УДК 683.03

О.Ю.Афанасьєва

АНАЛІЗ ПАРАМЕТРІВ СТЕГАНОСИСТЕМИ, ОРІЄНТОВАНОЇ НА ВИКОРИСТАННЯ ГРАФІЧНИХ ЦИФРОВИХ СЕРЕДОВИЩ

Загальна організація стеганосистеми (SS) повинна забезпечувати можливість автоматизованого виконання всіх функцій, які є необхідними для реалізації процесу укритого способу передачі інформації. Таку організацію розглянемо на прикладі SS, яка використовує графічне цифрове середовище в якості інформаційного потоку, оскільки останнє найбільш широко використовується у відомих SS [1].

Загальна організація SS в значній мірі обумовлюється процесом реалізації основних функцій SS. Такий процес можна представити у вигляді наступної послідовності дій та функцій.

1. Попередній аналіз та технологічне перетворення повідомлення.
2. Вибір компонент цифрового середовища (CS), в яких передбачається розміщати повідомлення.
3. Формування структури інформаційного потоку, що створюється з CS.
4. Визначення окремих залежностей між повідомленням (W_i) і інформаційним CS та вибір для W_i контейнера (KW).
5. Технологічні перетворення KW.
6. Впровадження W_i в KW та формування стеганограми (SG), або $W_i \,\&\, KW \rightarrow SG$.
7. Обернене перетворення SG і розміщення його і розміщення його в CS.
8. Аналіз стеганографічних параметрів SG та інформаційного потоку, що вміщає SG.

Спосіб реалізації приведеної послідовності загально описаних функцій залежить від параметрів, що характеризують SS в цілому та характеризують окремі компоненти, що входять в SS. Основні параметрами, що входять в SS визначаються наступним чином:

- невидимість впровадженого в CS повідомлення (η),
- міра утаємнення W_i в CS (μ),
- стійкість SG до технологічних перетворень (λ),
- розмір повідомлення (d_i),
- міра допустимих спотворень повідомлення ($\aleph$),
- час актуальності повідомлення (τ),

- розмір контейнера для повідомлення (h_i),
- модель чутливості по параметру p_i, що позначається як (m^i),
- розмір CS, що позначається символом (π),
- інформаційна узгодженість окремих компонент інформаційного потоку, що реалізується в цифровому середовищі (σ),
- пропускна здатність стеганоканалу (Λ),
- семантична надмірність повідомлення (χ).

Невидимість η є одним з важливих параметрів SS і на якісному рівні визначає міру, що тісно пов'язана з можливостями системи людського зору. Тому, її визначення доцільно привести на якісному рівні.

Визначення 1. Невидимість η визначає міру неможливості системи людського зору виявити впроваджене W_i в CS, при перегляді відображення CS, яке передбачає певну інтерпретацію відповідного середовища.

На основі якісного визначення уявлення про η не доцільно розглядати методи вимірювання її величини та всі інші питання, що пов'язані з цим параметром.

Утаємлення μ представляє собою параметр, який визначається параметрами SG та параметрами інформаційного потоку, що реалізується на основі використання CS. Очевидно, що величина μ тісно пов'язана з величиною η оскільки зрозуміло, що при зміні значення η може мінятися значення μ. Більш того, в рамках SS можуть використовуватися механізми впливу на параметр η. Наприклад, якщо в результаті впровадження W_i в CS, появилися видимі для системи людського зору (SLZ) модифікації CS, які просторово зв'язані з місцем розміщення елементів $\varpi_{ij} \in W_i$, то шляхом впровадження певним способом, наприклад, випадковим, або у вигляді певного шуму, у відповідне CS додаткових модифікацій, можна досягнути зменшення величини μ. При цьому, величина η залишається без змін. У зв'язку з тим, що параметр μ залежить від цілого ряду факторів, серед яких є фактори зовнішнього характеру, наприклад, наявність інформації про те, що деякий потік інформації може використовуватися для передачі стеганографічно укритого повідомлення, то впровадимо визначення параметра μ, яке буде відображати більш вузький та, по суті, технічний аспект цього параметру.

