**УДК 681.511:3**

***В.К. Задірака, С.С. Мельнікова, Н.В. Бородавка***
Інститут кібернетики ім. В.М. Глушкова НАНУ, м. Київ, Україна

# Спектральні алгоритми комп'ютерної стеганографії

У статті розглядається застосування теорії швидких ортогональних перетворень до розробки алгоритмів конструюючої комп'ютерної стеганографії.

## Вступ

Стеганографія – один із шляхів підтримки інформаційної безпеки. Вона являє собою метод організації зв'язку, який приховує сам факт наявності таємних повідомлень. Стеганографічні методи активно використовуються для захисту інформації від несанкціонованого доступу, для протидії системам моніторингу та керування ресурсами мереж, для маскування програмного забезпечення від незареєстрованих користувачів, а також для захисту авторського права на деякі види інтелектуальної власності.

На конференції Information Hiding (First Information Workschop) у 1996 році були обговорені всі базові поняття стеганографії та прийнята єдина термінологія. Згідно з цією термінологією стеганографічна система, або стегосистема, – це сукупність засобів та методів, які використовуються для формування таємного каналу зв'язку. Будь-яка інформація, у якій будуть приховані таємні дані, зветься контейнером. Контейнером може слугувати будь-який файл чи потік даних. Контейнер, який не містить таємного повідомлення, називають пустим, а той що містить – заповненим або стегоконтейнером. Канал передачі стегоконтейнера має назву стеганографічного каналу або стегоканалу. Таємний ключ, який необхідний для «вкраплення» інформації в контейнер, називається стегоключем або просто ключем. У залежності від кількості рівнів захисту у стегосистемі може використовуватись як один, так і декілька ключів.

Задача стеганографічної системи – розмістити вихідне повідомлення в контейнері таким чином, щоб жодна стороння людина не змогла помітити нічого, крім його основного вмісту. Основний вміст контейнера не відіграє ніякої ролі ні для відправника, ні для одержувача, яких цікавить лише успішна передача повідомлення, вміщеного в ньому (стеганограми). Потрібно обов'язково враховувати те, що сам факт відправлення контейнера від автора до одержувача не повинен виглядати дивним, а також не повинно бути помітних відхилень контейнера від норми.

Схематично узагальнену модель стеганографічної системи можна представити у такому вигляді (рис. 1):

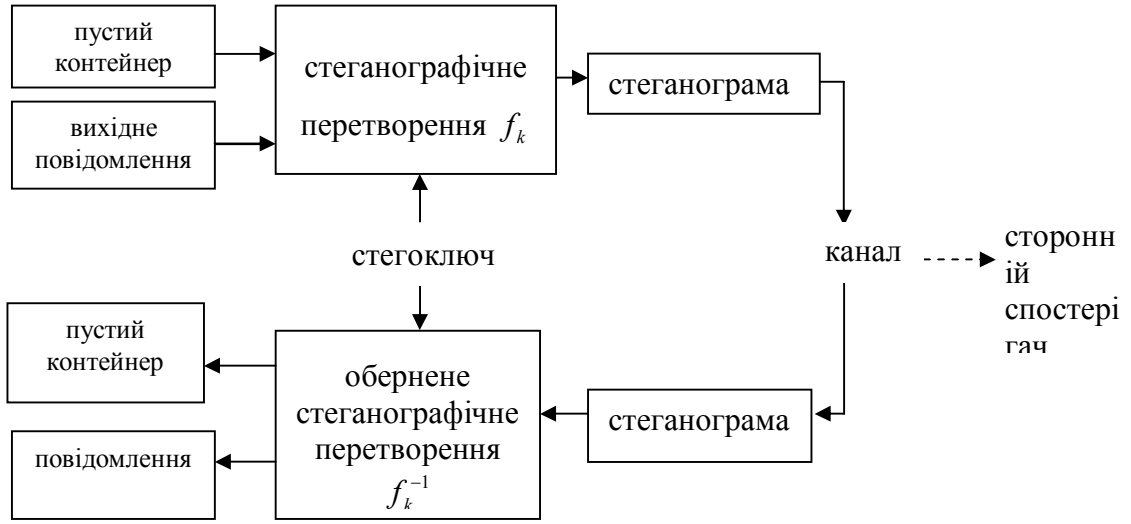


Рис. 1. Узагальнена модель стеганографічної системи

При побудові будь-якої стегосистеми потрібно враховувати наступні загальноприйняті правила:

