почве и донных отложениях // Атомная энергия. – 2000. – **88**, вып. 1. – С. 55-60.
6. *Aifantis E.C.* Continuum basis for diffusion in regions with multiple diffusivity // Journal of Applied Physics. – 1979. – **50**, № 3. – P. 1334-1338.
7. *Корн Г., Корн Т.* Справочник по математике для научных работников и инженеров. – М.: Наука, 1979. – 830 с.

Поступила 18.01.2010р.

УДК 683.03

О.Ю.Ю.Афанасьєва

АНАЛІЗ ПАРАМЕТРУ УТАЄМЛЕННЯ ФАКТУ СТЕГАНОГРАФІЧНО УКРИТОЇ ІНФОРМАЦІЇ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Відомим параметром, що характеризує не тільки саму стеганографічну систему (*SS*), а й принцип стеганографічного укриття, є параметр міри невидимості інформації, яка вбудована в цифрове середовище. Цей параметр використовується для характеристики стеганограми (*SG*) та для характеристики цифрових водяних знаків (*CVZ*). Останній відповідає ситуації, коли стороннім користувачам може бути відомим факт існування в даному цифровому середовищі (*CS*) стеганографічно укритої інформації. В цьому випадку, міра забезпечення безпеки, або захист інформації, грунтується, в першу чергу, на основі досягнення високого рівня невидимості вбудованої в *CS* інформації. В даному випадку, не будемо говорити про інші методи підвищення рівня захисту укритої інформації такі як, додаткове шифрування інформації, що укривається та використання інших перетворень самого відображення інформації, що призначена для унеможливлення її розкриття. Для впровадження однозначності в подальшому, приймемо наступні визначення.

Визначення 1. Всі перетворення інформаційного образу (*IO*) , які здійснюються з ціллю забезпечення захисту інформації від її розкриття неуповноваженим користувачем (*NK*) будемо називати додатковими стеганографічними перетвореннями (*DSP*).

Визначення 2. Розширеними стеганографічними перетвореннями (*RSP*) будемо називати такі перетворення *CS* , які направлені на укриття інформації в *CS* та забезпечують підвищення рівня її захисту, що забезпечується збільшенням величини значення параметру невидимості (η) вбудованої в *CS* інформації.

Прикладом *DSP* можуть служити перетворення *IO* з допомогою шифрування [1]. Прикладом *RSP* можуть служити перетворення

натурального простору представлення графічних образів, що використовуються в ролі CS, в частотно-часовий простір, що можна реалізувати на основі використання перетворень Фур'є, або вейвлет перетворень [2,3].

Основною відмінністю CVZ від SS являється наступне. Для CVZ характерним є те, що NK може знати про те, що в даному середовищі присутня стеганографічно укрита інформація. У випадку SS, NK не знає, чи укрита інформація в CS присутня, чи ні. Тому в SS може використовуватися не тільки параметр η, а й параметр, який визначає міру уявненості факту наявності в CS укритої інформації від NK. Параметр, який визначає міру уявненості інформації у відповідному CS, будемо позначати символом μ. В загальному випадку можна вважати, що параметр μ в значній мірі відображає суб'єктивні властивості окремих NK, оскільки один з NK може вважати, що в деякому середовищі є укритий IO, а у іншому його не має. Щоб уникнути такого суб'єктивізму, при визначенні величини параметру μ, приймемо слідуюче. Будемо розглядати деяке CS, в якому можуть бути виділені окремі фрагменти CS_i, в яких буде розміщатися інформація, яку передбачається укривати. Такі фрагменти CS_i з CS будемо називати контейнерами, або стеганографічними контейнерами (SKO). В цьому випадку, параметр μ будемо розглядати в рамках наступних умов.

Умова 1. NK відомо, що в CS не існує SKO, в якому укрита інформація, або в CS не існує SG.

