УДК 004.056.5(045)

Пузиренко О.Ю.

СИСТЕМА ОБРОБКИ ДОДАТКОВОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ЦИФРОВОГО ЗВУКОВОГО МОВЛЕННЯ

Національний авіаційний університет

Представлено новий спосіб і пристрої системи цифрового звукового мовлення DAB стандарту ETSI EN 300 401 з можливістю стеганографічної обробки циркулюючої в ній інформації шляхом введення до складу MPEG-кодека DAB стеганографічної системи.

Постановка проблеми

Необхідно провести пошук таких шляхів оптимізації цифрового звукового мовлення (ЦЗМ), які б дозволили знайти оптимум у досягненні зросту техніко-економічних переваг від його використання (спектральна ефективність, кількість платних послуг, якість звучання тощо) і надали б можливість організації стійкого і невідчутного людиною – як специфічним приймачем, – стеганографічного захисту інформацій-ного наповнення мереж ЦЗМ.

Аналіз досліджень і публікацій

Відомі способи ЦЗМ (*DAB – Digital Audio Broadcasting*) засновані на механізмах кодування аудіосигналів радіопрограм за відомими стандартами компресії *ISO/IEC MPEG Audio* (*Moving Picture Experts Group Audio*) [1, 2]. Сигнали від декількох радіопрограм перетворюються на стиснені з втратами цифрові потоки, які у подальшому об'єднуються з окремо створеним каналом передавання додаткової інформації (ДІ) (зокрема, сервісної (СІ) і конфіденційної (КІ) інформації) у цифровий потік (ансамбль), який транслюється в окремій смузі частот. У межах загальної і незмінної бітової швидкості передавання ансамблю (1168 кб/с) утворюючим його програмам можуть відповідати різні швидкості (зазвичай від 128 до 384 кб/с). Канал передавання ДІ може мати пропускну здатність (ПЗ) від 16 до 192 і більше кб/с. Кількість програм в ансамблі неоднозначно впливає на характеристики ЦЗМ [3]: їх збільшення веде до зросту спектральної ефективності, але якість звучання програм може стати гіршою чим при аналоговому мовленні; спроба ж підвищити аудіоякість збільшенням бітової швидкості трансляції веде до неефективного використання спектру. Низька якість прийому при ЦЗМ зумовлена слабким згортковим кодуванням, а введення додаткової надмірності вестиме до погіршення аудіоякості або ж до зменшення спектральної ефективності – оскільки за незмінної загальної бітової швидкості ансамблю треба або знижувати індивідуальну швидкість передавання аудіопотоків, або зменшувати кількість трансльованих в ансамблі програм. Розширення переліку і форм подання ДІ викликає необхідність створення для неї каналу з ПЗ, що стає порівнянною або навіть більшою за ПЗ каналу окремої аудіопрограми. Це також веде до неекономного використання РЧР або ж до погіршення якості звучання. Огляд структурних одиниць системи ЦЗМ [1] вказує на можливість модифікації мультиплексу (механізмів транспорту-вання), завдяки резервуванню груп, полів і міток при його організації. Разом з тим, базовими стандартами аудіокомпресії передбачено, що будь-який кодер, здатний створити коректно скомпресований цифровий потік, може вважатися кодером *MPEG* [2].

Відомі підходи до вирішення питань, пов'язаних із забезпеченням дієвого захисту авторських прав і прав інтелектуальної власності, з оперативним

контролем доступу до сучасного медіапродукту, СІ і КІ, шляхом застосування стеганографічних алгоритмів (СА) і перетворень, розкрито у [4].

Постановка завдання

Метою роботи є представлення концепції апаратно-програмного забезпечення процесів вбудовування, передавання і захисту ДІ в мережі ЦЗМ стандарту [1] в рамках взаємопов'язаних факторів обмеження економічного і радіочастотного ресурсів, задоволення вимог формування і надання великої кількості нових послуг – як основи для подальшої оптимізації систем перспективних радіотехнологій з урахуванням специфіки їх практичного застосування, шляхом впровадження до складу транспортних механізмів ЦЗМ алгоритмів цифрової стеганографії [4].

Виклад основного матеріалу дослідження

Потенційні сфери використання стеганографічних систем (СС) в якості структурного компонента *MPEG*-аудіокодека системи ЦЗМ представлено на рис. 1. Вирішені класичними шляхами, кожне з таких завдань призведе до втрати оптимальності у співвідношенні між якістю звучання програм і спектральною ефективністю ЦЗМ. Наявний оптимум буде збережений або покращений у результаті створення стеганографічного каналу передавання даних (СКПД).