1. Потенційний зловмисник має повне уявлення про стегосистему та деталі її реалізації. Єдина інформація, що йому невідома – це ключ, за допомогою якого можна встановити факт наявності повідомлення та його зміст.
2. Якщо зловмисник якимось чином дізнається про факт існування таємного повідомлення, це не повинно дозволити йому виявити подібні повідомлення з контейнерів доти, доки ключ зберігається в таємниці.
3. Потенційний зловмисник не повинен мати будь-яких технічних чи інших переваг перед користувачем у розпізнаванні чи розкритті змісту таємних повідомлень.

Усі існуючі стеганографічні методи можна розділити на два класи: технологічні та інформаційні (рис. 2).

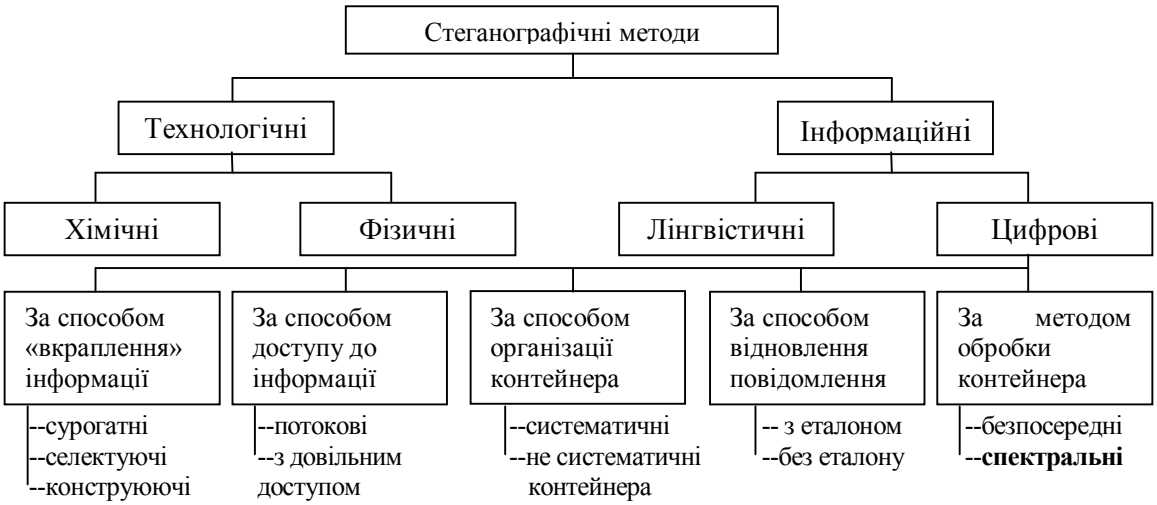


Рис. 2. Класифікація стеганографічних методів

До технологічних методів відносять ті, що базуються на використанні хімічних або фізичних властивостей різних матеріальних носіїв інформації. На сьогодні в цьому плані найбільше зацікавлення викликають стандартні носії інформації: аудіо, відео та обчислювальної техніки. Наприклад, багато мультимедійних форматів даних мають поля розширень, які заповнюються нульовою інформацією та не враховуються програмою; можна записати інформацію й на невикористовуваних місцях гнучких магнітних дисків (на нульовій доріжці тощо). Подібні методи прості у використанні, проте вони мають низький рівень стійкості та забезпечують передачу порівняно невеликих об'ємів даних.

Клас інформаційних методів містить у собі лінгвістичні та цифрові. Лінгвістичні методи базуються на використанні надмірності людської мови або іншого середовища, що не містить букв та цифр (фотографії, графіка, креслення та інше). До цього класу можна також віднести метод генерації псевдоосмисленого тексту, необхідного для приховання таємного повідомлення, а також методи, що базуються на зміні положення рядків на сторінці чи слів у реченні тощо.

Більшість цифрових методів базується на тому, що, з одного боку, файли, які не потребують абсолютної точності, можуть бути дещо видозмінені без втрати функціональності, а з іншого – на відсутності спеціального інструментарію або нездатності органів чуття людини надійно розрізняти незначні зміни в таких файлах.

