УДК 004:004.65

к.т.н. **Муляр І.В.**
(ХмНУ)
к.т.н. **Джулій А.В.** (ХмНУ)
Гіль Є.В. (НТУУ «КПІ»)

МЕТОДИ СТВОРЕННЯ І ПЕРЕВІРКИ ХЕШУ ГРАФІЧНИХ ЗОБРАЖЕНЬ

У статті розлянуті підходи для обчислення статистичних значень графічних зображень, які захоплять головні особливості зображення і залишаються по суті незміненними через прийнятні перетворення. Запропоновані методи є гнучкими і можуть використовуватися для рішення інших задач.

Ключові слова: графічні зображення, ідентифікації повідомлення, хешування зображення.

В статье рассмотрены подходы для вычисления статистических значений графических изображений, которые захватят главные особенности изображения и остаются по сути незминеннимы через приемлемые преобразования. Предложенные методы являются гибкими и могут использоваться для решения других задач.

Ключевые слова: графические изображения, идентификации сообщения, хеширования изображения.

In the article the approaches for calculation of statistical values of graphic representations which will grasp the main features of the image are considered and remain as a matter of fact not changed through comprehensible transformations. The offered methods are flexible and can be used for the decision of other problems.

Keywords: graphic representations, message identifications, hashing images.

Вступ. Задача методів ідентифікації графічних зображень - знайти спотворення вмісту та визначити автора об'єкта даних. Два головні криптографічні примітиви для забезпечення достовірності - це коди ідентифікації повідомлення (MAC) і цифрові системи підпису (DS). В даних системах, щоб ідентифікувати об'єкт даних m, алгоритм генерації використовується для отримання ознаки ідентифікації t, який приєднується до об'єкта, щоб сформувати $m||t$. Алгоритм перевірки бере об'єкт та пару ознак $o||t$ і проводить порівняння та визначає (достовірність) справжній об’єкт чи ні. У системах MAC ключ генерації і верифікації однаковий (або один може бути легко одержаний з іншого), і система називається симетричною ключовою система. Недоліком симетричних ключових систем – є те, що вони не забезпечують «неможливості відмови від авторства»: відправник може відхилювати повідомлення, яке він послав. У системах DS, ознака ідентифікації також називається підписом і використовується не тільки для ідентифікації але і для забезпечення «неможливості відмови від авторства». Головний недолік систем DS - те, що вони потребують багато дорогоцінних ресурсів для обчислень.

Постановка задачі. Метод хешування зображення H бере довільне зображення I і створює строку бітів x_i. На відміну від криптографічних хеш-функцій, алгоритми хешування зображення повинні бути позбавлені чутливості до бітів і створювати таке ж значення для подібних зображень, які є визначеними через набір A - допустимих перетворень, це ті перетворення, які не змінюють головні особливості зображення. Ми говоримо зображення I' подібне I, якщо $I' = a(I)$; $a \in A$. Нам також потрібно визначити набір A' неприпустимих перетворень, які складаються з перетворень, застосованих до цілого зображення, як наприклад компресія в низькому якісному чиннику з метою пошкодження важливих деталей зображення, і локалізованої модифікації вмісту.

Метод хешування повинен створювати 'близькі' значення для зображень, які одержані через прийнятні перетворення, і 'віддалені' значення для зображень, які одержані

через неприпустимі перетворення. Щоб визначити 'близькі' і 'віддалені' значення необхідна функції відстані.

Мірою відстані між двома значеннями *v* та *v'* є кореляційний коефіцієнт $d_{CC}(v,v')$

$$d_{CC}(v,v') = \frac{\sum_{i=0}^{n}(v_i - \overline{v_i})(v'_i - \overline{v'_i})}{\sqrt{\sum_{i=0}^{n}(v_i - \overline{v_i})^2} \cdot \sqrt{\sum_{i=0}^{n}(v'_i - \overline{v'_i})^2}} \quad (1)$$

та Евклідова відстань $d_{ED}(v,v')$

$$d_{ED}(v,v') = \sqrt{\sum_{i=0}^{n}(v_i - v_i')^2}. \quad (2)$$

Якщо хеш значення близькі $d_{ED}(H(I),H(I')) \in (-\varepsilon, 1+\varepsilon)$ або $d_{ED}(H(I),H(I')) < \varepsilon$, ми стверджуємо що два зображення є схожими і визначаємо рівень достовірності цього твердження.