Тоді суб'єктивні фактори, які можуть відрізняти одного NK_i від NK_j з точки зору величини параметра μ, будуть еліміновані наступною умовою, яку необхідно прийняти у зв'язку з введенням параметра μ і ця умова може бути сформульована наступним чином.

Умова 2. CS, в цілому не повинно семантично бути розподіленим на фрагменти CS_i, які з точки зору NK не можуть використовуватися для укриття інформації.

Якісно, приведені умови полягають у наступному. Суб'єктивне рішення окремого NK_i про можливість існування в даному CS укритої інформації приймається як подія випадкова, по відношенню до всіх існуючих в системі передачі даних CS. Ця подія залежить від випадкової події появи NK_i серед всіх можливих NK. Крім того, в певному CS завжди існує деяка множина CS_i, яка придатна для розміщення в ній SG, що також може привносити вклад випадковості, яка може використовуватися, для компенсації фактору суб'єктивності зі сторони NK_i. Очевидно, що умова 2 не означає, що абсолютно всі фрагменти CS_i з CS можуть бути придатними для вбудовування IO. В рамках SS повинні існувати алгоритми, або процедури,

які, у відповідності з певними критеріями, вибирають ті, або інші CS_i, для використання їх в якості контейнера.

Приймемо, що вибір CS_i з CS здійснюється у відповідності із співвідношенням:

$$CS_i = SK(CS),$$

де SK - стеганографічний ключ, для вибору контейнера. Таким чином, параметр μ може визначатися властивостями SK.

Оскільки, значення параметра η визначається різними факторами, які характеризують міру придатності окремих елементів SKO до невидимого укриття елементів інформаційного образу (EIO) у вибраному контейнері, або деякому CS_i, то доцільно, в рамках алгоритму вибору SKO і, відповідно, в рамках SK передбачити такі ознаки і критерії, які не зменшували б міри невидимості, при розміщенні відповідного IO у вибраному SKO.

Вирішення цієї проблеми можливо наступними способами:

- використанням інтегральних параметрів, які аналогічні параметрам, що використовуються SS, при розміщенні IO в SKO і формуються на основі параметрів, що використовуються на рівні аналізу SKO системою SS,
- визначення параметрів, які характеризують CS в цілому і можуть бути зв'язаними з технічними аспектами, що пов'язані з вбудовуванням інформації в CS,
- визначення параметрів, що характеризують CS з точки зору зовнішніх особливостей, що пов'язані з відповідним середовищем.

Перший підхід представляється найбільш природним, оскільки, визначення параметру утаємлення розглядається, як розвиток, або узагальнення параметру невидимості, який досить інтенсивно досліджується і має загально прийняту інтерпретацію [4].

Розглянемо більш детально другий підхід. Однією з загальних умов використання CS для визначення в ньому контейнера, є вимога, відповідно до якої розмір CS повинен бути більшим від передбачуваного контейнера. Ця умова може бути описана наступним співвідношенням:

$$\{[CS = k(SKO)] \& (k > 1)\}.$$

Для параметра μ в рамках даного співвідношення природно допустити, що μ зростає із збільшенням k. Отже, $\mu = 1$, якщо $k = 1$, тоді $CS = SKO$ і місце розміщення IO визначається однозначно розмірами SKO. Щоб приведену початкову умову можна було виконати, то μ з k повинно бути зв'язане логарифмічною залежністю, яку запишемо у вигляді:

$$\mu = A \ln k, \qquad (1)$$

де A деякий вираз, що описує залежність μ від інших параметрів CS,

якими останнє характеризується.