Визначення 2. Утаємнення μ визначає міру інтерпретаційної узгодженості інформаційного потоку, який переглядається неупередженим споживачем.

Параметр стійкості до технологічних перетворень λ представляє собою лінійну залежність окремих стійкостей по відношенню до окремих

технологічних перетворень, що записується у вигляді:

$$\lambda = \sum_{i=1}^{n} \alpha_i \lambda_i ,$$

де λ_i - стійкість по відношенню до i - того технологічного перетворення, кожний окремий λ_i визначається специфікою взаємодії даного технологічного повідомлення з інформаційним потоком, α_i - визначає міру домінування даного перетворення над іншими перетвореннями, що враховуються, при визначенні λ. До найбільш типових технологічних перетворень відносяться наступні [2]:

- компресія і декомпресія,
- фільтрація,
- перетворення форматів і т.д.

Очевидно, що до змін в CS може припровадити тільки компресія з втратами. Оскільки існує цілий ряд такого типу компресій, то величина λ_i залежить від конкретного типу алгоритму компресії. В загальному випадку, стійкість визначається мірою протидії відповідних компонент SS спотворенню в SG і, відповідно в CS.

Розмір повідомлення являється одним з ключових параметрів, який визначає певний спосіб формування контейнерів та структури інформаційного потоку. Однією з функцій SS є пристосування W_i до можливостей CS. Одне з таких пристосувань полягає у зміні величини d_i. Прикладом таких змін може служити кодування W_i, оскільки приймається, що W_i представляє собою опис повідомлення на природній мові користувача, а його впровадження в CS реалізується у вигляді бітових кодів відповідного повідомлення. Кодування може полягати у перетворенні опису повідомлення в іншу форму, при умові, що відповідний алгоритм є обернений, однозначний і відомий, що найменше, адресату повідомлення. Доцільність зміни величини параметру d_i обумовлюється наступними факторами:

- при збільшенні співвідношення між загальною довжиною інформаційного потоку повідомлення π і розміром повідомлення d_i, збільшується параметр утаємлення μ,
- використання додаткових кодувань W_i дозволяє підвищити рівень семантичної узгодженості σ, якщо алгоритми кодування вибираються орієнтованими на CS.

Міра допустимих спотворень повідомлення $\aleph$ визначається семантичною надмірністю повідомлення та досить широко використовується в SS. Прикладом такого зміни величини $\aleph$ може служити використання кодів, що виправляють помилки, а це приводить до збільшення величини $\aleph$ на рівні кодування. Зменшення величини $\aleph$ на семантичному рівні може

полягати у нормалізації повідомлення, що приводить до скорочення d_i і, відповідно, до збільшення η, при заданих розмірах CS. Крім того, розширення тексту без зміни його семантичного значення дозволяє підвищити величину λ і т.д.

Час актуальності повідомлення впливає на вибір способу функціонування SS, які відрізняються один від одного використанням тих, чи інших процедур. Очевидно, що цей параметр тісно зв'язаний з інтегральним параметром, що характеризує стійкість SG по відношенню до різних типів атак на SG. В даному випадку, приймається, що використання процедур в рамках SS, що є додатковими по відношенню до базових процедур, приводить до підвищення стійкості SG по відношенню до атак. Однією з мір стійкості до атак є час, який необхідно затратити на виявлення в CS повідомлення і видобування його з CS. Величина цього параметру залежить від цілого ряду факторів, які обумовлюються додатковими перетворюваннями та особливостями системи стеганоаналізу (SSA).