Сфери використання цифрових СС у ЦЗМ	
Захист прав власності Контроль за тиражуванням і розповсюдженням аудіо- та додаткової інформації	Приховане передавання КІ Застосування у конфіденційних цілях, а також випадках існування обмежень на використання криптографії
Прихована анотація Оптимізація організації мультимедійних баз даних і контентосховищ радіомовників	Приховане передавання СІ Реконфігурація мультиплексу ЦЗМ для збільшення економічних і технічних переваг його використання

Рис. 1. Потенційні сфери використання СС у складі ЦЗМ

При створенні СКПД ДІ на основі потоків трансльованих аудіопрограм ЦЗМ ключову роль відіграє модифікація механізму компресії аудіосигналу [2]. Використання психоакустичної моделі (ПАМ) у парі з динамічним розподілом бітів (ДРБ) при кодуванні вхідного сигналу з імпульсно-кодовою модуляцією (ІКМ) має наслідком диференціацію субсмугових відліків за кількістю кроків квантування і кінцеве зашумлення первинного сигналу, що порушує кореляційний зв'язок між найменшими значущими бітами (НЗБ) кодових комбінацій (КК) відліків. Відомо, що у полі аудіоданих *MPEG*-кадру найнижчу чутливість до помилок має контент субсмугових відліків: максимум – це подразнююче спотворення (3-й ступінь чутливості з 5 передбачених) при впливі завади на один з найстарших бітів (при 16-бітовому кодуванні), спотворення ж трьох НЗБ КК стандартом відноситься до нечутного (0-й ступінь чутливості) [2]. На основі аналізу СС як елемента системи цифрового стеганографічного звукового мовлення (ЦСЗМ) з позицій теорії зв'язку (рис. 2) запропоновано спосіб її введення до складу *MPEG*-аудіокодека модифікацією стандартних контроллера аудіокодека і блоку кодека відліків передавача і приймача до рівня можливості реалізації узгоджених СА (рис. 3). У ролі контейнера пропонується обрати один чи декілька *MPEG*-скомпресованих потоків аудіопрограм *DAB*-ансамблю. При цьому стеганокодер і декодер у складі *MPEG*-аудіокодера і декодера ЦСЗМ утворюють, відповідно, системи аудіостеганокодування (САСК) і декодування (САСДК) [5, 6].

На схемі рис. 3а джерело аудіоінформації (ДАІ) видає дані для передавання системою ЦСЗМ на входи аналізатора форматів (АФ) і аудіокодера (АК) з аналого-цифрового перетворювача (АЦП). АФ досліджує сліди застосування відомих операцій з цифрової обробки (ЦО), порівнюючи заголовки аудіоданих з наявними у банку даних форматів (БДФ) і видаючи на вхід АК сигнали про необхідність перекодування. Вбудовувана ДІ з джерел текстової і графічної

інформації (ДТІ/ДГІ) вводяться до САСК після надання їм потрібних форматів у системі попередньої обробки (СПО). Крім форматування, може бути проведене криптографічне, компресійне чи завадостійке кодування. ІКМ-аудіопотік надходить до банку фільтрів аналізу (БФА) і блоку ПАМ САСК. БФА ділить потік на субсмуги відліків, для груп яких визначаються індекси масштабних коефіцієнтів (ІМК) та інформація про вибір МК (ІВМК). ПАМ задає якість реалізації компресії і виконує аналіз кодованих аудіоданих, за результатами чого блок ДРБ зумовлює розрядність кодування субсмугових відліків. Дані про ІМК, ІВМК і ДРБ кодуються у кодері допоміжної інформації (КДІ). Потік з виходу блоку нормування і квантування субсмугових відліків (БНКВ) надходить на блок стеганокодування субсмугових відліків (БСКВ) і використовується як контейнер. БСКВ, застосовуючи певний СА, виконує вбудовування даних з КТД, КГД і СПО іншої ДІ до потоку субсмугових відліків. Роботою БСКВ керує контроллер аудіостеганокодування (КАСК), який обирає СА з множини можливих, оптимізує процес вбудовування, керує процедурами ключового захисту стеганошляху тощо. КАСК усіх аудіопрограм працюють у комплексі, а їх роботою керує багатоканальний контроллер стандартної схеми ЦЗМ. Потік заповнених контейнерів з БСКВ, інформація з КДІ, дані про формати вбудованих повідомлень і керувальні сигнали КАСК надходять на *формувач аудіостеганокадрів* (ФАСК). На виході САСК після мультиплексування потоків усіх субсмуг і даних управління формується потік аудіостеганокадрів ЦСЗМ, який подається на вхід стандартної системи авторизації доступу і згорткового кодування ЦЗМ.