Наступним параметром, який тісно пов'язаний з параметрами, що характеризують SS, є зашумлення CS. Природно припустити, що що будь яке середовище CS, особливо, якщо воно передається в просторі цифрової мережі, зазнає зашумлення. Впровадження інформації у вибраний фрагмент CS, або в SKO також може розглядатися, як деяке зашумлення. В цьому випадку, в середовищі CS може існувати неоднорідне зашумлення по всьому середовищу. Природно припустити, що зашумлення CS по всьому середовищу є рівномірним з точки зору спектральної потужності шуму, оскільки можна прийняти, що в процесі проходження CS через один і той же цифровий канал, на протязі всього розміру CS діють одні і ті ж причини зашумлення, або одні і ті ж джерела шуму. Тому, одним з параметрів CS, який можна прийняти незалежним, з точки зору методів впровадження інформації в CS, від параметра η, якщо останній забезпечує задану величину невидимості, є спектральна густина сигналу зашумлення. В даному випадку, спектральна густина шуму в CS розглядається на вході каналу і на виході каналу передачі CS. Вхід і вихід каналу будемо ідентифікувати з джерелом, в якому формується SG та користувачами, серед яких є адресат, якому призначена SG. Спектральна густина шуму обчислюється на вході каналу і позначається G_{xx} та обумовлюється вбудованим повідомленням, а спектральна густина шуму на виході каналу, який обумовлений зашумленням каналу позначається G_{yy}. Для аналізу шуму в CS розглядається взаємна спектральна густина G_{xy}. Тоді, для аналізу можна використовувати функцію когерентності [5], яка описується наступним співвідношенням:

$$\gamma_{xy}^2(f) = [\mathrm{I}G_{xy}(f)\mathrm{I}^2]/[G_{xx}(f), G_{yy}(t)] \ .$$

Змістовна суть $\gamma_{xy}^2(f)$ допускає в рамках μ наступну інтерпретацію. Якщо в середовищі CS $\gamma_{xy}^2(f)$ для шуму, який є в CS міняється нерівномірно, то це може означати, що в CS вибрано SKO, в який вбудовано IO, що приводить до зміни рівномірності величини $\gamma_{xy}^2(f)$ у відповідному фрагменті CS. Оскільки вбудований IO реалізується на вході каналу SS, то, для визначення величини $\gamma_{xy}^2(f)$, будемо її диференціювати по змінній x і тоді можна записати наступне співвідношення:

$$\delta_x[\gamma_{xy}^2(f_{sz})] = d[\gamma_{xy}^2(f_{sz})]/d[x(t_{sz})] ,$$

де f_{sz} - частота шумової складової інформаційного сигналу, який описується в CS. По відношенню до розміру CS, який визначається величиною k, частотну складову можна розглядати по відношенню до k, як адитивну змінну. Тому, співвідношення (1) можна записати у наступному вигляді:

$$\mu = A_1\{\delta_x[\gamma_{xy}^2(f_{sz})] + \ln k\}, \quad (2)$$

де A_1 можливе розширення залежності (2).

Зовнішні характеристики, що характеризують CS, в першу чергу, стосуються семантичних особливостей. До таких особливостей можна віднести наступні:

- тип CS,
- інформаційна однорідність CS,
- параметри CS, що характеризують семантичні властивості інформації в IO,
- функціональна орієнтація інформації, що розміщається у відповідному середовищі.

До типів CS можна віднести:

- графічне CS,
- аудіо CS,
- мультимедійне CS,
- текстове, або символьне CS і інші.

Інформаційна однорідність визначається мірою цілісності сюжету в CS інформації, яка розміщується в середовищі. Інформаційна однорідність має різну міру в залежності від типу CS. Це обумовлюється можливістю відтворення того, чи іншого сюжету у різних середовищах. Наприклад, найбільшої однорідності можна досягнути у випадку використання текстових середовищ, для яких розмір CS не впливає на міру інформаційної однорідності.

