УДК 004.[62+67]

О. Ю. Пузиренко, канд. техн. наук
(Національний авіаційний університет, Україна)

Пропускна здатність стеганографічних каналів на основі аудіоконтейнерів

Представлено спосіб усередненої на множині спектрів звукових сигналів оцінки пропускної здатності стеганографічних каналів на основі аудіоконтейнерів.

Як відомо, метою стеганоаналізу є дослідження мультимедійних моделей стеганографічних систем (СГС) з метою отримання кількісних і якісних оцінок ефективності використовуваного в них стеганоперетворення з аспектів стійкості до можливих видів атак [1]. Для випадку організації стеганографічних каналів передавання даних (СГКПД) на основі цифрових потоків аудіоконтейнерів (АК) є необхідним визначити, наскільки великою може бути отримувана при цьому пропускна здатність (ПЗ) СГКПД і як вона залежатиме від інших характеристик СГС та умов їхнього використання. Під ПЗ СГКПД в АК або просто стеганографічною ПЗ (СГПЗ) в АК розумітимемо максимальну кількість інформації повідомлення, що може бути вбудована до АК у приведенні до одиниці часу тривалості АК (кадру, субсмугового відліку тощо). Додатковою умовою, що при цьому висувається, є безпомилковість передавання приховуваних даних одержувачу, а також їхня стійкість до пасивних і активних атак.

СГКПД створюється всередині відкритого КПД (ВКПД), для якого ПЗ визначається як максимальна кількість інформації АК, яку потенційно можна передати без помилок за одне використання каналу або за одиницю часу [2]. Відтак, оскільки навіть в граничному випадку — при повній заміні всіх елементів стеганоконтейнера на елементи вбудовуваного повідомлення — СГПЗ лиш зрівняється зі значенням ПЗ ВКПД, можна стверджувати, що СГПЗ каналу, в якому за одиницю часу передається незначна кількість елементів повідомлення, не перевищуватиме ПЗ ВКПД. Відношення СГПЗ до ПЗ, визначеної основною швидкістю передавання відкритої інформації АК, являє собою відносний індекс ПЗ СГКПД, що має значення в межах від 0 до 1.

Останніми роками намітилися різні, часом абсолютно протилежні підходи до визначення граничної кількості інформації, що може бути захищена са́ме за допомогою стеганографічних методів. Ці розбіжності, як зазначено в [1], зумовлені відмінністю у цілях захисту інформації, типом противника (його можливостями та реалізованими ним атаками на СГС), видами контейнерів і приховуваних повідомлень та багатьма іншими факторами. Разом із тим, усі підходи до оцінки ПЗ СГКПД можна умовно поділити на такі два класи [1]:

1) орієнтовані на СГС, в яких захищувані повідомлення мають бути безпомилково передані в умовах активної протидії противника. При цьому розглядається сценарій, коли окрім спотворень структури контейнера власне в результаті вбудовування до нього елементів безнадлишкового стеганографіч-

ного повідомлення, можливі як навмисні спотворювання контейнера з боку активного противника, так і ненавмисні випадкові спотворювання внаслідок дії завад у відкритому каналі;

2) застосовувані для оцінки СГПЗ безпосередньо під час вбудовування повідомлень у надлишкових даних контейнера. При цьому береться до уваги, що контейнери формуються реальними надлишковими джерелами, які мають значну пам'ять (корельованість), а оцінки СГПЗ залежать від характеристик замаскованості СГКПД. Підходи такого класу є орієнтованими на СГС, які реалізують стеганографічне передавання даних, апріорі невідомих одержувачеві, причому пасивний противник, спостерігаючи за ВКПД, намагається виявити наявність у ньому СГКПД і, у випадку успіху, — розкрити вміст стеганограми.

З огляду на це, а також беручи до уваги класифікацію [3], можна стверджувати, що випадкові і зловмисні спотворення АК при передаванні останніх по відкритих каналах є підконтрольними вже існуючим системам захисту інформаційного контенту ВКПД, а основною небезпекою для СГКПД є загроза пасивних атак. Точна оцінка СГПЗ при використанні в якості аудіоконтейнерів субсмугових відліків стиснутих звукових чи мовних сигналів, яка була би справедливою для довільних аудіосигналів, є неможливою через очевидні причини ймовірнісного характеру: відмінність жанру, гучності, шумового забарвлення тощо. Тому бачиться за доцільне використати в якості АК середньостатистичний аудіозапис, усереднений спектр якого є близьким до так званого рожевого акустичного шуму [4], що дасть можливість отримати статистично усереднену оцінку СГПЗ та її індексу.