Методи цифрової стеганографії прийнято класифікувати за різними основами. За способом вкраплення інформації в контейнер розрізняють методи сурогатної, селектуючої та конструюючої стеганографії [1]. Сурогатна стеганографія може бути застосована для досить «шумних» контейнерів, у яких заміна частини бітів контейнера на біти таємного повідомлення не буде помітною для стороннього спостерігача. Що ж до методів селектуючої стеганографії, то вважається, що кодування захованого повідомлення повинно відповідати спеціальним статистичним характеристикам шуму контейнера. Для цього генерується велика кількість альтернативних контейнерів, з яких потім вибирається найбільш підходящий для «вкраплення» даного повідомлення. У конструюючій стеганографії вибір контейнера залежить від таємного повідомлення, тобто в цьому випадку контейнер генерується самою стегосистемою.

За способом доступу до інформації розрізняють потокові методи та методи з довільним доступом. Перші з них працюють із потоками неперервних даних, коли біти повідомлення необхідно включати в контейнер у режимі реального часу. Другі використовують контейнери фіксованої довжини, якими служать файли певного наповнення (текст, програми, графіка, звук тощо.). На практиці частіше всього використовують саме контейнери фіксованої довжини, як більш зручні та доступні.

За способом організації контейнерів методи цифрової стеганографії поділяються на систематичні та не систематичні [2]. У систематично організованих контейнерах інформаційні біти можна відокремити від шумових, у яких і буде розміщуватися таємне повідомлення. При несистематичній організації контейнера такого розділення не існує і для виділення повідомлення необхідно опрацьовувати всі біти контейнера.

При видобуванні таємної інформації в деяких стеганографічних методах необхідно мати еталон використовуваного контейнера. У цьому випадку потрібно забезпечити його надійне зберігання та захист від несанкціонованого викори-

стання. Більшість сучасних методів не потребують наявності еталона контейнера, а для його отримання використовується спеціальна обробка стеганограми.

За методом обробки контейнера цифрові методи поділяються на дві групи: безпосередні та спектральні. При використанні безпосередніх методів обробці підлягають біти самого контейнера, як, наприклад, у методі найменшого значущого біта, методі заміни палітри кольорів або методі сортування палітри [7]. Спектральні методи базуються на використанні дискретних унітарних перетворень: Фур'є, Уолша, Карунена-Лоєва, слент, вейвлет та інших. При використанні методів цієї групи обробці підлягає не вихідний, а відповідні спектральні контейнери [6].

## Спектральні методи на основі перетворення Фур'є

Якщо ми маємо деякий випадковий сигнал $x(t)$ (див. рис.3), що являє собою суму періодичних компонент $x_1(t)$ з накладеним на них шумом $n(t)$ та описується співвідношенням [1,2]:

$$x(t) = x_1(t) + n(t); \qquad x_1(t) = a_0 + \sum_{j=1}^{s} (a_j \cos w_j t + b_j \sin w_j t), \tag{1}$$

то його можна використати як контейнер для передачі таємного повідомлення.

