УДК 621.327

ОБҐРУНТУВАННЯ ДЕКОДОВАНОЇ СТІЙКОСТІ ДВОВИМІРНИХ ПОЛІАДИЧНИХ КОНСТРУКЦІЙ НА ПОМИЛКОВИХ ПІДСТАВАХ

Ларін В. В.

Харківський університет Повітряних Сил імені Івана Кожедуба

l_vv83@ukr.net

Обґрунтовано потенційну можливість для організації дешифровано-стійкого представлення зображень у системах поліадичного кодування. Показано, що поліадичне кодування дає змогу: будувати дешифровано-стійке представлення зображень у системах компресії; скоротити обсяг даних, що надходять на шифрування; знизити часові витрати на виконання шифрувальних операцій.

Ключові слова: криптосемантичні перетворення, компресія зображень, поліадичне кодування.

Proved the potential opportunity for the organization descramble resistant imaging systems in polyadyc coding. Shown that polyadyc encoding allows you to: builddescramble-resistant imaging systems in compression, reduce the amount of datagoing to encryption, reducing time spent on implementation of encrypting transactions.

Keywords: crypto semantic conversion, image compression, poliadical coding.

Основна частина

Побудова комбінованого дешифровано-стійкого представлення (ДШСП) зображень забезпечується в разі формування ключової інформації на основі вектора службової складової [1; 2]. Для поліадичної системи службові дані утворюються на базі динамічних діапазонів елементів двовимірного поліадичного числа (ДПЧ). Система службових даних ДПЧ має такі властивості:

а) впливає на процес формування кодограми інформаційної частини;

б) істотно характеризує зміст конкретного оброблюваного локального фрагмента зображення. Ця властивість заснована на тому, що динамічний діапазон є конкретною характеристикою оброблюваного фрагмента зображень і залежить від його семантичного змісту (отже, впливає на його смисловий зміст) [3; 4]. Динамічний діапазон не є усередненою характеристикою за класом зображень. Навпаки динамічний діапазон визначає як складову яскравості, яка має найбільше значення з позиції сприйняття зображення зором людини, а в деяких випадках характеризує позицію і величину контурного перепаду, що міститься в оброблюваному фрагменті зображення. Дійсно, якщо фрагмент зображення інформативний, тобто містить на основному тлі контур або дрібні об’єкти, то це приведе до наявності елементів зображень, що мають різні діапазони. Звідси динамічний діапазон у рядках і стовпцях, а отже, і підстави ДПЧ будуть нерівномірними.

Проте використання системи підстав G двовимірного поліадичного числа як базової інформації для побудови ключа в технології комбінованого ДШСП потребує наявності таких властивостей, а саме:

1) єдиності і взаємооднозначності декодування для варіанта безпомилкового відновлення всіх компонентів службових даних. Це означає необхідність виконання умов:

$$f^{(-1)}(N; G') = \begin{cases} A, \to G' = G; \\ A', \to G' \neq G, \end{cases} \qquad (1)$$

де $f^{(-1)}(N; G')$ — зворотний оператор отримання ДПЧ $A = \{a_{i,j}\}$ за значенням коду-номера N і системою підстав G'; G' — система підстав двовимірного поліадичного числа

Під умовою $G' = G$ розуміється випадок, коли підстави всіх елементів ДПЧ відновлені без помилок. Навпаки якщо $G' \neq G$, то знайдеться хоча б одна підстава системи G', для якого виконується умова $g'_{ij} \neq g_{ij}$.

Аналогічним чином під A' мається на увазі ДПЧ, що містить принаймні один елемент, для якого виконується умова $a'_{ij} \neq a_{ij}$.

Умова (1) указує на наявність властивості гарантованого спотворення як мінімум одного елементу початкового зображення у разі неправильного відновлення принаймні однієї підстави елементу ДПЧ;

2) поява помилки ε_{ij} у процесі відновлення елементу a_{ij} ДПЧ, підстава g_{ij} якого декодована неправильно, тобто якщо $g'_{ij} \neq g_{ij}$, то $a'_{ij} = a_{ij} \pm \varepsilon_{ij}$, де $|\varepsilon_{ij}| \neq 0$.

