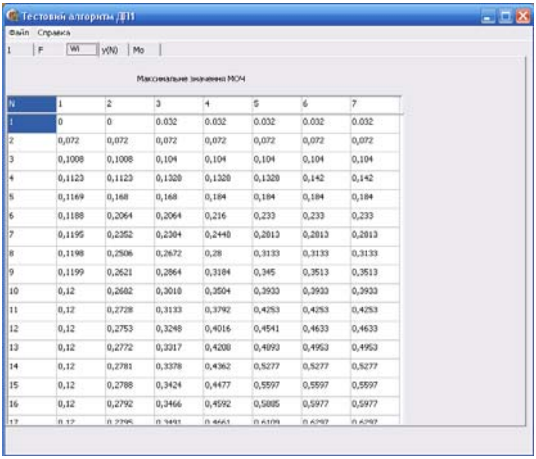
проектирования профилей, адаптивных угрозам за подклассами автоматизированных систем АС-1, АС-2, АС-3, разрабатываемая методика впервые будет предусматривать повышенное противодействие профилем угрозам нарушения не только конфиденциальности К, целостности Ц и доступности Д информации (подклассы К, Ц, Д), а также одновременно и угроз К, Ц, Д за подклассами КЦ, КД, ЦД, КЦД.



N	1	2	3	4	5	6	7
1	0	0	0.032	0.032	0.032	0.032	0.032
2	0,072	0,072	0,072	0,072	0,072	0,072	0,072
3	0,1008	0,1008	0,104	0,104	0,104	0,104	0,104
4	0,1123	0,1123	0,1320	0,1320	0,1320	0,142	0,142
5	0,1169	0,168	0,168	0,184	0,184	0,184	0,184
6	0,1188	0,2064	0,2064	0,216	0,233	0,233	0,233
7	0,1195	0,2352	0,2304	0,2440	0,2813	0,2813	0,2813
8	0,1198	0,2506	0,2672	0,28	0,3133	0,3133	0,3133
9	0,1199	0,2621	0,2864	0,3184	0,345	0,3513	0,3513
10	0,12	0,2682	0,3018	0,3504	0,3933	0,3933	0,3933
11	0,12	0,2728	0,3133	0,3792	0,4253	0,4253	0,4253
12	0,12	0,2753	0,3248	0,4016	0,4541	0,4633	0,4633
13	0,12	0,2772	0,3317	0,4208	0,4893	0,4953	0,4953
14	0,12	0,2781	0,3378	0,4362	0,5277	0,5277	0,5277
15	0,12	0,2788	0,3424	0,4477	0,5597	0,5597	0,5597
16	0,12	0,2792	0,3466	0,4592	0,5885	0,5977	0,5977
17	0,12	0,2795	0,3491	0,4661	0,6109	0,6297	0,6297

Рис 2. Программный модуль для оценки профиля противодействия угрозам на основе динамического программирования с использованием принципа оптимума Беллмана

1. *Гурин Л.С., Дымарский Я.С., Меркулов А.Д.* Задачи и методы оптимального распределения ресурсов. - М.: Сов. радио, 1968. - 464 с.

Поступила 22.02.2010р.

УДК 004.81

І.В. Хіміченко, аспірант МННЦІТтаС, Київ

МЕТОД ПІДВИЩЕННЯ ЧАСОВОЇ ЕФЕКТИВНОСТІ ПРИ ФРАКТАЛЬНОМУ СТИСНЕННІ ЗОБРАЖЕНЬ

У роботі P.Indyk і R.Motwani представлений метод вирішення задачі наближеного пошуку найближчого елементу, заснований на просторово чутливому хешуванні (метод LSH - locality sensitive hashing). Автори LSH пропонують використовувати просторове хешування для організації пошуку в додатках баз даних, розпізнаванні образів, пошуку в архівах документів.

Пропонується також модифікувати метод просторово чутливого хешування для організації пошуку найближчого сусіднього елементу при фрактальному стисненні зображень.

Мета

Метою статті є розгляд методу підвищення часової ефективності фрактального стиснення зображень на основі використання просторово-чутливого хешування.

Проблема

Однією з основних проблем при фрактальному стисненні зображень є розробка ефективного за часом методу зіставлення доменно-рангових областей.

Шляхи вирішення

На основі аналізу існуючих методів прискорення фрактального стиснення зображень зробити висновок про те, що найбільш перспективним і відповідним для подальшого поліпшення буде метод Саупа, який зведе задачу фрактального стиснення до задачі пошуку найближчого сусіднього елементу в багатовимірному метричному просторі за допомогою просторово-чутливого хешування.