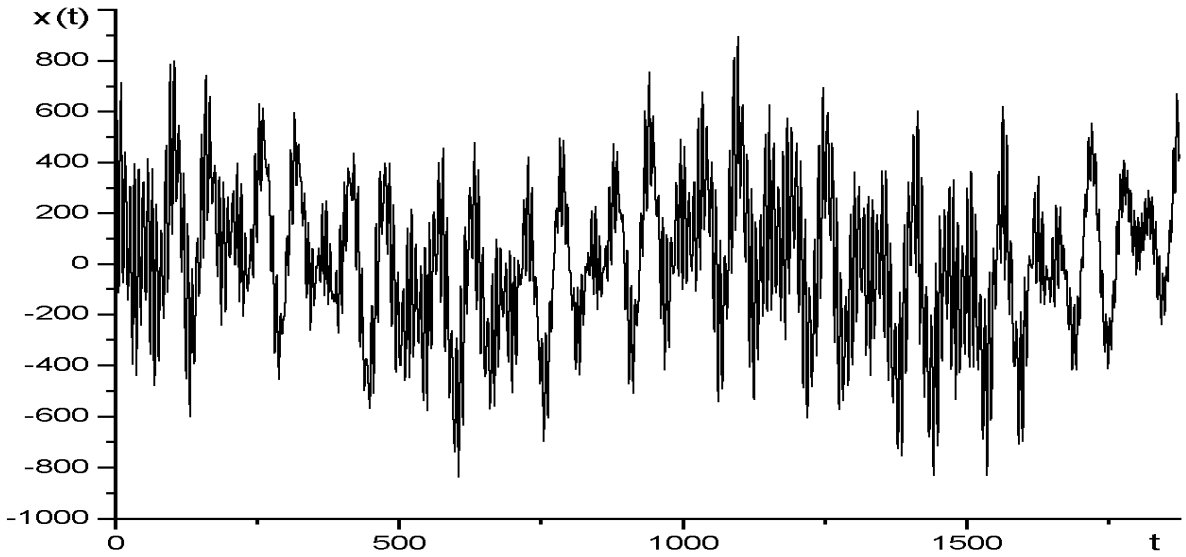


Рис. 3. Приклад випадкового сигналу, що використовується для передачі таємного повідомлення

Спектр зашумленого сигналу складається з головних та побічних пелюсток (див. рис. 4). Для «вкраплення» повідомлення використовуються побічні, які відповідають рівню шуму і похибці заокруглення, бо «вкраплення» в головні пелюстки приводить до великої похибки відновлення сигналу. Таке «вкраплення» дасть можливість приховати факт наявності повідомлення в

контейнері, так як похибка, що привноситься таємним повідомленням співставна з похибкою заокруглення, що виникає в процесі обробки сигналу.

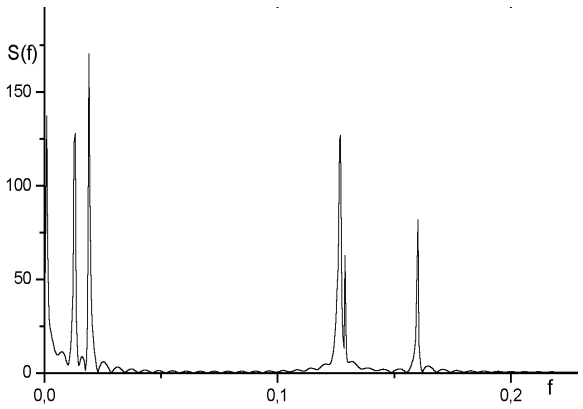


Рис. 4. Амплітудний спектр сигналу *(s=4)*

Необхідною процедурою є процедура формування ключа. В даному випадку це буде фіксація місць «вкраплення» бітів повідомлення у спектр використовуваного сигналу.

Розглянемо більш детально один із можливих класів спектральних алгоритмів. Нехай маємо випадковий сигнал $x(t)$. $x(t_j)=\{x_j\}_0^{N-1}-N$ відліків цього сигналу; $\hat{x}(l)$ – його дискретне перетворення Фур'є:

$$\hat{x}(l)=\sum_{j=0}^{N-1} x_j W^{tl},\ l=\overline{0,\ N-1},\ W=e^{-i\frac{2\pi}{N}}. \qquad (2)$$

Обернене дискретне перетворення Фур'є має вигляд :

$$x(t_j)=\frac{1}{N}\sum_{l=0}^{N-1}\hat{x}(l)W^{-tl}. \qquad (3)$$

Якщо сигнал задано на відрізку $[0,T]$, то його крок в просторово-часовому представленні $\Delta t=\frac{T}{N}$, а в частотному - $\Delta f=\frac{1}{T}$ (частота Найквіста).

Позначимо таємне повідомлення $y$: $y=(y_1,...,y_p)$, а ключ $z$: $z=(z_1,...,z_k)$.

Тоді для передачі таємного повідомлення $y$ в сигналі-контейнері $x(t)$, що задається формулою (1) можна використати наступний алгоритм:

1. В якості селективного перетворення [1], яке дозволяє посилити в сигналі роль періодичної компоненти, тобто здійснити селекцію періодичної компоненти для визначення частот $w_j$ та наближеного значення амплітуд $a_j,\ b_j,\ r_j=\sqrt{a_j^2+b_j^2}, j=\overline{0,s}$, використаємо алгоритм швидкого перетворення Фур'є (ШПФ) [2,3];
2. Для мінімізації похибки відновлення сигналу $x(t)$ будемо «вкраплювати» повідомлення $y$ в побічні пелюстки спектру $\hat{x}(l)$, амплітуди яких менші за максимальну амплітуду виділених піків на задану величину порогового значення $\varepsilon$ (для них виконується співвідношення $r(w_j)/r_{\max}\le\varepsilon$ або $a(w_j)/a_{\max}\le\varepsilon$ або
$b(w_j)/b_{\max}\le\varepsilon,\ \ j=\overline{0,N-1}$ ); (4)