Семантичні властивості інформації в IO являються одними з найважливіших параметрів, оскільки будь який користувач, в тому числі, неуповноважений до отримання укритої інформації, в першу чергу, використовує семантичний зміст відповідного IO. Різні типи IO відрізняються між собою мірою відображення семантики образу у вигляді інтерпретаційних описів. В найбільшій мірі інтерпретаційними описами IO забезпечуються текстові типи CS. Це зв'язано з тим, що вихідною формою представлення будь якої інформації, в основному, є мова, на якій спілкуються споживачі і, тому, остання використовується як засіб відображення IO, який має найбільші можливості для відображення семантики IO. Наступним, по своїх інтерпретаційних можливостях, є графічний тип CS. Проміжним між графічним і текстовим є мультимедійне середовище, оскільки в ньому відображається динаміка графічних образів, яка в певній мірі інтерпретує статичні графічні образи. В найменшій мірі по своїх інтерпретаційних можливостях є музикальні образи. В даному випадку, підкреслюється, що мова йде про музикальні образи, оскільки звукові образи можуть відображати текстові IO.

В рамках проблематики, що пов'язана з визначенням μ, важливою

задачею є визначення міри, або величини значення μ, для кожного окремого випадку стеганографічного укриття інформації в CS. У зв'язку з цим, сформулюємо наступні визначення.

Визначення 3. Технічна модифікація CS має місце тоді, коли остання не приводить до зміни семантики IO.

Під зміною IO в CS будемо розуміти не тільки зміни, що стосуються вихідного IO, а й зміни, які можуть розширяти семантику модифікованого IO. Наприклад, якщо, в результаті модифікації фрагмента CS, що вміщає IO, появляються елементи образу, що безпосередньо не впливають на семантику основного IO і представляють собою точки, плями чи інші елементи можуть спричинити до зміни семантики IO.

Визначення 4. Семантична модифікація CS має місце в тому випадку, коли в результаті вбудовування інформації в CS в IO вносяться зміни, що приводять до зміни семантики в IO.

Прикладом таких модифікацій може служити зміна кольору окремих елементів образу IO та інші. Приймемо, що довільний IO має еталонний IO, або IO^E, якщо існує інтерпретаційний опис відповідного образу. Очевидно, що в більшості випадків має місце співвідношення:

$$\forall(IO_i)[\Delta I_i = \mathrm{I}IO - IO^E\mathrm{I}]. \qquad (3)$$

Це означає, що IO являється еталоном тільки в тому випадку, якщо існує деяка множина IO таких, що виконується співвідношення:

$$\{[IO^k = \{IO_1^k,...,IO_n^k\}]\&[\forall(IO_i^k)[\Delta I_i \neq 0]\} \rightarrow \forall(IO_i^k)\exists(IO^{Ek}). \qquad (4)$$

Точність опису образів та їх відхилень від еталонів у співвідношеннях (3) і (4) визначається точністю інтерпретаційних описів відповідних образів, які будемо позначати символом $j(IO_i)$. Приймемо, інтерпретаційний опис $j(IO_i^k)$ представляється на природній мові споживача в нормалізованій формі, яка впорядковується у відповідності з семантичними акцентами важливості окремих елементів IO. Нормалізація опису полягає у використанні в текстових описах лише ключових слів та виключенні надмірностей, допоміжних граматичних виразів та слів. Під акцентною впорядкованістю розуміється таке розміщення тексту опису інтерпретації, при якому на початку опису $j(IO_i)$ розміщаються ті елементи $j_i(IO_i)$, які в рамках даного IO_i мають найбільшу семантичну значимість, з точки зору інформації, що передається через IO_i. Наступним $j_{i+1}(IO_i)$ розміщається елемент опису IO_i, який має слідуюче по значимості для інтерпретації IO_i значення і т.д. Приймемо, що $j_i(IO_i)$ представляє собою окрему фразу тексту $\varphi_i(IO_i)$. Однією з базових функцій еталону IO^E образу IO_i є визначення акцентів впорядкованості опису $j_i(IO_i)$ для образів IO^K класу