Ідея

Для множини точок S, що містить проекції доменних блоків $D_k^{\perp} = \phi(D_k)$ та рангових блоків $R_m^{\perp} = \phi(R_m)$ на $\Re^n \setminus \Im$, з мірою відстані (у нашому випадку Евкліда), сімейство LSH функцій визначене таким чином:

Множина хеш-функцій $H = \{h : S \to U\}$ називається (r_1, r_2, p_1, p_2)-чутливими для $d(\cdot,\cdot)$, якщо для будь-якої проекції рангового і доменного блоку $R_m^{\perp}, D_k^{\perp} \in S$ на $\Re^n \setminus \Im$ виконується

якщо $D_k^{\perp} \in B(R_m^{\perp}, r_1)$, *то* $\Pr_H\left[h(R_m^{\perp}) = h(D_k^{\perp})\right] \geq p_1$,

якщо $D_k^{\perp} \notin B(R_m^{\perp}, r_2)$, *то* $\Pr_H\left[h(R_m^{\perp}) = h(D_k^{\perp})\right] \leq p_2$.

де $B(x,r)$ - гіперсфера радіусом r в сенсі міри відстані $d(\cdot,\cdot)$ з центром в точці x, а $\Pr_H\left[h(R_m^{\perp}) = h(D_k^{\perp})\right]$ - вірогідність того, що хеш-функція утворює колізію для даних проекцій рангового і доменного блоку $R_m^{\perp}$ та $D_k^{\perp}$.

Застосування просторово-чутливого хешування для вирішення задачі фрактального стиснення зображень

Для того, щоб просторово-чутлива функція хешування була корисною з погляду її застосування до фрактального стиснення зображень, вона повинна задовольняти нерівностям $p_1 > p_2$ та $r_1 < r_2$.

У спеціальній літературі прийнято позначати задачу наближеного пошуку сусіднього елементу як $(\tau, c) - NN$ задачу, при цьому $r_1 = \tau$ та

$r_2 = c \cdot \tau$. Покажемо, як просторово-чутливі функції можуть бути використані для вирішення $(\tau, c) - NN$ задачі при фрактальному стисненні: для даного сімейства H хеш-функцій, що володіють параметрами (r_1, r_2, p_1, p_2), збільшимо розрив між «високою» вірогідністю p_1 і «низькою» вірогідністю p_2 шляхом з'єднання декількох функцій. Зокрема, для параметра K, значення якого буде встановлено нижче, визначимо сімейство функцій $\Psi = \left\{ g : S \to U^K \right\}$ таким чином, що $g(D_k^{\perp}) = \left(h_1(D_k^{\perp}), ..., h_K(D_k^{\perp}) \right)$, де $h_i \in H$. Для цілого числа L виберемо L функцій $g_1, ..., g_L$ з Ψ, незалежно і рівномірно, випадковим чином. Під час кроку передобчислень, збережемо кожну проекцію доменного блоку $D_k^{\perp} \in S$ в наборі $g_j(D_k^{\perp})$ для кожного $j = 1, 2, ..., L$. Оскільки загальна кількість таких множин може бути великою, залишимо тільки непорожні набори шляхом повернення до класичного хешування. Для того, щоб обробити ранговий блок R_m, проводимо пошук серед всіх множин $g_1(R_m^{\perp}), ..., g_L(R_m^{\perp})$. Оскільки можливо (хоча і маловірогідно) що спільна кількість доменів, збережених в цих множинах, є великою, то пошук домена припиняється після знаходження $3L$ елементів (включаючи дублікати). Нехай $D_1^{\perp}, ..., D_t^{\perp}$ - знайдені елементи. Для кожного домена $D_{1,...,t}$ повертаємо відповідь «ТАК» (тобто даний домен є потенційним кандидатом побудови перетворення в ранговий блок R_m), якщо $D_{1,...,t} \in B\left(R_m^{\perp}, r_2 \right)$, інакше повертаємо відповідь «НІ». Параметри K та L вибираються так, щоб гарантувати, що наступні дві властивості виконуються із заданою вірогідністю:

Якщо існує $D_k^* \in B\left(R_m, r_1 \right)$, то $g_j(D_k^*) = g_j(R_m^{\perp})$ для деякого $j = 1, ..., L$