3. Вкраплення біта $y_i$ будемо проводити в біт побічної пелюстки на місце, що є попереднім до першого вірного біту $\overset{1}{x}(\overset{1}{t})$ (відносно оцінки апостеріорної похибки заокруглення алгоритму ШПФ [2]). При цьому необхідно враховувати, що алгоритм ШПФ використовується три рази: для обчислення спектру $\overset{1}{x}(\overset{1}{t})$, при обчисленні сигналу $\tilde{x}(t)$, що містить повідомлення і з точністю до похибки заокруглення співпадає з $x(t)$, і для отримання спектру $\hat{\tilde{x}}(\overset{1}{t})$, з якого дане повідомлення буде «вийматись».
4. Ключем для даного контейнера є номер біта $\tau_k$ в значеннях амплітуд спектру, в які вкрапляються біти повідомлення *y*, а також *p* номерів *j*, для яких виконується співвідношення (4). Тобто загальна довжина ключа $k = p+1$, а у випадку коли повідомлення вкраплюється і в дійсну і в уявну частину спектру можлива ситуація, при якій $k = p+2$.

Для визначення відрізку, з якого можна обирати $\tau_k$ на класі сигналів (1) ($a_0$, $a_j$, $b_j$, $w_j$, $j=\overline{1,s}$; $n(t)$ змінюються в заданому діапазоні або обираються випадково із заданого діапазону за допомогою генератора псевдовипадкових чисел) визначаються апріорні та апостеріорні похибки заокруглення обчислення $\overset{1}{x}(\overset{1}{t})$, $\overset{1}{t}=\overline{0,N-1}$.

Нехай обчислення проводяться на ЕОМ в режимі плаваючої коми з $\tau$ двійковими розрядами у мантис чисел, $N=2^{\gamma}, \gamma>0$ – ціле. Апріорні асимптотичні оцінки похибки заокруглення $e_3$ алгоритму ШПФ мають вигляд [2]:

$$\|e_3\|_E \le 8\cdot 1{,}06\cdot \log_2 N \|\hat{x}\|_E \cdot 2^{-\tau}, \tag{5}$$

де $\|\cdot\|_E$ – евклідова норма вектора, $\tau$ – кількість двійкових розрядів у мантиси числа.

Для ШПФ при $N = N_1\cdot N_2\cdot\ldots\cdot N_{\gamma}$

$$\|e_3\|_E \le 8\cdot 1{,}06\cdot \sum_{j=1}^{\gamma}(2N_j)^{3/2}\|\hat{x}\|_E\cdot 2^{-\tau}. \tag{6}$$

В роботі [3] наведено апріорні асимптотичні оцінки $\|e_3\|_E$ у припущенні, що елементи матриці $W$ обчислені наближено. Нехай $fl(\sin(fl(a)))$ – результат наближеного обчислення $\sin\alpha$ на ЕОМ в режимі плаваючої коми з $\tau$ двійковими розрядами в мантисі числа і

$$fl(\sin(fl(a))) = \sin a + \delta\theta\varepsilon,\ \ \delta\ge 0, -1\le\theta\le 1,\ \ \varepsilon = 2^{-\tau}. \tag{7}$$

В цьому випадку оцінки при $N = N_1 = N_2 = \ldots = N_{\gamma}$ мають вигляд:

$$\|e_3\|_E < \left[K(N,\delta)\varepsilon + O(\varepsilon^2)\right]\cdot\|\hat{x}\|_E \tag{8}$$

$$\|e_3\|_1 < \left[\sqrt{N}\cdot K(N,\delta)\varepsilon + O(\varepsilon^2)\right]\frac{1}{\sqrt{N}}\cdot\|\hat{x}\|_E, \tag{9}$$

де: $K(N,\delta)=\sum_{j=1}^{\gamma}\alpha(N_j)+(\gamma-1)(3+2\delta)$, $\alpha(N_j)=\sqrt{2}$ при $N_j=2$,

$\alpha(N_j)=\sqrt{N_j(N_j+\delta)}$ в інших випадках.