Тут g'_{ij}, g_{ij} — значення підстав відповідно для відновленого і початкового $(i; j)$-го елементів ДПЧ. Зрозуміло, що для $|\varepsilon_{ij}| \neq 0$ виконується нерівність $a'_{ij} \neq a_{ij}$;

3) наявність лавиноподібного зв’язуваного ефекту, що полягає в появі помилок відразу в послідовності відновлюваних елементів зобра-

ження в результаті неправильно відновленої підстави одного елементу ДПЧ, тобто
якщо

$$g'_{ij} \neq g_{ij},$$

то

$$|\varepsilon_{\eta\xi}| \neq 0, \text{ де } \eta,\xi \in \Omega \text{ та } |\Omega| = \theta \geq 2.$$

Тут Ω — безліч позицій елементів ДПЧ, для яких виконується умова $a'_{\eta\xi} \neq a_{\eta\xi}$.

Інакше кажучи, помилка в процесі відновлення однієї підстави повинна привести до виникнення помилок у декількох елементах фрагмента зображення. Зрозуміло, що помилки при відновленні підстав виникають унаслідок несанкціонованого доступу.

Розглянемо властивість поліадичної системи. Для цього сформулюємо і доведемо таку теорему.

Теорема про єдність системи підстав. Якщо значення першого елементу ДПЧ не дорівнює нулю, тобто $a_{11} \neq 0$, то:

— для заданого фрагмента зображення $A=\{a_{i,j}\}$ та системи підстав $G=\{g_{ij}\}$ можна сформувати єдине значення коду-номера N;

— за заданим значенням коду-номера N відновлення початкового ДПЧ $A=\{a_{i,j}\}$ без помилок можливе тільки для однієї системи підстав $G=\{g_{ij}\}$.

Доведення. Переконаємося, що виконується перша частина теореми. Припустимо, що знайдеться принаймні два рівні за значенням кодиномери N та N', які виходять для двох систем підстав G та G', що відрізняються значенням як мінімум однієї компоненти $g'_{ij} \neq g_{ij}$. Від величини підстави $(i;j)$-го елементу залежать значення вагових коефіцієнтів попередніх елементів ДПЧ. Тоді на основі виразу

$$N = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} V_{ij} \qquad (2)$$

отримаємо:

$$N = \sum_{\eta=1}^{i-1}\sum_{\xi=1}^{n} a_{\eta\xi} V_{\eta\xi} + \sum_{\xi=1}^{j-1} a_{i\xi} V_{i\xi} + a_{ij} V_{ij} + \sum_{\xi=j+1}^{n} a_{i\xi} V_{i\xi} + \sum_{\eta=i+1}^{m}\sum_{\xi=1}^{n} a_{\eta\xi} V_{\eta\xi};$$

$$N' = \sum_{\eta=1}^{i-1}\sum_{\xi=1}^{n} a_{\eta\xi} V'_{\eta\xi} + \sum_{\xi=1}^{j-1} a_{i\xi} V'_{i\xi} + a_{ij} V_{ij} + \sum_{\xi=j+1}^{n} a_{i\xi} V_{i\xi} + \sum_{\eta=i+1}^{m}\sum_{\xi=1}^{n} a_{\eta\xi} V_{\eta\xi}.$$

Без втрати спільності припустимо, що $g_{ij} > g'_{ij}$. Тоді, оскільки за припущення виконується рівність $N = N'$, то віднімаючи від першого виразу друге, одержимо співвідношення

$$a_{11}(V_{11} - V'_{11}) = \sum_{\xi=2}^{n} a_{1\xi}(V_{1\xi} - V'_{1\xi}) + \sum_{\eta=2}^{i-1}\sum_{\xi=1}^{n} a_{\eta\xi}(V_{\eta\xi} - V'_{\eta\xi}) + \sum_{\xi=1}^{j-1} a_{i\xi}(V_{i\xi} - V'_{i\xi}).$$

Оскільки відібрані елементи відповідають старшим елементам ДПЧ, то розділивши кожен доданок даної рівності на величину вагового коефіцієнта V_{ij} молодшого елементу, одержимо:

$$a_{11}\prod_{\gamma=2}^{n} g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n} g_{\eta\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}) = \sum_{\xi=2}^{n} a_{1\xi}\prod_{\gamma=\xi+1}^{n} g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n} g_{\eta\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}) + \sum_{\eta=2}^{i-1}\sum_{\xi=1}^{n} a_{\eta\xi}\prod_{\gamma=\xi+1}^{n} g_{\eta\gamma}\prod_{\ell=\eta+1}^{i-1}\prod_{\gamma=1}^{n} g_{\ell\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}) + \sum_{\xi=1}^{j-1} a_{i\xi}\prod_{\gamma=\xi+1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}). \qquad (3)$$