Методи створення і перевірки хешу графічних зображень. Методи хешування зображення, які використовуються для ідентифікації повинні мати таку властивість, щоб було неможливо створити два зображення *I* та *I'* які схожі та $I' <> a(I);\ a \in A$.

Для гарного алгоритму хешування, вірогідність позитивної неправди і негативної неправди, повинна залишитися маленькою.

Основна ідея - вирахувати статистичні значення, які захоплять головні особливості зображення і залишаться по суті незміненими через прийнятні перетворення. Тут, незмінене означає що хеш значення буде близьким. Для набору допустимих перетворень відносимо компресію JPEG з різними якісними рівнями. Всі інші перетворення, зокрема фільтрацію, вважаємо неприпустимими маніпулюваннями, які повинні бути знайденими системою. Проте запропоновані системи є гнучкими і можуть використовуватися з іншими визначеннями.

Статистика отримується з певних регіонів зображення. Регіони можуть бути одержані через розподіл зображення на блоки або через алгоритми сегментації, або випадково за допомогою вибору підмножини пікселів. Використовуються дві наступні статистики:

- середнє $\overline{x} = \frac{\sum_1^n x_i}{n}$
- відхилення від норми $S = \frac{\sum_1^n (x_i - \overline{x})^2}{n}$

Алгоритм K-середні/LBG розроблений для процедур кластерізації в розпізнаванні образів і може бути описаний як вказано нижче.

Наданий великий набір векторів виходу від джерела, відомого як нвчальний набір, і початковий набір характерних зразків *k*, призначити кожний елемент нвчального набору найближчим характерним зразкам. Коли елементи призначені, характерний зразок відновлюється за допомогою обчислення центру нвчальних векторів, призначених для нього. Коли процес призначення завершений, ми матимемо групи *k* векторів, що зібрані навколо кожної з точок виходу.

Заснований на цьому алгоритмі метод складається з наступних етапів:

1. Починаємо з відновлених даних $\{v_i(0)\}_{i=1}^{M}$ і набору нвчальних значень $\{X_n\}_{n=1}^{N}$, встановимо $k = 0,\ D^{(0)} = 0$. Виберемо границю ε.

2. Регіони квантування $\{V_i(k)\}_{i=1}^{M}$ дані

$$V_i(k) = \{X_n : d(X_n, Y_i) \le d(X_n, Y_j)\ \forall\ j \ne i, i = 1,\ldots,M\}.$$

Припустимо жоден з регіонів не є порожнім.

3. Підрахуємо середнє викривлення $D(k)$ між нвчальними записами та відновленими.

4. якщо $\frac{D^{(k)}-D^{(k-1)}}{D^{(k)}}<\varepsilon$ вихід, якщо ні – продовжуємо.

5. *k=k+1.* Знаходимо нові відновлені значення які є середніми значеннями квантування регіонів $V_i^{(k-1)}$. Перехід на крок 2.

Створення хешу і перевірка складається з трьох методів. Перші два методи засновано на статистиці регіону: середнє, середнє квадратичне відхилення, і третій метод заснований на «книзі шифрування» навченій на стислих векторах особливостей зображень.

Метод 1.

Створення хешу. Нехай A_σ складається з усіх JPEG алгоритмів до рівня якості σ.

1. Поділимо зображення на блоки розміром $a\times b$. Припустимо ми отримали $m\times n$ блоків.

2. Для кожного блоку визначимо статистики S_{ij}^o, $i=1,...,m,\ j=1,...,n.$

3. Для всіх зображень $I_m=a(I),\ a\in A_\sigma$ повторимо кроки 1 та 2 для отримання S_{ij}^m.

4. Знайдемо різницю статистик між зміненим блоком та відповідним блоком оригінального зображення $\left|S_{ij}^o-S_{ij}^m\right|$.