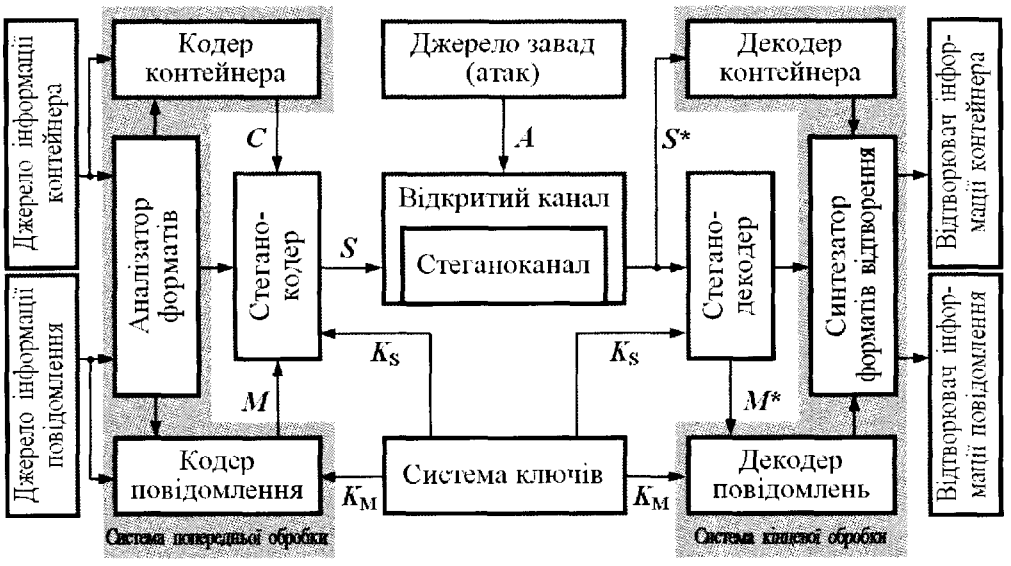


Рис. 2. Узагальнена структурна схема стеганографічної системи у складі ЦЗМ

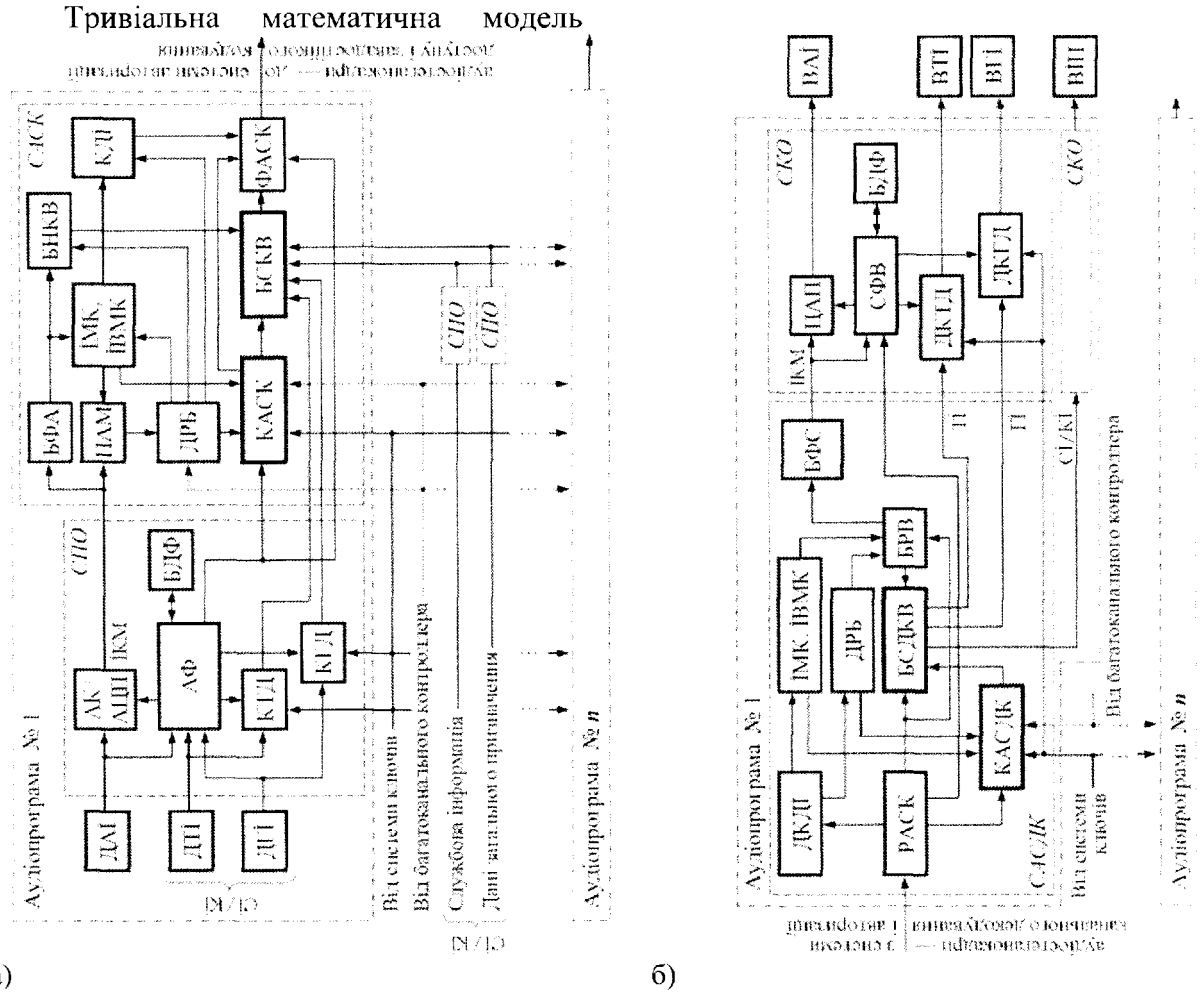
На схемі (рис. 3б) потік аудіопрограми з вбудованою ДІ надходить на розщеплювач аудіо-стеганокадрів (РАСК) для розділення потоків відліків, допоміжної інформації компресії, форматів і сигналів керування. Стиснені аудіодані надходять на блоки стеганографічного декодування (БСДКВ) і реквантування (БРВ) відліків. БСДКВ видобуває вбудовану ДІ з урахуванням даних про види і параметри СА, криптографічного захисту, а також виділених у декодері допоміжної інформації (ДКДІ) даних про ДРБ, ІМК та ІВМК, які подаються на контроллер аудіостеганодекодування (КАСДК). Видобута ДІ надходить на декодери текстових і графічних даних (ДКТД,

ДКГД) системи кінцевої обробки (СКО), які за допомогою синтезатора форматів відтворення (СФВ) і БДФ формують сигнали для відтворювачів текстової і графічної інформації (ВТІ, ВГІ). Можуть проводитися криптографічне і/або завадостійке декодування. Реквантовані у БРВ відліки проходять через банк фільтрів синтезу (БФС), утворюючи відновлені ІКМ-відліки, придатні для ЦАП і відтворення аудіоінформації (ВАІ).