K. Приймемо, що IO^E для класу образів K вміщає повне семантичне представлення відповідного IO_i^K. Очевидно, що в технічних застосуваннях еталонні образи використовуються в формі різних варіантів їх базового відображення, яке будемо називати базовим забезпеченням відповідного еталону. Введення уявлення про базове забезпечення IO^E, яке будемо позначати $B_i(IO^E)$, пов'язане з тим, що IO^E переважно використовуються для розпізнавання образів. Основний принцип розпізнавання IO_i полягає у тому, що текучий образ IO_i співставляється з рядом еталонів і у випадку його співпадання з одним з них, такий образ ідентифікується як такий, що відноситься до класу образів K. Тому, будемо вважати, що $j_i(IO_i)$ можна представляти, як опис семантики IO_i, який має змінну величину значимості, в залежності від кількості $j_i(IO_i)$, що включаються у $j(IO_i)$. У відповідності з уявлення про акцентовану впорядкованість $j(IO_i)$ приймемо, що міра семантичної значимості $j_i(IO_i)$, для опису семантики IO_i визначається величиною акцента, яка приписується фразам $\varphi_i[j_i(IO_i)]$, що складають текстовий опис $j(IO_i)$ та номером місця розміщення φ_i в $j(IO_i)$. У відповідності з нормалізацією опису $j(IO_i)$, приймемо, що φ_i з найвищими акцентами розміщаються на початку опису $j(IO_i)$. Якщо представити $j(IO_i)$ у вигляді послідовності фраз φ_i, то можна записати співвідношення:

$$j(IO_i) = \varphi_1^i * \varphi_2^i * ... * \varphi_m^i ,$$

де кожна φ_j^i має величину акценту ξ_j, при чому, $(j < k) \to (\xi_j > \xi_k)$. Щоб відійти від абсолютних величин ξ_j, приймемо, що $(\sum_{j=1}^{m} \xi_j) = 100\%$ для IO_i. В графічних образах може мати місце ситуація, коли IO_i в CS відповідає еталонному образу лише на $\alpha\%$. Це в свою чергу означає, що можна здійснювати семантичну модифікацію IO_i з CS таку, що:

$$[(IO_i) + (\Delta(IO_i))] \to [j(IO_i + \Delta I_i) \le j(IO^E)] .$$

Для того, щоб перейти до кількісної оцінки величини семантичної модифікації, яка буде черговою компонентою параметра μ, приймемо наступні умови і визначення.

Визначення 5. Образ IO_i буде представлений в неповній семантичній формі, якщо величина суми його акцентів менша суми акцентів його повного еталону.

Це визначення формально можна записати наступним чином:

$$[\sum_{i=1}^{k} \xi_i(IO^k)] < \{\sum_{i=1}^{m} \xi_i[P(j(IO^{kE}))]\} ,$$

де $P(j(IO^{kE}))$ - повний опис інтерпретації образу IO^k класу K, що являється еталоном, для IO^k. Оскільки, при впровадженні повідомлення V_i в CS, не можливо узгодити по всьому CS або по всіх елементах IO^k модифікацію їх семантики таким чином, щоб відповідна модифікація була однакова, для всіх компонент IO^k, то можна написати наступне співвідношення:

$$\lambda_i(IO_i) = \mathrm{I}[\sum_{i=1}^{k(i)} \xi_i(IO_j)] - \xi_p(IO_P^E)\mathrm{I} .$$

Складову для μ, що відображає модифікацію семантики в IO_i з CS, будемо позначати s_i. Для її визначення запишемо наступне співвідношення:

$$\{[[\lambda_i(IO_i) - \chi] \geq 0] \rightarrow (s_i = s_i + 1)\} \,\&\, \{[[\lambda_i(IO_i) - \chi] < 0] \rightarrow (s_i = s_i)\} , \qquad (5)$$

де χ - порогове значення різниць сум ξ_i між образами IO_i та IO_P^E. Тоді співвідношення (2) можна розширити наступним чином:

$$\mu = s_i(CS) + \delta_x[\gamma_{xy}^2(f_{sz})] + \ln k . \qquad (6)$$

Приймемо наступну умову використання окремих компонент EIO_i з IO_i.

