

$$\Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right),$$

$$\Phi_i \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\},$$

$$k \le M,$$

із базою $B = TF$, де T – тривалість елемента сигналу φ_{i_j}, F – полоса 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 блоку m_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 спектру 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 данні $\overline{E_i} = f(E_i, K_1)$ за допомогою відповідного пристрою поелементо 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 збереження початкового динамічного діапазону зображення-контейнеру, в результаті чого формуються окремі блоки стеганограми $\overline{S_i}$ 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 стеганограми $\overline{\overline{S_i}}$ 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 коефіцієнту 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:

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

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

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

Оскільки всі послідовності із множини Φ 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:

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

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 у якості шумоподібних дискретних сигналів $\Phi_i \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ з ансамблю Φ потужності M. 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 відомого способу є те, що в процесі вбудовування даних інформаційного повідомлення не враховуються статистичні властивості блоків контейнера C_i, тобто цифрові данні 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 блоку 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). Як довели проведені авторами дослідження, на практиці такі випадки відбуваються дуже часто. Це пов'язане з тим, що цифрові данні просторової області реальних зображень, використовуваних під час стеганографічного приховування інформаційних повідомлень, не володіють випадковою статистичною структурою, 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 данні у просторовій області зображень не є реалізацією випадкового процесу і навіть за своїми статистичними властивостями не подібні до псевдовипадкових послідовностей. Відповідні значення коефіцієнту кореляції:

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

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

2. Запропонований метод стеганографічного приховування та вилучення даних

В основу пропонованого методу поставлена задача створити спосіб стеганографічного в просторовій області зображень із використанням прямого розширення спектру приховування даних в просторовій області зображень із використанням прямого розширення спектру, який, за рахунок врахування статистичних властивостей контейнера C_i дозволить значно підвищити достовірність вилучення вбудованих даних, тобто шляхом введення додаткових обмежень на значення коефіцієнту кореляції використовуваних дискретних сигналів та окремих фрагментів просторової області зображення реалізація корисної моделі 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 коефіцієнту 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 порогу):

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

Таким чином, формування послідовностей $\Phi_j \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ 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 контейнеру, і відповідно, коефіцієнт кореляції і-го блоку 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 $|G \cdot m^*_{i_j}| < \rho_{max}$. Саме у цьому випадку відбудеться помилка вилучення інформаційних даних, але ймо-

вірність такої події буде значно менша за ймовірність випадку виникнення помилки вилучення даних у відомому способі [4]. Якщо значення порогу ρ_{max} задати менше, ніж значення коефіцієнту 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.

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

Запропонований спосіб стеганографічного приховування та вилучення даних може бути реалізований за допомогою введення відповідного блоку – пристрою відбору послідовностей за правилом (6).

Структурні схеми пристроїв стеганографічного приховування та вилучення даних в просторовій області зображень із використанням прямого розширення спектру, які побудовані за пропонованим способом, зображено на рис. 1, 2.

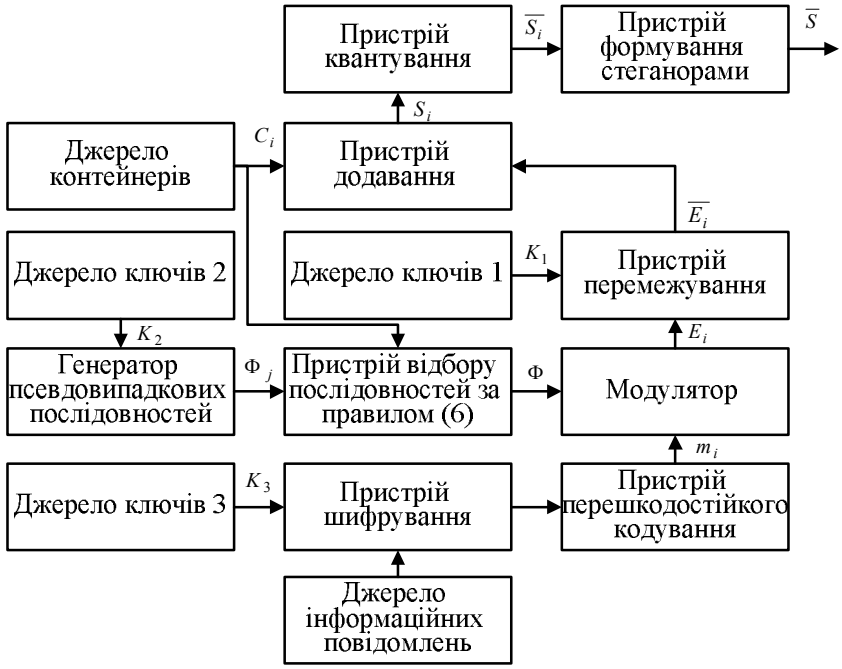

Рис. 1. Структурна схема запропонованого пристрою стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектру

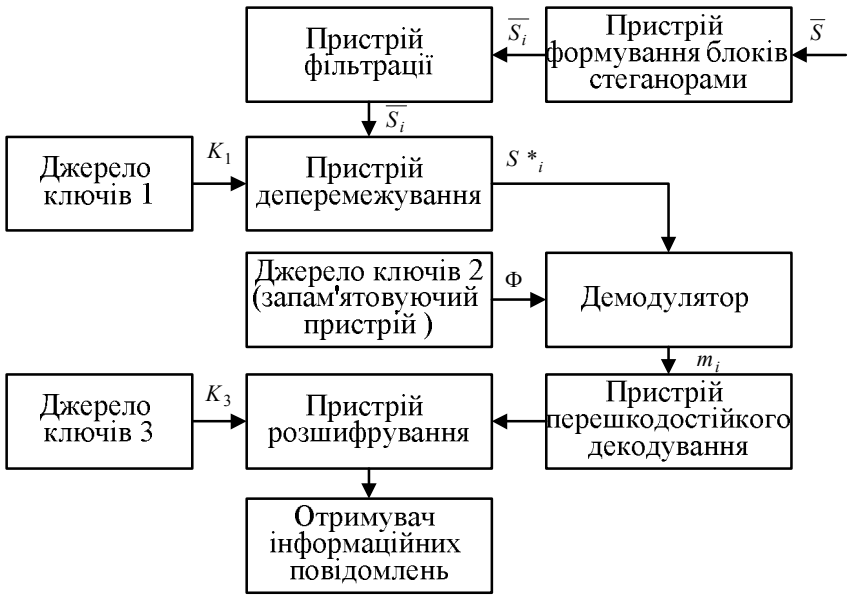

Рис. 2. Структурна схема запропонованого пристрою стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектру

Пристрій стеганографічного приховування даних (рис. 1) працює наступним чином. Джерело інформаційних повідомлень формує послідовність інформаційних даних, які подаються пристрій шифрування, ініційований таємним ключем K_3, що формується джерелом ключів 3. Зашифровані інформаційні повідомлення подаються на пристрій перешкодостійкого кодування, в якому виконується внесення спеціально формованої надмірності для підвищення достовірності інформаційних зашифрованих даних. Джерело ключів 2 формує таємний ключ K_2, який ініціює генератор псевдовипадкових послідовностей. Результатом роботи генератору псевдовипадкових послідовностей є дискретні сигнали, тобто дискретні послідовності, елементи яких сформовано псевдовипадковим чином. Сформовані псевдовипадкові послідовності Φ_j поступають на додатково (в порівнянні із відомим способом) введений пристрій відбору послідовностей за правилом (6), в якому для всіх $i = 0,..,N-1$ розраховується значення коефіцієнту кореляції:

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

та порівнюється із наперед визначеним значенням ρ_{max}.

У випадку, коли хоча б для одного $i \in \{0,..,N-1\}$ розраховане значення $\rho\left(C_i, \Phi_j\right)$ перевищить значення порогу ρ_{max}, сформована псевдовипадкова послідовність бракується, тобто дискретні сигнали Φ_j із $\rho\left(C_i, \Phi_j\right) > \rho_{max}$ 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 коефіцієнту кореляції $\rho\left(C_i, \Phi_j\right)$ менші або дорівнюють встановленому порогу ρ_{max}, тобто, якщо виконується умова (6) для всіх блоків даних контейнеру, 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 блок інформаційних даних $m_i = \left(m_{i_0}, m_{i_1}, ..., m_{i_{k-1}}\right)$, $k \le M$, який модулюється псевдовипадковими послідовностями за правилом (1).

Сформоване таким чином модульоване повідомлення E_i подається на пристрій перемежування, ініційованого таємним ключем K_1, який сформовано джерелом ключів 1. Пристрій перемежування обробляє модульоване повідомлення E_i, тобто за правилом f, яке задає таємний ключ K_1, псевдовипадковим чином переставляє місцями елементи E_i. Отримані дані $\overline{E_i} = f(E_i, K_1)$ подаються на пристрій додавання, у якому виконується поелементне додавання з даними контейнеру 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. Контейнер формується джерелом контейнерів. Отримані дані S_i подаються на пристрій квантування, який виконує певне перетворення для зберігання початкового динамічного діапазону зображення-контейнеру, в результаті чого формуються окремі блоки стеганограми $\overline{S_i}$ та заповнений контейнер $\overline{S} = \overline{S_0} \cup \overline{S_1} \cup ... \cup \overline{S_{N-1}}$, який передається приймальній стороні.