Тривіальна математична модель (ММ) організації СС [4, 7]

$$E\colon \mathbf{C}\times\mathbf{M}\to\mathbf{S};\qquad D\colon \mathbf{S}\to\mathbf{M};\qquad \mathbf{\Sigma}=(\mathbf{C},\mathbf{M},\mathbf{S},E,D), \tag{1}$$

де E і D – алгоритми прямого і зворотного стеганоперетворень відповідно; $\mathbf{C}$ і $\mathbf{S}$ – множини пустих і заповнених контейнерів відповідно, причому E зумовлює $|\mathbf{S}|=|\mathbf{C}|$ і подібність $sim[c, E(c, m)]\approx 1\ \ \forall\ m\in\mathbf{M},\ c\in\mathbf{C}$; $\mathbf{M}$ – множина повідомлень,



а) б)

Рис. 3. Структурна схема СС окремої програми передавача (а) і приймача (б) ЦСЗМ

$|\mathbf{M}|\le|\mathbf{C}|$; $\mathbf{\Sigma}$ – сукупність множин пустих і заповнених контейнерів, повідомлень і пов'язуючих їх перетворень, — не достатня для докладного опису процесів, здійснюваних при формуванні СКПД у системі ЦСЗМ, оскільки не враховує характерні особливості використання СС у складі аудіокодека *MPEG*. Пропонується модифікація тривіальної ММ СС з урахуванням можливості приховувань на нижньому (субсмугові відліки у межах цифрового потоку окремої програми) і верхньому (цифрові потоки усіх програм ансамблю) рівнях контейнера:

$$\bigcup_{i\in\mathbf{C}^{\ddot{\imath}}}\mathbf{C}_i^{\hat{\mathbf{a}}}=\mathbf{C}\ \text{ при}\qquad |\mathbf{C}_1^{\hat{\mathbf{a}}}|+|\mathbf{C}_2^{\hat{\mathbf{a}}}|+\ldots+|\mathbf{C}_{|\mathbf{C}^{\ddot{\imath}}|}^{\hat{\mathbf{a}}}|=|\mathbf{C}|, \tag{2}$$

де $|\mathbf{C}^{\mathbf{n}}|$ і $|\mathbf{C}_i^{\mathbf{B}}|$ – потужності множин

програмних (ПК) і відлікових (ВК) контейнерів у межах i-го ПК (радіопрограми).

Введемо поняття селективного оптимального контейнера СС ЦСЗМ — частини відкритого ПК чи ВК, що оптимально підходить для вбудовування, задовольняючи основним елементам множини вимог до якості СС $\mathbf{Q}$, яка встановлює зв'язок між якістю СС і об'ємами контейнерів V_c і повідомлень V_m (рис. 4). Обрання оптимальних ПК і ВК здійснюється функцією відбору O:

$$O\colon \mathbf{C}^{\text{п(в)}} \times \mathbf{Q} \to \mathbf{C}^{\text{п(в)Q}} \text{ при } \mathbf{C}_i^{\text{âQ}} \subset \mathbf{C} \ \forall i \in \mathbf{C}^{\text{ï Q}}, \quad (3)$$

де $\mathbf{C}^{\text{п(в)Q}}$ – підмножина оптимальних пустих ПК чи ВК, відібраних згідно вимог до якості СС:

$$\mathbf{C}^{\text{Q}} = \bigcup_{i \in \mathbf{C}^{\text{ï Q}}} \mathbf{C}_i^{\text{âQ}}. \quad (4)$$

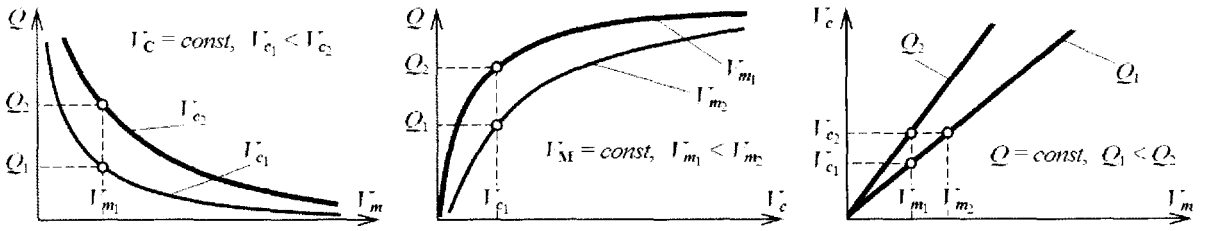


Рис. 4. Взаємозв'язок між якістю СС Q та об'ємами контейнера c і стеганограми m

Передавану у ЦСЗМ ДІ, згідно з її пов'язаністю з ПК та рівнем доступу до неї з боку споживачів, розіб'ємо на класи [8]: «1-1» — пов'язана з аудіопрограмою ДІ, що має безумовний допуск (дані,пов'язані з програмою, анотації); «1-2» — пов'язана з аудіопрограмою ДІ з умовним допуском (цифрові водяні знаки (ЦВЗ), цифрові відбитки тощо); «2-1» — непов'язана з аудіопрограмою ДІ, що має безумовний допуск (наприклад, службова інформація); «2-2» — непов'язана з аудіопрограмою ДІ з умовним допуском (наприклад, передплачена СІ або КІ).

