Robust label coding of digital watermark in the speech communication

Peter Likholob

Department of Information and Telecommunication Systems and Technologies, National Research University "BelSU", Belgorod, RUSSIA, S. Pobedi 85,
E-mail: likholob@bsu.edu.ru

The mathematical model of label coding, representing the digital watermark hidden in the audio file container, is observed. Implementation takes place in the energy field file-container, divided by the window in time domains. Coding is done by replacing the part of energy windows of audio file container with eigenvector energy of subband-pass matrix (part of the energy is concentrated in the indicated frequency range). It is recommended to estimate the concentration of energy by eigenvalues of subband-pass matrix. It is offered to control the level of implemented parts of the energy using the calculation of normalizing coefficients with automatically adjustable threshold. The threshold left after optimal filtering subband-pass matrix is based on residual energy (percolation energy from adjacent frequency intervals).It is important to note that the proposed method involves saving the amount of energy, concentrated in adjacent frequency intervals, unchanged. Key parameters determining the work of the mathematical model are proposed.The key identifies: the duration of the window N, the width of the frequency intervals, where the encoding $2\Delta F$ takes place, robustness of the system e, position of labels in frequency domain F_0. The label is destroyed as a result of intentional attacks of digital watermark, thus, the structure of eigenvector $\mathbf{q}_{kr}$ of the subband-pass matrix A_r is preserved , whose presence indicates that this audio file $\mathbf{X}$ has previously been labeled. The usage of the eigenvectors $\mathbf{q}_{kr}$, Eigen values of which are close to one $l_r \cong 1$, can increase the resistance to intentional and passive attacks of the elaborated system. The system itself determines the coding threshold and can operate without human intervention while maintaining a high resistance to passive attacks proposed by different methods of assessment. After label coding, changes in the audio file container are not visible to human senses.

Переклад зроблено Горьковою Н.Г., центр іноземних мов «Universal Talk», www.utalk.com.ua.

Кодування робастних міток ЦВЗ у речовому повідомленні

Петро Лихолоб

Кафедра інформаційно-телекомунікаційних систем та технологій, НИУ «БелГУ», РОСІЯ,
м.Белгород, вул.Перемоги, 85,
E-mail: likholob@bsu.edu.ru

Розглянуто математичну модель кодування крихких міток цифрового водяного знаку (ЦВЗ) в відрізках аудіо-сигналу, що представляє собою мовне повідомлення. Описаний метод може бути застосований у випадку, коли необхідно провести маркування і підтвердити автентичність і апеллируемость захищаємого звукозапису. Руйнування мітки відбувається при внесенні змін до звукозапису.

Ключові слова – стего, файл-контейнер, речове повідомлення, захист інформації, ЦВЗ, мітка.

I. Вступ

Вагому роль в економіці будь-якого суспільства займає інформація. З розвитком технологій передачі та зберігання інформації в цифровому вигляді виникає завдання захисту інформації. Найбільш поширеною, природною і однією з основних форм інформаційного обміну між людьми є мова. Результати такого інформаційного обміну, що представляють собою звукозаписи, вироблені під час нарад, конференцій, переговорів в диспетчерських, а також при передачі мовних команд управління, часто об'єднують в банки даних. В останні роки широке поширення одержали системи захисту інформації та підтвердження авторського права, засновані на внесення в файл з даними спеціальних міток (ідентифікаторів), об'єднаних в послідовність символів, які мають смисловий зміст, таке об'єднання прийнято називати цифровим водяним знаком (ЦВЗ). Цифровий водяний знак (ЦВЗ) – набір міток представлених спеціальним чином, непомітно впроваджуваних (кодованих) в основне покриваюче повідомлення (ОПП) з метою тим чи іншим чином контролювати його використання. Системи, що використовують ЦВЗ є окремим випадком застосування методів цифрової стеганографії. Особливість поширення стеганографічних методів стало те що зміни в ОПП не можливо відчути органами почуттів людини.