Розмір контейнера h_i тісно зв'язаний з розміром повідомлення, але такий зв'язок не являється безпосереднім в, в більшості випадків, він не апроксимується лінійною залежністю. Це обумовлюється наступними причинами. Збільшення розмірів контейнера KW дозволяє, при дотриманні певних вимог, підвищити рівень η і, відповідно, μ. Підвищення η досягається за рахунок зменшення рівня спотворення в SG, якого складно уникнути, при впровадженні W_i в KW. Приймаючи, що вибраний KW по відношенню до ознак, по яких вибираються місця розміщення елементів W_i є однорідним і розширення KW не порушує таку однорідність, то можна вважати, що має місце співвідношення:

$$\eta_i = \alpha d_i + b .$$

Модель чутливості по параметру $p_i(m^i)$ є однією з базових компонент SS, оскільки на основі такої моделі m^i визначається значення η. Модель m^i описує залежність між параметрами, що характеризують візуальні можливості системи людського зору та параметрами, які характеризують основні параметри SS, наприклад, параметри η та μ [3]. Очевидно, що для досягнення більш високого значення η та μ доцільно використовувати модель $M = F(m^1,...,m^k)$, де кожна з m^i може бути зв'язана з окремим параметром, що характеризує візуальні характеристики образу. В цьому випадку, укриття W_i в CS реалізується по всіх візуальних характеристиках образу. Використання окремої моделі m^i, чи сукупності моделей визначається характером образу. Наприклад, існують образи, що в основному, характеризуються такими параметрами, як контрастність, всі інші

параметри у порівнянні з ним являються мало ефективними. Якщо позначити параметри, що характеризують візуальні властивості образу символом P^0, і відповідні їм параметри моделі чутливості людської системи зору p_i^m, то характер моделі, що вибирається для реалізації її в SS зв'язаний з η у відповідності з наступним співвідношенням:

$$\eta_j = f\{p_j^0, [\varphi(p_i^m)], \alpha m^i\},$$

де α - коефіцієнт ефективності моделі m^i, при її використанні для визначення величини η_j.

Розмір цифрового середовища π впливає і, в значній мірі визначає, величину параметра μ. Інтуїтивно, така залежність очевидна, оскільки, чим більший розмір інформаційного середовища по відношенню до розміру повідомлення, тим менш помітним може бути факт розміщення W_i в CS, при заданому d_i. Якщо не приймати інші фактори, що впливають на величину μ, такі як додаткова інформація про стеганоканал (SK), чи спотворення в CS, то можна прийняти лінійну залежність між μ і π, яка визначає нижню границю величини μ. Очевидно, що при збільшенні π і заданому d_i існують порогові значення π, після яких лінійна залежність $\mu_i = \beta\pi_i$ переростає у нелінійну залежність, яка приводить до нелінійного збільшення μ. Це означає, що не лінійність приводить до більш швидкого зростання μ з ростом π ніж це відбувається у випадку $\mu_i = \beta\pi_i$.

Семантична узгодженість окремих компонент інформаційного потоку σ, як параметр SS представляє собою в більшій мірі параметр, який характеризує можливості системи зору людини на її психофізіологічному рівні. Оскільки систему людського зору описати на потрібному формальному рівні досить складно, то уявлення про цей параметр доцільно інтерпретувати в рамках методів відображення відповідного інформаційного потоку. Визначення σ у випадку текстового відображення інформаційного потоку ґрунтується на використанні граматики мови, що використовується для формування відповідного тексту [4]. У випадку графічних образів ситуація більш складна, оскільки, на відміну від мови, у графічних образів відсутній загально прийнятий аналог алфавіту. Це не дозволяє формувати правила побудови образів у відповідності з правилами, які були б аналогічні граматичним правилам. Тому, у випадку використання потоків інформації, що відображаються у вигляді графічних образів, необхідно формувати індивідуальний алфавіт. Такий алфавіт не мусить відображати лише закінчені елементи, що мають загально прийняту інтерпретацію. Такими елементами можуть бути такі фрагменти образу, які мають достатньо індивідуальних ознак, якими вони можуть виділятися по відношенню до інших фрагментів образу. Наприклад, таким фрагментом може бути частина образу, яка