5. Для всіх $i=1,...,m,\ j=1,...,n.$ знайдемо $\tau=\max_{a\in A_\sigma}\left|S_{ij}^o-S_{ij}^m\right|$ та поріг $T_\sigma=\tau$.

Хеш значення зображення складається з послідовності статистик оригінального зображення S_{ij}^o, розміром $a\times b$, та пороговим значенням T_σ. Розмір блоку визначає рівень похибки статистики. Вибір малого блоку $a\times b$ створить довгі рядки підпису, вибір великого – до втрати деяких даних.

Перевірка хешу. Щоб визначити чи кандидат I_c має той самий хеш x_i що і I виконаємо наступні кроки:

Обчислимо $\left|S_{ij}^o-S_{ij}^c\right|,\ i=1,...,m,\ j=1,...,n$

якщо $\left|S_{ij}^o-S_{ij}^c\right|\le T_\sigma,\ i=1,...,m,\ j=1,...,n$ то I_c перекривається з I.

Експерименти показали, що в більшості випадків середнє квадратичне відхилення виконувалося краще, ніж середнє значення, вибір середнього квадратичного відхилення, компенсував більше компресії, ніж вибір середини. Тому ми рекомендуємо використовувати середнє квадратичне відхилення замість середини. Також помічено, що за винятком умисних маніпулювань, обертання створило максимальну різницю в статистиках.

Метод -2.

Генерація хеш. Створення хешу на основі методу *к-середини*. Оригінальне зображення поділено на P частин за допомогою алгоритму *к-середини*. «Книга шифрування» навчена на векторах особливостей оригінального та стиснутого зображення.

1. Визначаємо статистику S_i^o для кожного регіону $i=1,...,P$.

2. Для всіх зображення $I_m=a(I),\ a\in A$ використовуємо «книгу шифрування» для сегментування та отримання статистики S_i^m.

3. Знаходимо евклідову відстань D_m між статистикою зміненого зображення та статистикою оригінального зображення S_i^o, $D_m=\sqrt{\sum\left(S_i^o-S_i^m\right)^2}$.

4. Визначаємо поріг T на основі D_m для змінених зображень $I_m=a(I),\ a\in A$.

5. Хеш значення складається з послідовності статистик оригінального зображення S_i^o, кількості регіонів P, статистики, що використовується, «книги шифрування» та порогу T.

Перевірка хешу. Щоб перевірити чи значення хешу зображення кандидата I_c таке ж як значення хешу початкового зображення зробимо наступне.

1. Сегментуємо зображення I_c на P частин, використовуємо алгоритм *к-середини* для отримання «книги шифрування»

2. Визначаємо статистику S_i^c для цих регіонів.

3. Визначаємо Евклідову відстань D_c між I_c та I. Якщо $D_c \le T$ то хеш значення однакові, інакше – різні.

"Книга шифрування" отримується за допомогою прийнятних модифікацій зображення. Зараз, якщо зображення кандидата створено за допомогою прийнятної модифікації, сегменти є дуже подібними до сегментів початкового зображення і відтепер статистика регіонів близька до початкового зображення і відстань Евкліда між двома сегментами найменша. Якщо зображення отримане в результаті неприпустимого перетворення, регіони різні і відстань велика.

Метод - 3 - використовує книгу шифрування навчену на векторах особливості зображень.

1. Беремо зображення I та зображення JPEG стиснуте з різними рівнями якості.

2. Знаходимо вектори особливостей які містять значення пікселів (p), середні значення сусідніх пікселів $\bar{x}$, та стандартне відхилення сусідніх пікселів σ для всіх вищезгаданих зображень. Це і є набір нвчальних значень T_c. З цього слідує, що $(p, \bar{x}, \sigma) \in T_{c_i}$ та $(p, \bar{x}, \sigma) \in T_c = T_{c_1} \cup T_{c_2} \cup \ldots \cup T_{c_k}$, де T_{c_i} - набір нвчальних значень векторів особливостей стиснутих зображень I_i.

3. Навчаємо книгу шифрування I_c на наборі значень T_c створеного вище, використовуючи тільки стиснуті зображення.