Маючи функціональні залежності від бітових швидкостей R кількості кодованих відліків s рожевого шуму $G_s(R)$ та кількості виділених на таке кодування бітів $Б_{відл.}(R)$, можна визначити усереднену кількість АК $N(R, L, \varphi)$, придатних для заповнення, — з урахуванням порогових значень довжин кодових комбінацій (КК) відліків L і частот їхніх субсмуг φ:

$$N(R, L, \varphi) = \sum_{s=0}^{S(R)-1} [G_s(R) \cdot v(L) \cdot \upsilon(\varphi)], \tag{1}$$

де коефіцієнти $v(L) = \begin{cases} 1 \text{ для } Б_{відл.}(R) > L; \\ 0 \text{ для } Б_{відл.}(R) \le L, \end{cases}$ $\upsilon(\varphi) = \begin{cases} 1 \text{ для } s \ge \varphi; \\ 0 \text{ для } s < \varphi. \end{cases}$

Якщо вважати, що заповнення АК зводиться до модифікації одного біта з L у складі його КК і, таким чином, один контейнер вміщує в собі один біт повідомлення, то усереднену СГПЗ $C(R, L, \varphi)$ створюваного стеганоканалу можна обчислити як віднесення усередненої кількості заповнених контейнерів $N(R, L, \varphi)$ до часу τ, що відповідає тривалості аудіофрагмента (кадру):

$$C(R, L, \varphi) = N(R, L, \varphi) / \tau. \tag{2}$$

Результати експериментів та підсумкових обчислень (1) і (2) для різних значень L та φ при $\tau = 24$ мс наведений на рис. 1.

Як видно з рис. 1, кількість обраних для перенесення елементів повідомлення АК (придатних згідно висунутих до стеганограм вимог з аспектів

стійкості СГКПД до атак) при намаганні зберегти якість звучання кадрів заповнених АК встановленням завищених порогових значень L та φ зменшується. Найбільш суттєво тенденція до зменшення N і, відповідно, C простежується під час встановлення при обранні контейнера обмеження на мінімальну довжину ($Б > L$) КК відліку (особливо це помітно на малих швидкостях R). Заборона вбудовування до відліків НЧ-субсмуг ($s < \varphi$) має своїм наслідком зменшення кількості відібраних для заповнення АК на величину, що відповідає кількості відліків у відкинутих субсмугах. Слід зважати й на те, що в реальних умовах СГПЗ буде змінною величиною не тільки для різних аудіосигналів, але й для різних кадрів в межах окремого аудіосигналу.

Результат обчислення усередненого індексу СГПЗ за формулою

$$I(R, L, \varphi) = C(R, L, \varphi) / R \tag{3}$$

наведений на рис. 2. З графіку видно, що за цілковитої відсутності обмежень на обрання контейнерів або ж тільки при забороні вбудовування до відліків НЧ-субсмуг, СГС з більш низькими швидкостями R характеризуються вищим індексом СГПЗ. Введення процедури обрання АК з достатньою довжиною КК L також має своїм наслідком програш СГС з найбільшою швидкістю R, оскільки за великих бітових швидкостей частка субсмугових відліків, які представлені більш довгими КК, серед усієї множини відліків у межах кадру є значно вищою, аніж це спостерігатиметься при малих швидкостях. Наслідком цього є зменшення загальної кількості придатних до заповнення АК.