У зв'язку з тим, що величина $(g_{ii} - g'_{ij})$ є константою для всіх доданків виразу (2), його можна розглядати як запис співвідношення для визначення коду-номера двовимірного поліадичного числа, кількість елементів якого становить $n(i-1)+(j-1)$. У такому числі молодшим елементом буде елемент початкового ДПЧ, що має координати $(i;j-1)$. Водночас на основі властивостей поліадичної системи між ваговим коефіцієнтом першого елементу і правою частиною виразу (2) повинна виконуватися нерівність

$$\prod_{\gamma=2}^{n} g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n} g_{\eta\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}) > \sum_{\xi=2}^{n} a_{1\xi}\prod_{\gamma=\xi+1}^{n} g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n} g_{\eta\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}) + \sum_{\eta=2}^{i-1}\sum_{\xi=1}^{n} a_{\eta\xi}\prod_{\gamma=\xi+1}^{n} g_{\eta\gamma}\prod_{\ell=\eta+1}^{i-1}\prod_{\gamma=1}^{n} g_{\ell\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}) + \sum_{\xi=1}^{j-1} a_{i\xi}\prod_{\gamma=\xi+1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}). \qquad (4)$$

З іншого боку, згідно з припущенням $g_{ij} > g'_{ij}$ виконується нерівність

$$a_{11}\prod_{\gamma=2}^{n} g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n} g_{\eta\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}(g_{ii} - g'_{ij}) \geq \prod_{\gamma=2}^{n} g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n} g_{\eta\gamma}\prod_{\gamma=1}^{j-1} g_{i\gamma}.$$

Проте ця нерівність суперечить умові (3).

Звідки одержуємо, що таке припущення відносно $g'_{ij} \neq g_{ij}$ неправильне. Це означає, що для заданих елементів ДПЧ і фіксованої системи підстав у разі, коли $a_{ij} \neq 0$, можна отримати тільки одне значення коду-номера. Перша частина теореми доведена.

Доведемо другу частину теореми. Покажемо тепер єдність зворотного перетворення, тобто якщо $a_{ij} \neq 0$, то за заданим значенням коду-номера N відновлення початкового ДПЧ $A=\{a_{i,j}\}$ без помилок можливе тільки для однієї системи підстав $G=\{g_{ij}\}$. Інакше, якщо знайдеться принаймні одна підстава, для якої виконуватиметься нерівність $g'_{ij} \neq g_{ij}$, то при фіксованому N буде отримано ДПЧ $A'=\{a'_{i,j}\}$, отже, як мінімум, для одного елементу виконуватиметься нерівність $a'_{ij} \neq a_{ij}$.

Доведення проводитимемо від зворотного. Припустимо, що для $g'_{ij} \neq g_{ij}$ буде отримано ДПЧ без спотворень, тобто для всіх відновлених елементів виконується рівність $a'_{ij} = a_{ij}$, $i=\overline{1,m}$ та $j=\overline{1,n}$, тобто знайдеться як мінімум дві системи підстав, що відрізняються однією компонентою, так, що за заданим значенням коду-номера буде без помилок одержано початкове ДПЧ.

Тоді відповідно до виразу (2) для одного і того ж ДПЧ на основі двох різних систем підстав $G=\{g_{ij}\}$ та $G'=\{g'_{ij}\}$ можна сформувати як мінімум два однакові за значенням коди-номери. Але це твердження суперечить твердженню, доведеному в першій частині теореми.

Отже, для умови коли $a_{11} \neq 0$, за заданим кодом-номером і наявною системою підстав можна відновити тільки одне ДПЧ. Інакше кажучи, помилка хоч би в одній підставі поліадичної системи призведе до неправильного відновлення як мінімум одного елементу ДПЧ.

Початкове ДПЧ без помилок можна відновити за заданим кодом-номером тільки для відповідної системи підстав. Теорема повністю доведена.

На основі доведеної теореми витікає такий наслідок (висновок).

Висновок. У випадку, якщо перший елемент ДПЧ дорівнює нулю, тобто $a_{11} = 0$, то виведення теореми не виконується.