Загальна кількість колізій $R_m^{\perp}$ з точками з $S - B(D_k^{\perp}, r_2)$ менша, ніж $3L$ (параметр визначений емпіричним шляхом) тобто:

$$\sum_{j=1}^{L} \left| \left(S - B(D_k^{\perp}, r_2) \right) \cap g_j^{-1} \left(g_j(D_k^{\perp}) \right) \right| < 3L .$$

Якщо виконуються обидві властивості, то алгоритм є коректним. Звідси випливає, що якщо встановити $K = \log(1/p_2)$, і $L = n^{\rho}$, де

$$\rho = \frac{\ln(1/p_1)}{\ln(1/p_2)}, \tag{1}$$

то властивості (1) і (2) виконуються з постійною вірогідністю. Таким чином, отримуємо наступну теорему, яка стосується залежності ефективності вирішення $(\tau,c)-NN$ задачі при фрактальному стисненні зображень від параметрів LSH:

Передбачимо, що існує $(\tau, c\cdot\tau, p_1, p_2)$ - чутливе сімейство функцій хешування H для міри відстані $d(\cdot,\cdot)$. Тоді існує алгоритм для вирішення $(\tau,c)-NN$ задачі для міри $d(\cdot,\cdot)$, який використовує $O\left(dn_d + n_d^{1+\rho}\right)$ пам'яті, з часом обробки одного запиту, визначеним $O(n_d^{\rho})$ обчислень відстані і $O(n_d^{\rho}\log(1/p_2)\cdot n_d)$ обчислень хеш-функцій з H, де ρ визначений як (1).

Адаптація просторово-чутливих хеш-функцій до фрактального стиснення зображень на основі p-стійких розподілів

Стійкі розподіли визначаються як границі нормалізованих сум незалежних рівномірно розподілених випадкових змінних (нижче дано альтернативне визначення). Найбільш відомий приклад стійкого розподілу - це нормальний (гаусовий) розподіл. Проте, клас таких розподілів є значно ширшим. Розподіл μ над $\Re$ називається p-стійким, якщо існує $p \geq 0$ таке, що для будь-яких d, дійсних чисел $v_1,...,v_d$ та змінних $X_1,...,X_d$ з розподілом μ, випадкова змінна $\sum_i v_i X_i$ має такий же розподіл, як і змінна $\left(\sum_i |v_i|^p\right)^{1/p} X$ де X - випадкова змінна з розподілом μ.

Відомо, що стійкі розподіли існують для будь-якого $p \in (0,2]$. Зокрема, гаусовий (нормальний) розподіл μ_G, визначений як функція щільності вірогідності

$$g(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2},$$

є 2-стійким.

Зауважимо, що з практичної точки зору, не дивлячись на недолік закритих форм функцій розподілу щільності, відомо, що можна створити p-стійку випадкову змінну з двох незалежних випадкових змінних, рівномірно розподілених на інтервалі $[0,1]$.

Використовуючи p-стійкі розподіли, побудуємо сімейство хеш-функцій H, адаптоване до фрактального стиснення зображень. Інтуїтивно, сімейство хеш-функцій має бути просторово-чутливим, тобто якщо два вектори $R_m^{\perp}, D_k^{\perp}$ близькі один до одного (значення $\left\|R_m^{\perp} - D_k^{\perp}\right\|_p$ відносно невелике), то вони повинні з великою вірогідністю викликати колізію (мати одне і те ж значення хеш-функції) і, якщо вони розташовані далеко один від одного, то вірогідність колізії має бути мала. Нехай a - вектор розмірності d, елементи якого вибираються незалежно з p-стійкого розподілу. Скалярний добуток $\left\langle a, R_m^{\perp} \right\rangle$ проектує кожен вектор на множину дійсних чисел. З p-стійкості випливає, що для двох векторів $R_m^{\perp}, D_k^{\perp}$ відстань між їх проекціями $\left| \left\langle a, R_m^{\perp} \right\rangle - \left\langle a, D_k^{\perp} \right\rangle \right|$ розподілено як $\left\| R_m^{\perp} - D_k^{\perp} \right\|_p X$, де X - це випадкова змінна, що вибрана з p-стійкого розподілу. Якщо «розділити» множину дійсних чисел на підмножини рівного розміру r та визначити значення хеш-функції для вектора залежно від того, на яку підмножину він проектується, то інтуїтивно ясно, що така хеш-функція буде просторово чутлива в описаному вище сенсі.