II. Математичні основи

Під звукозаписом потребуючим в захисті будемо розуміти відрізок аудіо- файл-контейнера мовного повідомлення, що складається з послідовності відліків або вибірок миттєвих значень сигналу ($\mathbf{X} = [x_1, x_2, \mathbf{K}, x_l, \mathbf{K}, x_L]^T$, $L \in \mathrm{N}$), віддалених один від одного на інтервал часу, T_∂. Який умовно розділяють на вікна $\mathbf{C}_z = [c_1, \mathbf{K}, c_n, \mathbf{K}, c_N]^T = [x_l, \mathbf{K}, x_{(l+N-1)}]^T$ довжиною

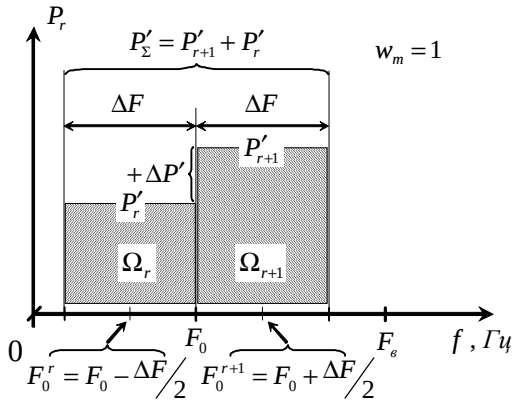
N вибірок. Далі в кожному вікні кодується цифрова мітка $w_m \in \{-1, 1\}$, біортогональний біт ЦВЗ $\vec{\mathbf{W}}$.

Процес стеганографічного перетворення, описується співвідношенням:

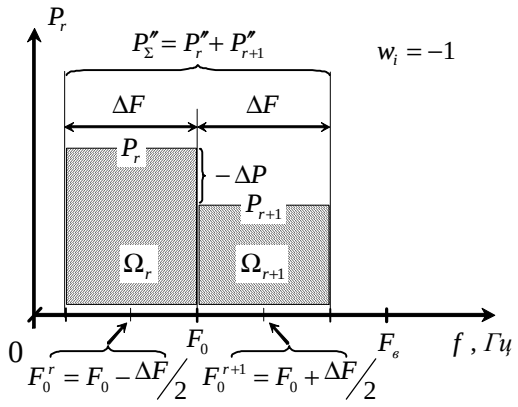
$$\vec{\mathbf{Y}} = \mathrm{E}\left(\vec{\mathbf{X}}, \vec{\mathbf{W}}, \mathbf{K}\left((N, \Delta F), e, \vec{F}_0\right)\right), \quad (1)$$

де $\mathbf{K}(\ )$ – функціонал обчислення нормувальних коефіцієнтів; N – довжина вікна, в який впроваджується цифрова мітка; e – параметр стійкості системи; $\vec{F}_0$ – центральні частоти відносно, яких відбувається кодування міток.

Кодування цифрової мітки w_m, визначається як знак різниці в частинах енергії $\pm\Delta P = \left(P'_r - P'_{r+1}\right)$ (рис. 1).



а)



б)

Рис.1 Модель кодування мітки ЦВЗ.

Частина енергії (P_r), зосередженна в заданих частотних інтервалах $\Omega_r \in [F_0 - \Delta F, F_0]$ та $\Omega_{r+1} \in [F_0, F_0 + \Delta F]$ ($0 < \Omega_r < p$, $0 < \Omega_{r+1} < p$) вікна аудіо- файла-контейнера $\vec{C}$, обчислюють на основі формули [1]:

$$P_r = \left(\vec{\mathbf{C}}^T \cdot A_r \cdot \vec{\mathbf{C}}\right) \quad (2)$$