Для ДІ класу «1-1», коли з множини загальнодоступних повідомлень підмножина $\mathbf{M}_{\text{á/ó}\,i}^{\text{ï}} \subset \mathbf{M}$ пов'язана з відліками i-го ПК $\mathbf{C}_i^{\text{ä}} \in \mathbf{C}$, довільне обрання інших контейнерів неможливе. Перенесення повідомлень організовується на базі i-го ПК з застосуванням (3) на рівні ВК; приховування стеганошляху не здійснюється, а СС являє собою сукупність:

$$\Sigma_{\text{á/y}}^{\text{ï}} = (\mathbf{C}_i^{\text{ä}}, \mathbf{Q}, \mathbf{C}_i^{\text{âQ}}, \mathbf{M}_{\text{á/ó}\,i}^{\text{ï}}, \mathbf{S}, E, D, O).$$

До безальтернативного ПК вбудовується ДІ класу «1-2», коли з відліками ПК $\mathbf{C}_i^{\text{ä}} \in \mathbf{C}$ пов'язується підмножина повідомлень $\mathbf{M}_{\text{ó}\,i}^{\text{ï}} \subset \mathbf{M}$ з умовним допуском, перенесення яких здійснюється в i-му ПК, з урахуванням (3) для ВК й організацією захисту стеганошляху (зокрема, ініціюванням множини ключів $\mathbf{K}$ псевдовипадкових перестановок):

$$\Sigma_{\text{y}}^{\text{ï}} = (\mathbf{C}_i^{\text{ä}}, \mathbf{Q}, \mathbf{C}_i^{\text{âQ}}, \mathbf{M}_{\text{ó}\,i}^{\text{ï}}, \mathbf{K}, \mathbf{S}^{\text{K}}, E, D, O).$$

Якщо повідомлення підмножини $\mathbf{M}^{\text{нп}} \subset \mathbf{M}$ не пов'язані з контейнерами $\mathbf{C}$, організовується зовнішня (для ПК) і внутрішня (для ВК) процедури обрання. Для перенесення ДІ класу «2-1» $\mathbf{M}_{\text{á/ó}}^{\text{í ï}} \subset \mathbf{M}^{\text{нп}}$, серед множини ПК $\mathbf{C}^{\text{п}}$ обирається оптимальний по заданим вимогам до якості СС (3), в якому обирається множина оптимальних ВК: $\Sigma_{\text{á/y}}^{\text{í ï}} = (\mathbf{C}^{\text{п}}, \mathbf{Q}, \mathbf{C}_{\vec{n}^{\text{ï Q}}}^{\text{âQ}}, \mathbf{M}_{\text{á/ó}}^{\text{í ï}}, \mathbf{S}, E, D, O)$.

Перенесення ДІ класу «2-2» $\mathbf{M}_{\text{ó}}^{\text{í ï}} \subset \mathbf{M}^{\text{нп}}$ вимагає приховання стеганошляху, тому серед множини ПК $\mathbf{C}^{\text{п}}$ обирається підмножина оптимальних згідно вимог до якості СС (3), після чого у відібраних ПК обирається множина оптимальних ВК, що заповнюються у визначеній

множиною **K** псевдовипадковій послідовності (ПВП):

$$\Sigma_{\text{ó}}^{\text{í ï}} = (\mathbf{C}^{\text{n}}, \mathbf{Q}, \mathbf{C}_{\tilde{\text{N}}^{\text{i}}\text{Q}}^{\hat{\text{a}}\text{Q}}, \mathbf{M}_{\text{ó}}^{\text{í ï}}, \mathbf{K}, \mathbf{S}^{\text{K}}, E, D, O).$$

За класифікацією методів стеганографічної обробки ДІ [8] встановлено, що визначальна для розробки програмної моделі (ПМ) відмінність між класами СС ЦСЗМ зводиться до різного простору відбору оптимальних ВК (або в межах безальтернативного ПК, або в межах усіх ПК ансамблю) і наявності чи відсутності захисту стеганошляху. Показниками ефективності створюваних класів СС ЦСЗМ можуть виступати час вбудовування повідомлень, значення прихованої ПЗ СКПД, рівень акустичних спотворень, рівень стійкості повідомлення ДІ до перекомпресії, час знаходження стеганошляху [4, 8].