Умова 3. Якщо в IO_i з CS використовується компонента EIO_i з IO_i, яка має власне семантичне значення, що обумовлює наявність відповідного еталону IO_i^E і EIO_i має не повну семантичну інтерпретацію, то $j(EIO_i) = \varphi_1 * \ldots * \varphi_k$ повинна мати найвище значення акцептації з повного інтерпретаційного опису $j(IO_i)$.

Приведена умова означає, що у випадках, коли в графічних або яких небудь інших символьних образах IO_i відсутні компоненти інтерпретаційного опису, то від повідні φ_i, що описують окремі фрагменти інтерпретаційного представлення, відповідають елементам такого представлення в IO_i^E, що мають максимальні значення ξ_i.

На якісному рівні, в певному наближенні, приведена умова означає, що коли графічний образ сформовано таким чином, щоб він відображав певний об'єкт, або деяку сутність з певним семантичним наближенням, то для цього використовуються такі елементи відповідного образу, які є найбільш інформативними для даного IO_i. Це означає, що такі компоненти мають більше значення ξ_i по відношенню до елементів, які використовуються при реалізації IO_i, але існують в IO_i.

Співвідношення (6) дозволяє здійснювати моніторинг CS з ціллю виявлення факту наявності V_i в CS на основі аналізу семантичних модифікацій, що обумовлюються введенням V_i в CS.

Співвідношення (6) доцільно розділити на дві частини одна з яких має відношення до технічних модифікацій, а друга до семантичних модифікацій CS. Такий розподіл грунтується на тому, що технічна модифікація CS, при вбудовуванні V_i не завжди може безпосередньо переходити в модифікацію семантичну. Щоб забезпечити такий перехід, необхідно провести дослідження можливості відповідного звязку, що не являється предметом досліджень в даній роботі. Тому, розглянемо більш детально модифікацію CS, що обумовлюється вбудовуванням в CS інформації IO_i. Якщо в якості CS вибираються графічні образи, або інші символьні середовища, то необхідно ввести наступну умову.

Умова 4. При використанні графічних CS для вбудовування V_i, не доцільно використовувати IO_i, що мають загально відомі еталони.

Зразком графічного образу являється такий образ, який в тій, чи іншій мірі являється відомим, або являється еталоном і тому ті чи інші відхилення в його семантиці, чи структурі можуть бути легко розпізнані. Тому CS, в які передбачається вводити V_i на основі використання семантичних модифікацій, доцільно формувати спеціально, наприклад, з використанням стандартних графічних пакетів [5], або зображення, що отримані на основі використання цифрових знімків. Використання семантичної модифікації в графічних CS потребує розв'язку наступних задач:

- створення універсального методу кодування повідомлень відповідними модифікаціями,
- створення методів семантичного аналізу графічного середовища,
- дослідження параметрів невидимості, який розглядається як семантична невидимість.

Перша задача, по суті, представляє собою створення перетворень текстових повідомлень, які дозволили б перевести останні в форму елементів графічних образів, або у способи представлення коду текстів у коди образів. Друга задача тісно пов'язана з першою, оскільки, основою семантичного аналізу є аналіз можливостей перетворень $V_i \to IO_i$. Третя задача пов'язана з інтерпретацією семантичних перетворень в їх технічній реалізації.

1. *Смарт Н.* Криптография. М.: Техносфера, 2005.
2. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М.: Мир, 1989.
3. *Чуи К.* Введение в вейвлеты. М.: Мир, 2001.
4. *Афанасьева О.Ю.* Звязок стеганографічних параметрів з параметрами графічних образів.// Зб. наук. Праць "Моделювання та інформаційні технології", ІПМЕ НАН України, 2006.
5. *Бендат Дж., Пирсол А.* Прикладной анализ случайных данных. М.: Мир, 1989.

Поступила 17.02.2010р.