Для ШПФ з основами 2 та 4 [2]:

$$K\left(2^{\gamma},\delta\right)=\left(3+\sqrt{2}+2\delta\right)\gamma-\left(3+2\delta\right), \quad (10)$$

$$K\left(4^{\gamma},\delta\right)=\left(8+2\delta\right)\gamma-\left(3+2\delta\right). \quad (11)$$

В [3] також наведені оцінки похибки заокруглення алгоритму ШПФ у припущенні, що сигнал $x(t)$ є «білим», тобто являє собою $2N$ взаємонезалежних дійсних випадкових величин з нульовим математичним сподіванням та рівними дисперсіями і використовується рандомізоване правило заокруглення [2].

Експериментально отримано значення дисперсії $\sigma_{\varepsilon}^2=0{,}21\cdot 2^{-2\tau}$, що по суті являє собою емпіричне середнє $\sigma_{\varepsilon}^2$ для всіх множень та додавань, які використовуються для обчислення ШПФ «білого шуму». В цьому випадку

$$\sigma_{\varepsilon_3}^2/\sigma_x^2=0{,}21\cdot\gamma\cdot 2^{-2\tau}. \quad (12)$$

При відсіканні результатів в правій частині (12) отримуємо не лінійну залежність від $\gamma$, а квадратичну.

У випадку детермінованого сигналу $|x(t)|<1/2$ та обчислень в режимі з фіксованою комою отримано наступну двосторонню оцінку:

$$(\gamma-2{,}5)C^2\cdot 2^{-2\tau}\le\sigma_{\varepsilon_3}^2/\sigma_x^2\le 2^{\gamma+1}\cdot C^2/\sqrt{N}, \quad (13)$$

де $K=\sum_{t=0}^{N-1}|x(t)|^2/\sqrt{N}$, $C=0{,}3$ для заокруглення, $C=0{,}4$ для відсікання результатів операції.

Використовуємо значення $e_3$ для визначення номеру розряду «вкраплення» біта відкритого тексту таким чином, щоб ця операція практично не впливала на похибку заокруглення.

При цьому також враховується похибки заокруглення оберненого перетворення Фур'є та обчислення $\hat{\hat{x}}(t)$.

Недоліком даного алгоритму є велика довжина ключа - $p+1$. Для того, щоб її зменшити можна «вкраплювати» $y$ в $x(t)$ з рівномірним кроком $l=N/p$, починаючи з відліку $i=n_0$ на рівні похибки заокруглення, але без попереднього аналізу спектру сигналу. В цьому випадку ключ складається з трьох чисел $Z=\{\tau_k,n_0,l\}$, але разом з тим зростає похибка відновлення сигналу що в свою чергу зменшує стійкість цього алгоритму в порівнянні з попереднім.

# Реалізація спектральних алгоритмів на ЕОМ

Наведемо покроковий опис реалізації розглянутого алгоритму:

1. *Вибір сигналу*: Обираємо випадковий сигнал $x(t)\in X(t)$. Параметрами контейнера є амплітуди $a_j$, $b_j$ та частоти $f_j=w_j/2\pi$, $j=\overline{1,s}$. Обчислюємо сигнал згідно з формулою (1). Накладаємо на нього шум за допомогою генератора випадкових чисел, що видає послідовність чисел рівномірно розподілених на заданому інтервалі. Рівень шуму можна регулювати заданням різних інтервалів;