Обрання оптимальних ПК $\mathbf{C}^{\text{nQ}} \in \mathbf{C}^{\text{n}}$ (для ДІ класів «2-1» і «2-2») полягає у критеріальному відборі за швидкістю передавання, атрибутами контенту, аудіорежимом і потужністю завадостійкого кодування. Оптимальні ВК у межах i-го ПК, $\mathbf{C}_i^{\hat{\text{a}}\text{Q}} \subset \mathbf{C} \ \forall i \in \mathbf{C}^{\text{i Q}}$, відбираються за результатами стандартизованих [2] етапів (субсмугового аналізу, обчислення і кодування МК, ПАМ, ДРБ, ІВМК і квантування відліків), які виконуватимуться й без створення СКПД. Вбудовування повідомлень (стеганограм) зводиться до реалізації певного СА по заповненню обраних ВК:

1) для вбудовування ДІ класів «1-1» і «2-1» використано адаптований до особливостей *MPEG*-кодера [2] алгоритм заміни НЗБ [4] у КК субсмугових відліків:

$$\text{Í ÇÁ}\left(bin \vee bin\_v, \mu\right) = Mbin_{\mu} \text{ при } 0 \le \mu < L_M, \ index(\text{НЗБ}) > \lambda, \quad (5)$$

при цьому біти повідомлення *Mbin* (бінарного вектора довжиною L_M) послідовно заміщують собою НЗБ КК лише тих відліків і гранул кожного аудіокадру, на кодування яких після ДРБ було виділено достатню для створення комфортного ефекту маскування кількість бітів (більше деякого заданого порогу λ);

2) для ДІ класу «1-2» представлено адаптацію алгоритмів відносної заміни [4] до особливостей аудіоформату ПК і ВК, що передбачає маніпуляцію фаз відліків-коефіцієнтів субсмугового аналізу сигналу у БФА шляхом відносної заміни їх нормованих і квантованих версій Ξ у парі кодованих за результатом ДРБ в a-му аудіокадрі субсмуг середньочастотному діапазону $s1$ і $s2$, $s1 \neq s2$ (обрання яких може ініціюватися ключами $K1$, $K2$), реалізуючи симетричну модель СС змішаного типу. Вбудовування бітів бінаризованого повідомлення *Wbin* здійснюється у відповідності до наступної процедури $\forall b$:

$$\Xi_b(s1 = K1_a) > \Xi_b(s2 = K2_a) \text{ при } Wbin_a = 0,$$
$$\Xi_b(s1 = K1_a) < \Xi_b(s2 = K2_a) \text{ при } Wbin_a = 1;$$

3) для ДІ класу «2-2» модифіковано алгоритм заміни НЗБ [4] з наданням черговості внесення бітів повідомлення до ВК $\mathbf{C}_{\beta}^{\text{в}}$ у межах кадру ПК ознак псевдовипадковості. Генератор ПВП створює послідовність індексів $\beta_0, \beta_1, ..., \beta_{11(35)}$, що залежить від ключа $k \in \mathbf{K}$, зберігаючи μ-й біт повідомлення *Mbin* довжини L_M у НЗБ відліку з індексом $\beta_{\text{mod}[\mu, 12(36)]}$. Процедура вбудовування здійснюється згідно (5), при цьому внесення бітів $Mbin_{\mu}$ виконується лише до субсмуг s (починаючи з певної ζ-ї) a-го кадру, відліки яких кодуються окремо, а розрядність їх кодування n перевищує поріг λ.

Процедура видобування стеганограм для методів всіх класів ДІ є оберненою процедурі вбудовування і ґрунтується на послідовно застосовуваних процедурах обрання ПК (якщо це передбачено методом), розщеплення аудіостеганокадрів останніх у РАСК з наступним обранням і дослідженням заповнених ВК — на основі урахування інформації з виходу ДКДІ і попередніх

домовленостей з передавальною стороною, дотримання яких контролюється у КАСДК. Для ДІ класів «1-1» і «2-1» зчитування НЗБ КК субсмугових відліків або гранул радіопрограмних потоків аудіостеганокадрів здійснюється тільки для тих ВК, які після ДРБ були кодовані кількістю бітів, більшою за поріг λ. При ДІ класу «1-2» для порівняльних оцінок значень реквантованих субсмугових відліків треба виконати процедуру реквантування ВК; для врахування їх можливих спотворень рішення про кожен біт стеганограми приймається аналізом співвідношень усереднених на множині з 36 відліків b псевдовипадково обраних за погодженим алгоритмом субсмуг $s1$ і $s2$ реквантованих відліків поточного аудіостеганокадру. При видобуванні ДІ класу «2-2» вважається, що використовуються генератори ПВП, які для обраних ключів $k \in \mathbf{K}$ виробляють ідентичні послідовності індексів β, а також узгоджені пороги розрядності кодування ВК λ і субсмуг, що містять відібрані ВК, ζ.

Висновки і перспективи дослідження

Для дослідження ефективності ММ і ПМ СС ЦСЗМ з аспектів їх надійності представлено класифікації стеганографічних систем за рівнем стійкості і схильності до типових атак (рис. 5).

Оцінено стійкість СС класу «1-2» до руйнування стеганограми (ЦВЗ) застосуванням активних атак, спрямованих на внесення спотворень у ПК перекомпресією і додаванням білого шуму (рис. 6). Результати дозволяють вважати досліджуваний СА стійким до зазначених класів атак у межах, обумовлених достатністю кореляційного зв'язку між оригіналом і спотвореною копією ЦВЗ.