У цьому випадку різні системи підстав, що відрізняються підставою першого елементу, тобто $g'_{11} \neq g_{11}$, приведуть до отримання однакових кодів-номерів.

Доведення (наслідку, висновку) витікає з того, що підстава першого елементу не бере участі в отриманні значення коду-номера. Тому нульове значення першого елементу приводить до можливості вибору довільної цілочислової підстави, величина якої не впливатиме на код-номер.

Водночас зауважимо, що цей випадок не впливає на зниження рівня стійкості зображень, що дешифруються. Це зумовлено тим, що:

- нульове значення відповідає чорному кольору, тобто з погляду характеристик, яскравості, не несе інформацію про змістовне навантаження оброблюваного фрагмента зображення;
- на ідентифікацію решти елементів ДПЧ така умова не впливає, тобто значення коду-номера для решти елементів без урахування першого буде вже єдиним;
- вірогідність появи нульового елементу на початку поліадичного числа маловірогідна.

Звідси видно, що для безпомилкового дешифрування початкових даних потрібна інформація про значення коду-номера N і системи підстав ДПЧ $G=\{g_{ij}\}$.

Поліадичне кодування має властивість взаємооднозначності, що полягає в тому, що для послідовності елементів $A=\{a_{i,j}\}$, у якої всі елементи не дорівнюють нулю $a_{i,j} \neq 0$, і заданої системи підстав $G=\{g_{ij}\}$ можна сформувати тільки один код-номер N і навпаки.

Тому в разі застосування криптографічного перетворення для послідовності підстав ДПЧ точне відновлення початкових елементів буде неможливим, тобто не всі елементи поліадичного числа будуть одержані без похибки.

Висновки

Обгрунтовано можливість організації дешифровано-стійкого представлення мультимедійної інформації на етапі її кодового представлення на основі двовимірної поліадичної системи. Розроблений підхід ґрунтується на:

1) формуванні системи службових даних на базі динамічних діапазонів елементів ДПЧ, що забезпечує:

- створення умов для значущого впливу службових даних на процес формування кодограми інформаційної частини;
- службових даних, що характеризують зміст конкретного оброблюваного локального фрагмента зображення. Ця властивість заснована на тому, що динамічний діапазон є конкретною характеристикою оброблюваного фрагмента зображень і залежить від його семантичного змісту (отже, впливає на його зміст). Динамічний діапа-

зон не є усередненою характеристикою за класом зображень. Навпаки динамічний діапазон визначає як складову яскравості, яка має найбільше значення з позиції сприйняття зображення зором людини, а в деяких випадках характеризує позицію і величину контурного перепаду, що міститься в оброблюваному фрагменті зображення.

2) обґрунтуванні взаємооднозначності поліадичного уявлення, а саме:

- для заданого фрагмента зображення і системи підстав можна сформувати єдине значення коду-номера;
- за заданим значенням коду-номера, відновлення початкового ДПЧ без помилок можливе тільки для однієї системи підстав.

Отже, для умови коли $a_{11} \neq 0$, за заданим кодом-номером і наявною системою підстав можна відновити, тільки одне ДПЧ. Інакше кажучи помилка принаймні в одній підставі поліадичної системи призведе до неправильного відновлення як мінімум одного елементу ДПЧ. Початкове ДПЧ без помилок можна відновити за заданим кодом-номером тільки для відповідної системи підстав.

ЛИТЕРАТУРА

1. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. — М. : Техносфера, 2005. — 1073 с.

2. *Баранник В. В.* Структурно-комбинаторное представление данных в АСУ / В. В. Баранник, Ю. В. Стасев, Н. А. Королева // Монография. — Х. : ХУПС, 2009. — 252 с.

3. *Баранник В. В.* Методология создания криптографических преобразований на базе методов исключающих избыточность / В. В. Баранник, С. А. Сидченко, В. В. Ларин // Сучасна спеціальна техніка. — 2009. — № 4. — С. 5—17.

4. *Баранник В. В.* Формирование дешифрируемо-стойкого представления изображений в системах компрессии / В. В. Баранник, С. А. Сидченко, В. В. Ларин // міжнародна науково-практична конференція «Інформаційні технології та комп'ютерна інженерія», (Вінниця, 19—21 травня 2010 р.) / Вінницький національний технічний університет, 2010. — С. 40—41.

Стаття надійшла до редакції 15.05.11.