Для чого розраховують матрицю ($A_r = \{a_{ki}^r\}$, $i, k = 1, \mathbf{K}, \mathrm{N}$), з елементами виду:

$$a_{ki}^r = \begin{cases} 2 \cdot \dfrac{\Delta F}{F_o}, & i = k \\ 2 \cdot \dfrac{\sin\left(\dfrac{2p \cdot \Delta F/2}{F_o} \cdot (i-k)\right)}{p \cdot (i-k)} \cdot \cos\left(\dfrac{2p \cdot F_0^r}{F_o} \cdot (i-k)\right), & i \neq k \end{cases} \quad (3)$$

Матрицю A_r прийнято називати субполосной. Субполосная матриця є симетричною і позитивно визначеною. Тому вона має повну системою ортогонормальних власних векторів $\vec{\mathbf{q}}_{kr}$, які відповідають власним числам l_{kr}, в дискретному випадку власні числа кількісно рівні зосередженим у вибраних частотних інтервалах часткам енергій відповідних власних векторів. Тако ж вони задовольняють співвідношенням [1].

$$l_{kr}\vec{\mathbf{q}}_{kr} = A_r\vec{\mathbf{q}}_{kr} \quad (4)$$

$$A_r = \sum_{k=1}^{N} l_{kr}\vec{\mathbf{q}}_{kr}\vec{\mathbf{q}}_{kr}^T = \mathbf{Q}_r\mathbf{L}_r\mathbf{Q}_r^T; \quad (5)$$

$$\mathbf{Q}_r = \left\{\vec{\mathbf{q}}_{kr}\right\}_{k=1}^{N}; \quad (6)$$

$$\mathbf{L}_r = diag\left(l_1^r, l_2^r, \mathbf{K}, l_N^r\right); \quad (7)$$

$$l_1^r > l_2^r > \mathbf{K} > l_N^r \geq 0. \quad (8)$$

Впровадження мітки відбувається на основі заміщення частин енергії сусідніх частотних інтервалів відрізка аудіо-файл ($\vec{\mathbf{C}} = \left[\vec{C}_z\right]$, $z \in \mathrm{N}$), математична модель :

$$\vec{\mathbf{S}} = \vec{\mathbf{C}} - \vec{\mathbf{C}}^T \cdot (A_r + A_{r+1}) + \sqrt{K_r} \cdot \vec{\mathbf{q}}_{kr} + \sqrt{K_{r+1}} \cdot \vec{\mathbf{q}}_{k(r+1)}, \quad (9)$$

Виберемо k-й власний вектор ($\vec{\mathbf{q}}_{kr}$ для першого і $\vec{\mathbf{q}}_{k(r+1)}$ другого частотних інтервалів), що відповідають максимальному власному числу (першого, виходячи з умов (4) - (8)), тому він володіє максимальною часткою енергії в замещаємой частотному інтервалі.

Нормуючі коефіцієнти K_r і K_{r+1} для власних векторів субполосних матриць $\vec{\mathbf{q}}_{kr}$ та $\vec{\mathbf{q}}_{k(r+1)}$, частка енергії яких зосереджена в заміщаємих частотних інтервалах вікна аудіо-сигналу та визначаються співвідношеннями:

$$K_r = \left(\frac{P_\Sigma}{2}\right) - \Delta P. \quad (10)$$

$$K_{r+1} = P_\Sigma - K_r. \quad (11)$$

Суму значень частин енергії першого (Ω_r) і другого (Ω_{r+1}) частотного інтервалу, складає:

$$P_\Sigma = \vec{\mathbf{C}}^T \cdot \left(A_r + A_{r+1}\right) \cdot \vec{\mathbf{C}}. \quad (12)$$

В моделі також автоматично вирахуване значення порогу різниці в частинах енергії ΔP між двома частотними інтервалами (Ω_r та Ω_{r+1}) вікна аудіо

сигналу $\vec{C}_z$, яке становить частини енергії яка залишилась після оптимальної фільтрації (рис. 2):

$$\Delta P = e \cdot \left(\tilde{P}_r + \tilde{P}_{r+1}\right) \cdot w_m \qquad (13)$$