Для врахування часових і спектральних ефектів маскування слуху при оцінці стійкості СС класів «2-2» до виявлення стеганограм при пасивних атаках, що визначається рівнем акустичної прихованості, запропоновано використати резуль-

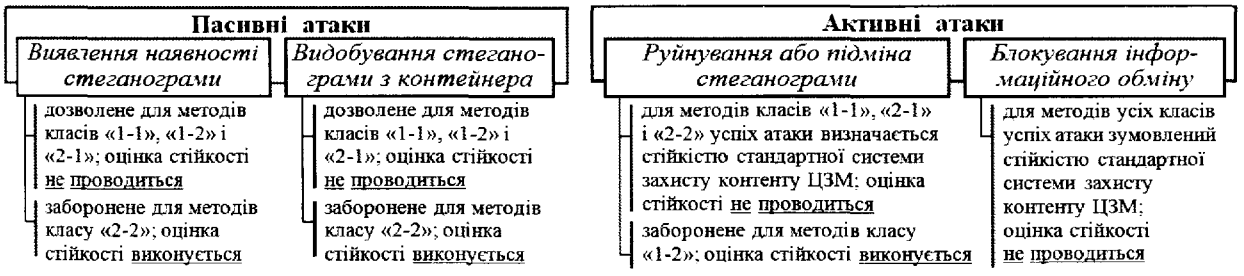


Рис. 5. Класифікація СС за схильністю до атак і потребою в оцінці стійкості

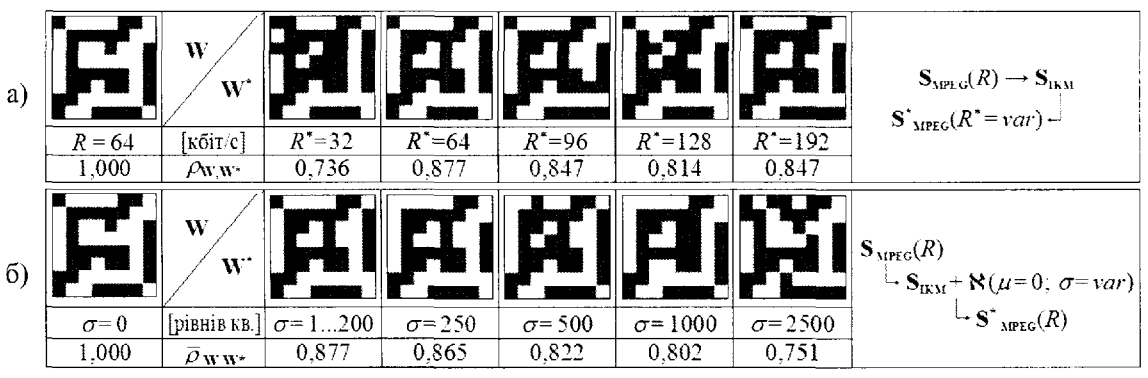


Рис. 6. ЦВЗ $\mathbf{W}^*$, видобуті з ПК після перекомпресії із швидкістю R^* ($а$) та адитивним білим шумом потужності σ ($б$), й оцінка їх кореляції $\rho_{\mathbf{W},\mathbf{W}^*}$ з оригіналом $\mathbf{W}$

тати ПАМ — нормовані по рангу r відношення рівня сигналу до порогу маскування — у кожній субсмузі аудіокадрів пустого і заповненого ПК, за якими обчислено адаптовані показники [4] акустичного спотворення ПК. Відзначено вплив на невідчутність стеганограми кількості бітів, виділених ДРБ на кодування ВК. Проте, навіть при вбудовуванні до всіх субсмуг, прихованість лишалася високою. Підтверджено стійкість СС класу «1-2» до активних атак видалення ЦВЗ перекомпресією чи зашумленням, оскільки вони призводять до суттєвої і невідновлюваної втрати якості звучання ПК, а зважаючи на зміну властивостей ПК навіть при незлонавмисній його перекомпресії, можна казати й про ускладненість пасивних атак.

Рівень стійкості СС класу «2-2» до видобування елементів стеганограми визначається комбінаторною кількістю можливих комбінацій індексів під час їх перебирання. Для пропонованого СА загальна кількість можливих ПВП при повному їх перебиранні:

$$N_\beta = N_{\hat{I}\,\hat{C}\hat{A}}!/(N_{\hat{I}\,\hat{C}\hat{A}} - n)!. \qquad (6)$$

При вбудовуванні до НЗБ КК субсмугових відліків $N_\beta(36) = 36!$ — отже, достатня стійкість може бути забезпечена часом, тривалість якого перевищує передбачуваний час актуальності видобування.