2. *Визначення номера біта для «вкраплення»*. Визначаємо оцінки похибок заокруглення. Апріорна оцінка визначається за формулою (5), враховуючи що обробці підлягають дійсні числа представлені в розширеному форматі (загальна довжина числа 80 біт, з них 1 біт – це знак, 15 – характеристика, 64 – мантиса). З іншого боку використовуємо оцінку, одержану за формулою $\tilde{e}_3 = \left\| \hat{x}_j - \hat{\tilde{x}}_j \right\|_E$. За допомогою цієї оцінки визначається кількість десяткових цифр після коми, яка обов'язково співпадає в спектрі сигналу, що отриманий після ШПФ ($\hat{x}(t)$) та в спектрі, що отриманий після ШПФ, ОШПФ та знову ШПФ ($\hat{\tilde{x}}(t)$). Таким чином ми визначаємо десятковий розряд числа, правіше якого «вкраплювати» повідомлення не має сенсу. Проаналізувавши «коридор» між оцінками $e_3$ та $\tilde{e}_3$ визначаємо перший елемент ключа $\tau_k$. Враховуючи загальну теорію похибок, будемо вважати, що «коридор» десяткових цифр, які можуть слугувати носіями бітів повідомлення лежить в межах між тим розрядом, який дала апріорна оцінка та розрядом на одиницю більшим ніж дала оцінка $\tilde{e}_3$;
3. «*Вкраплення» повідомлення.* Задавши порогове значення $\varepsilon$ (див. співвідношення (4)), визначаємо максимальну кількість інформації, яку можна «вкрапити» в контейнер, та номери відліків спектру куди відбуватимуться «вкраплення». Зчитуємо біти повідомлення та заносимо їх в $\tau_k$ десятковий розряд відібраних відліків. Запам'ятовуємо ключ, по якому можна вийняти повідомлення з контейнера. Виконуємо ОШПФ і отримуємо сигнал $\tilde{x}(t)$, який з точністю до похибки заокруглення співпадає з $x(t)$. Передаємо $\tilde{x}(t)$ та ключ одержувачу. При цьому ключ можна передати як по захищеному каналу зв'язку, так і за допомогою засобів асиметричної криптографії;
4. *Відновлення повідомлення.* Одержувач виконує для отриманого контейнера ШПФ і по ключу «витягає» таємне повідомлення зі спектра.

Можна будувати модифікації даного алгоритму, що використовують в якості контейнера не сформовані за заданими параметрами сигнали, а сигнали, що вже представлені сукупністю своїх відліків.

Зважаючи на багаторазове використання алгоритму ШПФ у реалізації була використана модифікація ШПФ з попередньою заготовкою матриці перетворень [2], що дозволило суттєво скоротити час роботи алгоритму.

Реалізовані версії алгоритму, що «вкрапляють» повідомлення тільки в дійсну частину спектру, тільки в уявну, початок повідомлення – в дійсну, а кінець – в уявну, і навпаки. Ці версії направлені на ускладнення задачі стегоаналізу.

# Підсумки

Дослідження впливу параметрів контейнера на роботу алгоритму показало, що:

1. Чим більше піків має спектр сигналу, тим менша місткість контейнера і тим більша похибка відновлення.

2. Обробці підлягає дійсний сигнал, спектр якого є симетричним. Для збереження симетричності при «вкрапленні» потрібно використовувати тільки першу половину відліків спектра.
3. Очевидно, що повідомлення можна «вкраплювати» або в дійсну частину, або в уявну, або в модуль. З позицій збільшення місткості контейнера найкраще використовувати і дійсну і уявну частини одночасно. Це ніяк не впливає на якість відновлення.
4. Якщо вкраплення відбувається тільки в дійсну, або тільки в уявну частини, то повинна виконуватися умова $N/2 > p$, а якщо в обидві, то $N > p$.
5. Реалізація алгоритму рівномірного вкраплення бітів повідомлення без аналізу спектру сигналу оправдовує себе тільки для класу сигналів з досить рідкими піками.

Для практичного дослідження розглянутого нами спектрального алгоритму було створено комплекс програм, загальним об'ємом 670 Кб. Використано мову програмування Паскаль, тестування проводилося на ПК з процесором CELERON 950 MHz.

# Література

1. Серебренников И.Г., Первозванский А.А. Выявление скрытых периодичностей. – М.: Наука, 1965. – 224 с.
2. Задирака В.К. Теория вычисления преобразования Фурье. – К.: Наук. думка, 1983. – 215 с.
3. Задирака В.К., Мельникова С.С. Цифровая обработка сигналов. – К.: Наук. думка, 1983. – 294 с.
4. Залманзон Л.В. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. – М.: Наука, 1989. – 496 с.
5. Чуи К. Введение в вэйвлеты: Пер. с англ. – М.: Мир, 2001. – 288 с.
6. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія. – К., 2002. – 488 с.
7. Кустов В.Н., Федчук А.А. Методы встраивания скрытых сообщений // Конфидент. – 2000. – № 3. – С. 34-37.
8. Шелест М.Е. Цифровая стеганография и ее возможности // Захист інформації. – 1999. – № 1. – С. 11-19.

Using of the fast orthogonal transforms theory to the developing of constructing computer stenography algorithms is considered.

*Статья поступила в редакцию 11.07.02.*