виділяється на основі свого кольору, який є контрастним для найближчого оточення, фрагмент образу може представляти собою деяку аналогію або асоціацію з компонентою, що має загально прийняту інтерпретацію і т.д. В загальному, у всіх випадках, коли відсутня загально прийнята обмежена сукупність елементів, яку можна було би вважати аналогом алфавіту, з допомогою яких формуються більш складні конструкції, то використовуються методи накопичення елементів, що складають досліджувані конструкції у вигаді деяких баз даних. В рамках таких баз даних вибираються базові елементи і в подальшому останні використовуються для аналізу відповідних конструкцій, або об'єктів. У випадку графічного інформаційного потоку такими конструкціями являються окремі образи, що виділяються окремим сюжетом, а елементами являються графічні компоненти образу, що описуються власними інтерпретаційними описами. Відповідні елементи з власними інтерпретаційними описами формують певну базу даних. В цьому випадку, параметр семантичної узгодженості визначається і обраховується його значення по інтерпретаційних описах, які представляють собою текстову інформацію на природній мові користувача.

Пропускна здатність стеганоканалу Λ досить широко використовується в дослідженнях SS. На якісному рівні, Λ означає кількість інформації в W_i, яку можна укрити в контейнері KW розміром h_i. В більшості випадків, цей параметр визначається співвідношенням розміру d_i повідомлення до розміру KW, в якому укривається W_i, що описується наступним співвідношенням:

$$\Lambda = \alpha d_i / h_i ,$$

де α - коефіцієнт розмірності.

Семантична надмірність повідомлення χ представляє собою досить важливий параметр повідомлення і SS в цілому. Цей параметр визначається для нормалізованих форм W_i. Це означає, що вона не пов'язана з надмірністю, що обумовлюється синтаксисом мови, не може обумовлюватися використанням неоднозначних елементів мови для опису деякої семантики, чи іншими можливостями, що існують в рамках граматики природної мови. Семантична надмірність, на якісному рівні, визначається наступними особливостями:

- суть семантично надмірного W_i може бути виражена більш коротким повідомленням по відношенню до сформованого повідомлення, при цьому, обидва варіанти повідомлення є нормалізованими,
- з семантично надмірного W_i можна вилучити фрагмент $\varpi_i \in W_i$ таким чином, що по $W_i - \varpi_i$ можна відновити семантичну суть оригінального повідомлення W_i,
- параметр семантичної надмірності залежить від способу її реалізації у

відповідному повідомленні.

Перша і друга особливість не потребують коментарів. Третя особливість пов'язана з технічними аспектами її використання. Семантична надмірність використовується в тому випадку, коли W_i, по визначенню, може спотворюватися перш ніж буде отримана адресатом. Тому, від природи механізмів спотворення залежить той, чи інший метод синтезу семантично надмірного W_i. Наприклад, коли спотворення можуть носити в межах тексту W_i випадковий характер, то семантична надмірність повинна формуватись таким чином, щоб такі спотворення можна було елімінувати. З викладеного видно, що параметр χ є досить важливим для SS і залежить від багатьох факторів, що пов'язані з методами формування W_i та окремими технічними параметрами SS.

1. *Cox J., Miller M.L., Bloom J.A*. Digital watermarking. Morgan Kaufman Publizhers, 2002.
2. *Быков С.Ф.* Алгоритмы сжатия JPEG с позиций компьютерной стеганографии.// Защита информации. Конфидент. 2000, N3.
3. *Mlodkowski J.* Aktywnosc wizualna czlowieka. PWN, Warszawa, 2000.
4. *Вольф Е.М*. Функциональная семантика оценки. М.:URSS, 2006.

Поступила 15.01.2009р.

УДК 683.03

Б.В.Дурняк, Т.Равецки

МЕТОДЫ ЛИНЕЙНОГО И НЕЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

Управление предприятием в условиях отсутствия централизованного управления промышленностью и системой хозяйствования обуславливает необходимость в каждом отдельном предприятии решать задачи управления, с учетом особенностей соответствующих предприятий, условий рынка и рыночных отношений между субъектами предпринимательской деятельности.

В процессе функционирования фирмы, возникает целый ряд задач связанных с оптимизацией соответствующих производственных процессов. С формальной точки зрения, каждый процесс функционирования может быть описан в виде некоторой математической модели. В большинстве случаев, описание такого процесса в виде модели требует определенных допущений и ограничений. Такие ограничения представляются приемлемыми, если