Визначено ефективність СС за індексом прихованої ПЗ створюваних СКПД, усередненою на множині спектрів середньостатистичного аудіозапису (модель рожевого шуму). Значення Θ та індекси I прихованої ПЗ (рис. 7), одержані

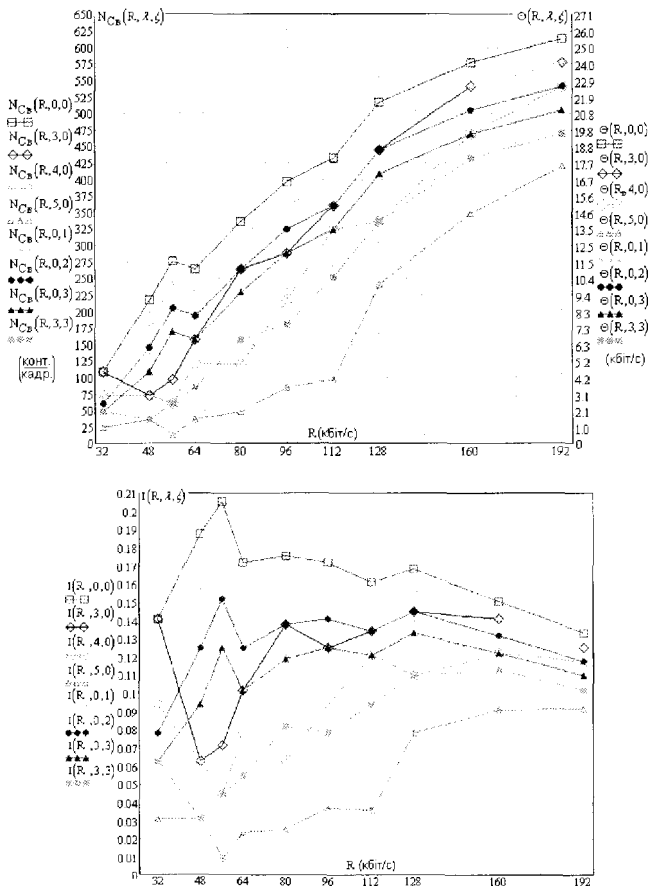


Рис. 7. Усереднена кількість оптимальних ВК в окремому кадрі *MPEG*-потоку і прихована ПЗ створсного на їх основі СКПД (*а*); індекс прихованої ПЗ СКПД (*б*)

для різних бітових швидкостей R, порогових значень довжин КК відліків λ і частот їх субсмуг ζ, можуть вважатися гранично досяжними для будь-яких СС на основі *MPEG*-скомпресованих ПК.

Зважаючи на обмеженість значень стандартних бітових швидкостей ПК, деякі з стеганографічних реконфігурацій надають можливість лише покращення середньої якості звучання аудіопрограм ансамблю, проте можливість додавання ще одного каналу мовлення існує для випадків, коли ПЗ субканалів передавання ДІ первісно була високою — спектральна ефективність досягає 20-50%.

Наведене теоретичне підтвердження можливості збільшення потужності завадостійкого кодування, якщо після конвертації субканалу передавання ДІ на СКПД частину ПЗ, що при цьому звільнилася, використати для внесення додаткової надмірності до інформаційних потоків.

Проведено оцінку обчислювальної складності СА вбудовування і зчитування стеганограм. Пропоновані СА характеризуються низькою складністю реалізації і на фоні основних процедур компресії не призводять до помітного зростання часу підготовки заповненого ПК перед випуском його в ефір або часу наступного видобування стеганограми одержувачем.

Список літератури

1. Radio Broadcasting Systems. Digital Audio Broadcasting to mobile, portable and fixed receivers: ETSİ EN 300 401. – [İn force since 2006-06-01]. – European Telecommunications Standards İnstitute, 2006. – 197 p.

2. İnformation technology. Coding of moving pictures and associated audio for digital storage media at up to 1,5 Mbit/s. Part 3. Audio : İSO/İEC 11172-3:1993. – [İn force since 1993-01-01]. – 1993. – 150 p.

3. Рихтер С. Г. Цифровое радиовещание / Сергей Рихтер. – М. : Горячая линия – Телеком, 2003. – 352 с.

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

5. Пат. 89054 UA, МПК H 04 J 4/00. Спосіб цифрового радіомовлення з передаванням сервісної інформації стеганографічним каналом передавання даних, створеним на основі аудіоінформації радіопрограм, що транслюються, і пристрій для його реалізації / Бабак В. П., Конахович Г. Ф., Пузиренко О. Ю.; власник Нац. авіац. ун-т. – № а 2007 02490; заявл. 06.03.2007; опубл. 25.12.2009, Бюл. № 24.

6. Пузиренко О. Ю. Стеганографічні канали передавання даних у системах цифрового звукового мовлення / О. Пузиренко // Захист інформації: Зб. наук. пр. – К. : НАУ, 2008. – Спец. вип. – С. 81-86.

7. Пузиренко О. Ю. Математичні моделі стеганосистем цифрового стеганографічного звукового мовлення / О. Пузиренко // Захист інформації: Зб. наук. пр. – К. : НАУ, 2008. – Спец. вип. – С. 87-92.

8. Пузиренко О. Ю. Класифікація методів стеганографічного приховання повідомлень додаткової інформації у системі цифрового звукового мовлення / О. Пузиренко, О. Шевченко // Захист інформації: Зб. наук. пр. – К. : НАУ, 2010. – Вип. 17. – С. 57-62.

9. Пузиренко О. Ю. Концепція здійснення стеганографічного перенесення додаткової інформації у модифікованих системах цифрового звукового мовлення / О. Пузиренко, О. Шевченко // Захист інформації: Зб. наук. пр. – К. : НАУ, 2010. – Вип. 17. – С. 153-158.