Формально, кожна хеш-функція $h_{a,b}(v) : \Re^d \to N$ відображує вектор v розмірності d (проекція рангового $R_m^{\perp}$ або доменного блоку $D_k^{\perp}$) на множину цілих чисел. Кожна хеш-функція в сімействі однозначно визначається вибором випадкового вектора a, визначеного вище, і дійсного числа b, вибраного випадковим чином з діапазону $[0, r]$. Для даних a, b визначимо хеш-функцію $h_{a,b}$ таким чином:

$$h_{a,b}(v) = \left\lceil \frac{\langle a, v \rangle + b}{r} \right\rceil \tag{2}$$

Тепер обчислимо вірогідність колізії хеш-функції, вибраної випадково згідно описаним вище міркуванням, для двох векторів $R_m^{\perp}, D_k^{\perp}$. Нехай $f_p(t)$ позначає щільність вірогідності абсолютного значення p-стійкого розподілу. Для двох векторів $R_m^{\perp}, D_k^{\perp}$ Нехай $c = \left\| R_m^{\perp} - D_k^{\perp} \right\|_p$. Для випадково вибраного вектора a, елементи якого узяті з p-стійкого розподілу, $\left| \left\langle a, R_m^{\perp} \right\rangle - \left\langle a, D_k^{\perp} \right\rangle \right|$ розподілене як cX, де X - випадкова змінна, вибрана з p-стійкого розподілу. Оскільки b вибране випадково з діапазону $[0, r]$, легко побачити, що

$$p(c) = \Pr_{a,b}\left[h_{a,b}(R_m^{\perp}) = h_{a,b}(D_k^{\perp}) \right] = \int_0^r \frac{1}{c} f_p\left(\frac{t}{c}\right)\left(1 - \frac{t}{r}\right) dt$$

Для фіксованого параметра r вірогідність колізії монотонно зменшується із зростанням з $c = \left\| R_m^{\perp} - D_k^{\perp} \right\|_p$. Згідно визначення, що було дане на початку параграфа, сімейство хеш-функцій $h_{a,b}(v)$ є (r_1, r_2, p_1, p_2)-чутливим для $p_1 = p(1)$ та $p_2 = p(c)$ при $r_2 / r_1 = c$.

Параметр r не був чітко визначений, оскільки він залежить від значень c та p. Для кожного даного c задача полягає у виборі такого кінцевого значення r, яке робить ρ якомога меншим.

Висновок

У даній статті розглянуті аспекти застосування просторово-чутливого хешування при фрактальному стисненні зображень. Описані достоїнства даного методу, його природна пристосованість для вирішення задач, що виникають при фрактальному стисненні. Стаття може бути використана для наведення оцінок вимог алгоритму до пам'яті і вірогідності негативної відповіді на запит для кожної рангової області.

Результати проведеної роботи говорять про доцільність застосування просторово-чутливого хешування при вирішенні задач фрактального стиснення зображень.

1. *Indyk P.. Motwani R.* Approximate nearest neighbor: towards removing the curse of dimensionality. Proceedings of the Symposium on Theory of Computing, 1998.
2. *Indyk P.* Stable distributions, pseudorandom generators, embeddings and data stream computation. Proceedings of the Symposium on Foundations of Computer Science, 2000.
3. *Saupe D., Hamzaoui R.* A guided tour of the fractal image compression literature, in: New Directions for Fractal Modeling in Computer Graphics, J. Hart (ed.), ACM SIGGRAPH'94 Course Notes 13, 1994.
4. *Friedman J.H., Bentley J.L., Finkel R.A.* An algorithm for finding best matches in logarithmic expected time, ACM Trans. Math. Software 3,3 (1977) 209-226.
5. *Darrell T., Indyk P., Shakhnarovich G. (eds.)*, Locality-sensitive hashing using stable distributions, Nearest Neighbor Methods in Learning and Vision: Theory and Practice, MIT Press, 2006.
6. *Boss R.D., Jacobs E.W.* Archetype classification in an iterated transformation image compression algorithm, in: Fractal Image Compression Theory and Applications, Y. Fisher (ed.), Springer-Verlag, New York, 1994.
7. *Arya S., Mount D.M., Netanyahu N.S., Silvernam R., Wu A.* An optimal algorithm for approximate nearest neighbor searching, Proc. 5th Annual ACM-SIAM Symposium on Discrete Algorithms (1994) 573-582.

Поступила 25.02.2010р.