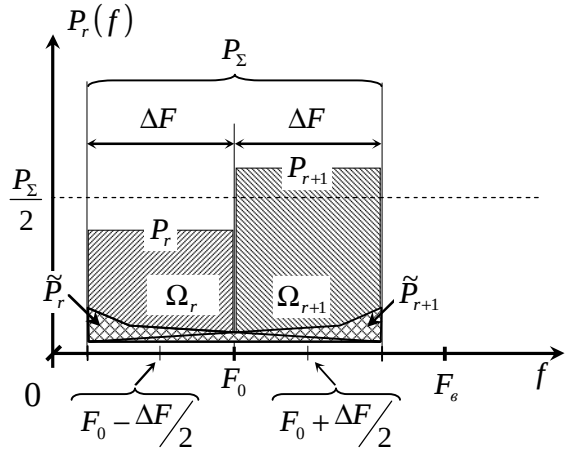


Рис.2 Модель розподілення частин енергії між двома частотними інтервалами Ω_r та Ω_{r+1}.

Обчислимо енергію, яка залишилася після оптимальної частотної фільтрації для першого (Ω_r) і другого (Ω_{r+1}) частотного інтервалу:

$$\tilde{P}_r = \left(C - C^T\left(A_r + A_{r+1}\right)\right)^T \cdot A_r \cdot \left(C - C^T\left(A_r + A_{r+1}\right)\right) \quad (14)$$

$$\tilde{P}_{r+1} = \left(C - C^T\left(A_r + A_{r+1}\right)\right)^T \cdot A_{r+1} \cdot \left(C - C^T\left(A_r + A_{r+1}\right)\right) \quad (15)$$

Декодування мітки здійснюють на основі формули:

$$\hat{w}_m = \begin{cases} 1, & \hat{P}_r > \hat{P}_{r+1} \\ -1, & \hat{P}_r < \hat{P}_{r+1} \end{cases}, \qquad (16)$$

Частина енергії ($\hat{P}_r$), зосередженна в заданих частотних інтервалах $\Omega_r \in [F_0 - \Delta F, F_0]$ ($0 < \Omega_r < p$) вікна аудіо- стего-контейнера $\vec{S}$, обчислюють по формулі:

$$\hat{P}_r = \left(\vec{S}^T \cdot A_r \cdot \vec{S}\right) \qquad (17)$$

Частина енергії ($\hat{P}_{r+1}$), зосередженна в заданих частотних інтервалах $\Omega_{r+1} \in [F_0, F_0 + \Delta F]$ ($0 < \Omega_{r+1} < p$) вікна аудіо- стего-контейнера $\vec{S}$, обчислюють по формулі:

$$\hat{P}_{r+1} = \left(\vec{S}^T \cdot A_{r+1} \cdot \vec{S}\right) \qquad (18)$$

Важливо відзначити, що пропонований метод передбачає збереження суми частин енергії, зосередженої в сусідніх частотних інтервалах незмінною ($P_\Sigma = \left(P_r + P_{r+1}\right) \cong P'_\Sigma = \left(P'_r + P'_{r+1}\right) = \hat{P}_\Sigma = \left(\hat{P}_r + \hat{P}_{r+1}\right)$ або $P_\Sigma = \left(P_r + P_{r+1}\right) \cong P''_\Sigma = \left(P''_r + P''_{r+1}\right) = \hat{P}_\Sigma = \left(\hat{P}_r + \hat{P}_{r+1}\right)$). Збереження незмінною сумарної енергії ($P_\Sigma \cong P'_\Sigma$ або $P_\Sigma \cong P''_\Sigma$) дає можливість забезпечення енергетичної (частотної) скритності пропонованої системи.