Пристрій стеганографічного вилучення даних (рис. 2) працює аналогічно відповідному пристрою як і у відомому способі [1 – 3], за винятком генератора псевдовипадкових послідовностей, що формує відповідні дискретні сигнали. Пристрій функціонує наступним чином. Отримана стеганограмма $\overline{S}$ на приймальній стороні подається на пристрій формування блоків стеганограми, в якому формуються блоки $\overline{S_i}$ та подаються на пристрій фільтрації. Після фільтрації отримані дані $\overline{\overline{S_i}}$ подаються на пристрій зворотного перемежування, на якому виконується дія, інверсна перемежуванню на передавальній стороні. Пристрій деперемежування ініційовано секретним ключем K_1, який сформовано джерелом ключів 1. Отримані після деперемежування дані S^*_i подаються на демодулятор, який виконує функцію кореляційного приймача дискретних сигналів за розглянутим вище правилом. Тобто в демодуляторі обчислюється значення коефіцієнту кореляції даних S^*_i та псевдовипадкових послідовностей Φ_i (дискретних сигналів). Ансамбль дискретних сигналів не формується (як у відомому способі) відповідним генератором псевдовипадкових чисел, що ініційований секретним ключем K_2, а зберігається у запам'ятовуючому пристрою, тобто весь ансамбль псевдовипадкових послідовностей $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ виступає у ролі секретного ключа K_2 і зберігається цілком в такому вигляді. Таким чином, запам'ятовуючий пристрій можна розглядати як аналог джерела ключів 2 у відомому

способі [3], а послідовності, які надходять з нього, є тотожними тим, які застосовуються на передавальній стороні при вбудовуванні інформаційних повідомлень. Таким чином, в демодуляторі обчислюється значення коефіцієнту кореляції між отриманими даними S^*_i та послідовностями, які застосовувалися при вбудовуванні інформації. Рішення стосовно значення вбудованих даних приймається відповідно до значення обрахованого коефіцієнту кореляції за правилом (5). Вилучені дані m_i подаються на пристрій 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, які після декодування подаються на пристрій розшифрування, ініційованого таємним ключем K_3, що формується джерелом ключів 3. Розшифровані повідомлення подаються отримувачу інформаційних повідомлень.

Висновки

Таким чином, запропонований спосіб стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектру за рахунок врахування статистичних властивостей контейнера дозволяє значно підвищити достовірність вилучення вбудованих даних, тобто шляхом введення додаткових обмежень на значення коефіцієнту кореляції використовуваних дискретних сигналів та окремих фрагментів просторової області зображення реалізація корисної моделі дозволяє значно зменшити кількість виникаючих помилок при вилученні відповідних блоків інформаційних даних на приймальній стороні.

Список літератури

1. Smith J.R. Modulation and information hiding in images / J.R. Smith, B.O. Comisky // R. Anderson, editor, Information Hiding, First International Workshop, volume 1174 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996. – P. 207-226.

2. 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.

3. Patent No.: US 6,557,103 B1, Int.Cl. 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.Cl. G06F 11/30. – № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003.

4. Кузнецов О.О. Дослідження ймовірнісних властивостей стеганографічного захисту інформації із використанням прямого розширення спектру. / О.О. Кузнецов, О.А. Смірнов, Л.Т. Пархуць, Ю.М. Рябуха // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІНУ», 2012. – Вип. 1(21). – Т. 1. – С. 115-121.

5. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А. Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с., ил.

6. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.

7. Хорошко В.А. Введение в компьютерную стеганографию / В.А. Хорошко, М.Е. Шелест. – К., 2002. – 140 с.

8. Кузнецов А.А. Встраивание информационных данных в неподвижные изображения с использованием прямого расширения спектра / А.А. Кузнецов, А.М. Ботнов, П.А. Лаптий // Прикладная радиоэлектроника: науч.-техн. журн. Харьк. нац. ун-т радиоэлектроники. – Х., – Т.9 N 3. – С.470-478.

Надійшла до редколегії 27.02.2012

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОД СТЕГАНОГРАФИЧЕСКОГО УТАИВАНИЯ И ИЗЪЯТИЯ ДАННЫХ В ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПРЯМОГО РАСШИРЕНИЯ СПЕКТРА

А.А. Смирнов

Рассматриваются стеганографические системы защиты информации, в которых скрывается не только смысловое содержание информационных данных, но и сам факт организации тайной передачи сообщений. Предлагается метод стеганографического утаивания и изъятия данных в пространственной области изображений с использованием прямого расширения спектра. Предложенный метод отличается от известных учетом статистических свойств контейнера-изображения, которые разрешают значительно повысить достоверность изъятия встроенных данных, т.е. за счет введения дополнительных ограничений на значение коэффициента корреляции используемых дискретных сигналов и данных пространственной области изображения удается значительно уменьшить количество возникающих ошибок при изъятии информационных данных на приемной стороне.

Ключевые слова: *стеганография, защита информации, прямое расширение спектра.*

METHOD STEGANOGRAPHY HIDING AND WITHDRAWAL GIVEN IN SPATIAL AREA OF THE SCENES WITH USE THE DIRECT EXPANSION OF THE SPECTRUM

A.A. Smirnov

They are considered steganography of the system of protection to information, in which escapes not only semantic contents information data, but also fact itself to organizations by secret of the issue of the messages. The method steganography hiding and withdrawal given are offered in spatial area of the scenes with use the direct expansion of the spectrum. The Offered method differs from the known account statistical characteristic container-scenes, which allow vastly to raise validity of the withdrawal built-in data i.e. to account of the entering the additional restrictions on importance of the factor to correlations used discrete signal and given spatial area of the scene manages vastly to reduce the amount appearing mistake when removing information given on receiving end.

Keywords*: steganography, protection to information, direct expansion of the spectrum.*