4. Нехай $FC = \{C_1, C_2, \ldots, C_p\}$ - книга шифрів створена вище.

5. За допомогою FC виконаємо декілька ітерацій алгоритму використовуючи набір значень T_{c_i}.

6. Припустимо $FC' = \{C'_1, C'_2, \ldots, C'_p\}$ відхиленням у Евклідової відстані буде $ED_{comp} = \sqrt{\sum_{i=1}^{p} (C_i - C'_i)^2}$

7. Повторимо крок 5 знову, використовуючи набір значень T_f створеного з векторами особливостей зміненого зображення I_f. Нехай $FC^o = \{C^o_1, C^o_2, \ldots, C^o_p\}$ - книга шифрування після одної ітерації. Тоді відхилення у Евклідової відстані буде $ED_{other} = \sqrt{\sum_{i=1}^{p} (C_i - C^o_i)^2}$.

8. Шукаючи максимальне і мінімальне значення ED_{comp} для кожного стиснутого зображення I_i, встановлюємо границі для прийнятних відстаней Евкліда $[a, b]$.

9. Хеш складається з *FC*, *a* і *b*. Розмір хешу буде $(p \times 3) + 2 \times r$ байтів де p – розмір книги шифрування, а r –кількість байтів для представлення справжнього значення.

Перевірка хешу. Для того щоб перевірити чи зображення I_c має той самий хеш, що і I необхідно:

1. Створимо послідовність векторів особливостей для кожного значення пікселя, середні значення сусідніх пікселів, та стандартне відхилення сусідніх пікселів.

2. Зробимо ітерацію *LBG* на отриманій *DC*. Нехай $FC^r = \{C^r_1, C^r_2, \ldots, C^r_p\}$ - книга шифрування після іншої ітерації, тоді відхилення у Евклідової відстані буде $ED_{received} = \sqrt{\sum_{i=1}^{p} (C_i - C^r_i)^2}$.

3. Якщо отримана Евклідова відстань попадає в проміжок $[a,b]$ тоді хеші зображень співпадають.

Експеримент, для підтвердження Методу-3 показав, що при збільшенні чіткості зображення має найвище відхилення на всіх зображеннях. На деяких зображеннях, оскільки розмір книги шифрування було збільшено, початкове зображення показало невелике відхилення в Евклідових відстанях в порівнянні зі стиснутими.

Висновки. Алгоритм хешування графічних зображень повинен створювати 'близькі' значення для зображень, які одержані через прийнятні перетворення, і 'віддалені' значення для зображень, які одержані через неприпустимі перетворення.

Метод-1 використовує блоки однакового розміру для кожної модифікації, тоді як регіони, що є результатом *k-седенинної сегментації* методу-2, не є однаковими для кожної модифікації. Метод-1 виконується краще, тому що він порівнює статистику відповідності блоків такого ж розміру, тоді як в методі-2 регіони, поділені на сегменти, не можуть зберігати такий же розмір для кожної модифікації. Метод-1 простий для здійснення і система відносно швидка, тоді як метод-2 дуже дорогий в термінах часу і складності за рахунок сегментації. Збільшення числа блоків або зменшення розміру блоку покращує роботу методу-1 за рахунок довгого хешу, тоді як збільшення числа регіонів не сильно впливає на продуктивність роботи методу-2.

ЛІТЕРАТУРА:

1. Арун Н. “Цифрові зображення: Представлення і компрессія”/ Нетравалі, Арун Н. та Хаскель, Баррі Г./ Нью-Йорк, 2002р. – 430 с.

2. Лин та Чанг, ”Створення надійного цифрового підпису для идентифікації медіа”/ Лин та Чанг /, 1998р.- 270 с

3. Анин Б.Ю. Защита компьютерной информации / Анин Б.Ю. / – СПб.: БХВ. – Санкт-Петербург, 2000г. – 580 с, ил.

4. Ричард Э.Смит «Аутентификация: от паролей до открытых ключей / Ричард Э.Смит // Издательский дом «Вильяме», 2002 г. – 348 с, ил.

Рецензент: д.т.н., проф. Лєнков С.В.