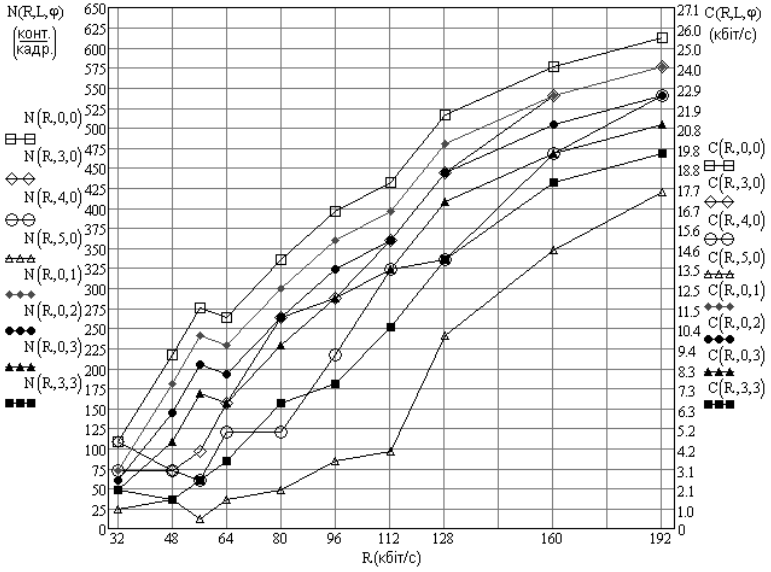

Рис. 1. Усереднена кількість АК, придатних для заповнення в окремому кадрі стиснутого сигналу (ордината ліворуч), і СГПЗ створеного на їх основі стеганоканалу (ордината праворуч), як функції R, L та φ

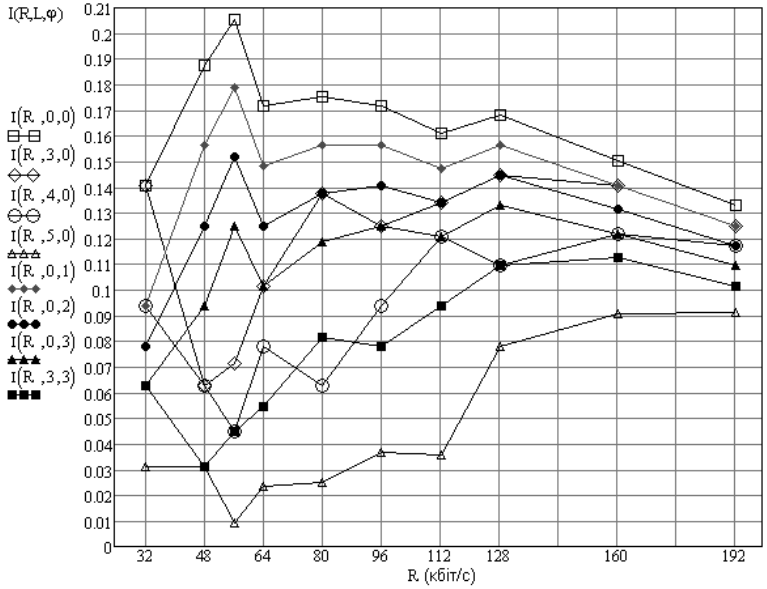

Рис. 2. Усереднений індекс СГПЗ стеганоканалу, як функція R, L та φ

Значення C та індекси I СГПЗ, одержані для різних бітових швидкостей R, порогових значень довжин КК відліків L і частот їхніх субсмуг φ, можуть вважатися гранично досяжними для будь-яких СГС на основі стиснутих АК, не зважаючи на принципи, закладені до основи побудови останніх. Для випадку стереорежиму аудіосигналу представлені вище усереднені показники та індекси СГПЗ СГКПД при одноканальному аудіорежимі мають бути збільшені вдвічі.

Список літератури

1. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.

2. Конахович Г. Ф., Мачалін І. О., Пузиренко О. Ю. Теорія електричного зв'язку : [навч. посіб.]. — [2-е вид., випр. і доп.]. — К. : ТОВ «НВП Інтерсервіс», 2013. — 368 с.

3. Пузиренко О. Ю., Шевченко О. В. Класифікація методів стеганографічного захисту інформації у цифровому звуковому мовленні // Захист інформації в інформаційно-комунікаційних системах : наук.-практ. конф., 7–10 червня 2011 р. : тези доп. — К. : НАУ, 2011. — С. 30.

4. DSP generation of Pink (1/f) Noise [Електронний ресурс] – Режим доступу до ресурсу: https://www.firstpr.com.au/dsp/pink-noise/