III. Критерії оцінювання якості кодування

В якості критеріїв оцінки якості вкладення будемо використовувати ступінь схожості двох аудиосигналів визначаємих як кореляційний момент:

$$cor_{\vec{C},\vec{S}} = \frac{\sum_{n=1}^{N}\left((c_n - \bar{c})(s_n - \bar{s})\right)}{\sqrt{\sum_{n=1}^{N}(c_n - \bar{c})^2 \sum_{n=1}^{N}(s_n - \bar{s})^2}}, \qquad (19)$$

де c_l – вибірки миттєвих значень файла-контейнера; s_l – вибірки миттєвих значень стего-контейнера; $\bar{c}$ – середнє значення вибірки миттєвих значень файла-контейнера; $\bar{s}$ – середнє значення вибірки миттєвих значень стего-контейнера.

А також середньоквадратичну похибку, розрахованої по формулі:

$$s_{\vec{C},\vec{S}} = \frac{\left\|\vec{C} - \vec{S}\right\|}{\left\|\vec{C}\right\|} \cong \frac{\sum_{l=1}^{L}(c_l - s_l)}{\sum_{l=1}^{L}(c_l)}, \qquad (20)$$

IV. Обчислювальні експерименти

Приклад роботи математичної моделі розглянутий на тестовому звукозапису запропонованому системою MATLAB (mtlb.mat, рис.1). Довжина відрізка $L = 4001$ вибірки миттєвих значень амплітуди взятих з частотою дискретизації $F_s = 7418$ Гц.

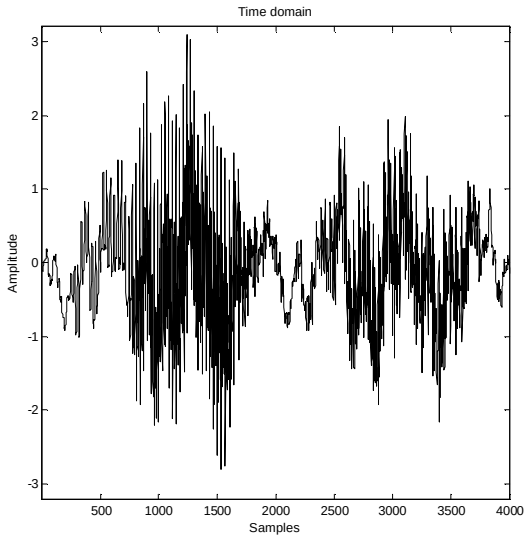


Рис.3 Відрізок аудіо- файла-контейнера.

В якості кодуємої послідовності символів в аудіо-файлі-контейнері виступає назва організації «BSU», яка з перекодується в послідовність біт (w_m), результати перекодування а також центральна частота внесення представлені у таблиці 1.

ТАБЛИЦЯ 1

ПАРАМЕТРИ СТЕГО-КЛЮЧА І КРИТЕРІЇ ОЦІНЮВАННЯ ЯКОСТІ

Символ ЦВЗ	вікно	ASCII	w_m	F_0	$s_{\vec{C},\vec{S}}$	$cor_{\vec{C},\vec{S}}$
1	2	3	4	5	0.0042	0.9995
B	1		-1	2580	0.0037	0.9996
	2		-1	1050	0.0003	0.9998
	3		1	2550	0.0004	0.99994
	4	42	-1	1300	0.0003	0.9998
	5		1	2550	0.0095	0.9949
	6		-1	1300	0.0029	0.995
	7		1	3000	0.0032	0.9999
	8		-1	3400	0.0018	0.9998
S	9		-1	3150	0.0092	0.9924
	10		-1	2300	0.0028	0.9998
	11		1	3100	0.0067	0.9993
	12	53	1	2300	0.0004	0.9999
	13		-1	3000	0.0013	0.9998
	14		1	1800	0.0042	0.9998
	15		-1	2200	0.0031	0.9995
	16		1	2600	0.0129	0,9962
U	17		-1	1100	0.0025	0.9983
	18		-1	2100	0.0046	0.9993
	19		1	3100	0.0052	0.9957
	20	55	1	2250	0.0005	0.9973
	21		1	1350	0.0002	0.9973
	22		-1	2250	0.0099	0.9983
	23		1	1800	0.0064	0.9986
	24		1	1400	0.0054	0.9992

Довжина вікна для кодування мітки взято $N = 166$, а ширина частотного інтервалу замішування $\Delta F = 70$ Гц. Нижче на рис. 3 розташовано вікно мовного файла-контейнера.

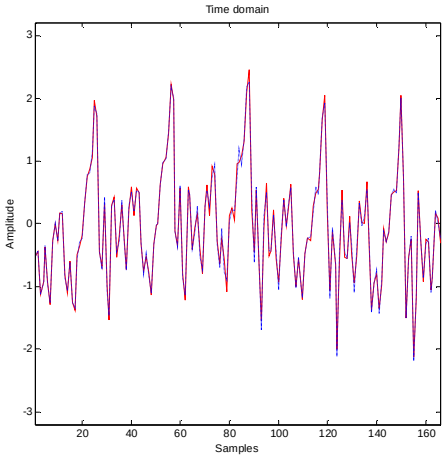


Рис.4 Сьоме вікно мовного сигналу файла-контейнера

Як видно з рис. 5 (а, б) після кодування біта, зміни в частотній області вікна аудіо- файла-контейнера не вплинуло на частотні інтервали, де не відбувалося кодування. При цьому ми бачимо зміни в тих частотних інтервалах, де відбувалося впровадження.

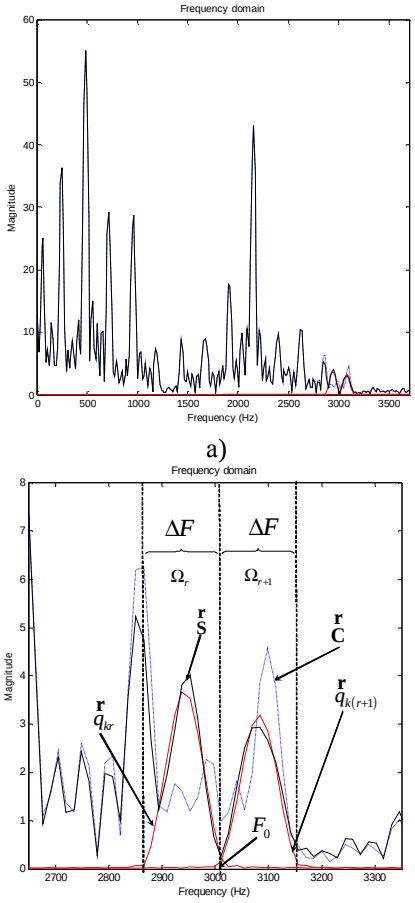


Рис.5 Модуль трансформанти Фур'є, для 7-го вікна

Висновок

Описаний спосіб рекомендується застосовувати як метод кодування з закритим ключем $\mathbf{K}\left((N,\Delta F),e,\vec{F}_0\right)$. Ключ визначає: тривалість вікна N, ширину частотних інтервалів де відбувається кодування $2\Delta F$, робастність системи e, позицію внесення мітки у частотній області F_0. Мітка руйнується в результаті навмисної атаки ЦВЗ, при цьому зберігається структура власного вектора $\vec{q}_{kr}$ субполосной матриці A_r, наявність якого свідчить про те, що даний аудіо- файл $\vec{X}$ був раніше помічений. Використання власних векторів $\vec{q}_{kr}$, власні числа яких близькі до одиниці $l_r \cong 1$, дозволяє підвищити стійкість до навмисним і пасивним атакам розробленої системи. Система самостійно визначає порог кодування, та може працювати без участі людини зберігаючи при цьому високу стійкість до пасивних атак запропонованих різними методами оцінювання.

Література

[1] Жиляков Е.Г. Вариационные методы анализа и построения функций по эмпирическим данным. – Белгород, Изд-во БелГУ, 2007. – 160с.