DOI 10.31891/2307-5732-2020-281-1-76-79
УДК 004.891

В.М. ДЖУЛІЙ, Ю.П. КЛЬОЦ, І.В. МУЛЯР, В.М. ЧЕШУН
Хмельницький національний університет

ІТЕРАЦІЙНО-ГЕОМЕТРИЧНИЙ МЕТОД ДЛЯ СТІЙКОГО ПЕРЦЕПТУАЛЬНОГО ХЕШУВАННЯ ЗОБРАЖЕННЯ

В роботі запропоновано уніфіковану структуру для перцептивного медіа хешування. Також розвивається формальний (кількісний) опис потрібних властивостей перцептивного хешування зображення. Головна мета – розглянути фундаментальні ідеї у перцептивному хешуванні зображення. Для підвищення ефективності обробки інформації в автоматизованих системах управління та обробки зображень виникає необхідність розробки методів надійного хешування та ідентифікації графічних зображень. У статті розглянуті підходи для обчислення статистичних значень графічних зображень, які захоплять головні особливості зображення і залишаються по суті незмінними через прийняті перетворення. Запропоновані методи є гнучкими і можуть використовуватися для розв'язування інших задач.

Ключові слова: хешування зображення, алгоритми, ідентифікація, метод, хеш функція, ідентифікатор, електронний підпис.

V.M. DZHULII, Y.P. KLOTS, I.V. MULIAR, V.M. CHESHUN
Khmelnytskyi National University

ITERATION-GEOMETRIC METHOD FOR PERMANENT PERCIPTUAL HASHING OF IMAGE

The purpose of the work is to create a unified structure for perceptual media hashing. The main goal is to consider fundamental ideas in perceptual hashing of an image. To increase the efficiency of information processing in automated control systems and image processing, there is a need to develop methods for reliable hashing and identification of graphic images. Improving the efficiency will significantly expand the scope of application software in control systems and information processing. This approach will be useful for identifying images in databases, in which it is possible to make various changes to the image, such as compression and format changes, general signal processing algorithms, scanning, or creating watermarks. Developed basic clustering, allows clusters not to bear any losses. Based on the study, two main goals of perceptual image hashing have been identified: resistance to unintentional or perceptually minor image modifications - perceptual hash persistence; the ability to withstand deliberate attacks (caused by a malicious opponent) is a hash of security. The hash of the security properties is closely related to the randomization scheme that is used when creating the hash algorithm. Another extremely important question that needs to be answered is what hash length is required to successfully obtain the desired level of stability. The theoretical analysis of randomized media hashing algorithms and the quantitative relation of randomized parameters with hash security has not yet been addressed in the literature. 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: image hashing, algorithms, identification, method, hash function, ID, electronic signature.

Вступ

Зображення як носій інформації є джерелом первинних даних у численних напрямках людської діяльності: екологічні, космічні, геологічні та біологічні дослідження. Проблемам створення комп'ютерного зору та питанням цифрової обробки зображень приділяють велику увагу багато дослідників, оскільки кількість практичних задач, у яких використовуються зображення або результати їх аналізу, весь час зростає. Тому оброблення та розпізнавання зображень є невід'ємною складовою частиною сучасних інформаційних систем.

Важливе значення в конструюванні технологій машинного сприйняття та інтерпретації зображень мають методи та алгоритми розпізнавання зображень. Завдяки популярності цифрових технологій, сьогодні створюється та зберігається все більше і більше цифрових зображень. Виникає проблема управління великими базами зображень. Без ретельного пошуку по всіх записах, важко визначити чи вже існує зображення у базі даних. Подальші труднощі виникають через те, що два зображення, які видаються однаковими для ока людини, можуть мати різні цифрові представлення, що ускладнює порівняння пари зображень, наприклад, оригінальне зображення та його стиснута версія; зображення, що зберігається із використанням чітких перетворень, чи зображення, поліпшене через операції загальної обробки знаків.

Все це спонукало до розробки алгоритмів для створення підходящих ідентифікаторів зображення, або хеш функцій зображення. Одним з можливих варіантів отримання із зображення залежних від вмісту, коротких двійкових ланцюжків, є використання традиційних криптографічних хешів, таких як MD5 та SHA-256, SHA-384, SHA-512 [1]. Проте, проблема, яка пов'язана з ними, полягає в тому, що вони надзвичайно чутливі до повідомлення, тобто найменша зміна у введеній інформації радикально змінює результат. Замість цього, ці ідентифікатори повинні обов'язково брати до уваги зміни у візуальній зоні та фіксувати важливі перцептивні властивості зображення. Подальша потреба для такого дескриптора зображення виникає на підставі контролю цілісності. Через легкість копіювання цифрових медіа, цифрові дані можуть підроблятись, тому існує потреба перевірки вмісту медіа, щоб переконатись у його автентичності.

Постановка задачі

На основі проведеного дослідження встановлено дві головні мети перцептивного хешування

зображення: стійкість проти ненавмисних чи перцептивно незначних модифікацій зображення – перцептивна стійкість хешу; здатність протистояти навмисним атакам (спричинені зловмисним супротивником) – хеш безпека. Хеш властивості безпеки тісно пов'язані із схемою рандомізації, яку застосовують при створенні хеш алгоритму. Інше надзвичайно важливе питання, на яке потрібно знайти відповідь, це яка (мінімальна) довжина хешу потрібна, щоб успішно отримати потрібний рівень стійкості. Теоретичний аналіз алгоритмів рандомізованого медіа хешування, та кількісного відношення рандомізованого параметру(ів) з хеш безпекою, ще не розглядався в літературі.

Для підвищення ефективності обробки інформації в автоматизованих системах управління та обробки зображень виникає необхідність розробки методів надійного хешування та ідентифікації графічних зображень. Підвищення ефективності дозволить значно розширити область використання прикладного забезпечення у системах управління і обробки інформації.

Основна частина

В криптографії хеш функції використовуються для електронного підпису, щоб підтвердити відправку повідомлення, а також щоб отримувач міг перевірити його достовірність. Хеш функція «дуже» чутлива до зміни повідомлення, це виражається в тому, що зміна повідомлення m поверне інший бітовий рядок h [1]. В додатках, що включають цифрове створення водяних знаків та аутентифікацію електронних зображень, вимоги, на яких повинне відбуватися стиснення картинок, дещо різняться. Зміна значення одного пікселя не зробить зображення іншим чи ненадійним. Стиснення чи типова обробка зображення не змінюють візуальний вміст зображення. Важливим є механізм, який повертав би майже такий же бітовий рядок для усіх подібних зображень, в той же час, два зовсім різних зображення будуть видавати некорельовані рядки хешування. Це ми і називаємо функцією стійкого перцептуального хешування зображення. Необхідно отримати майже схожі бітові рядки для двох зображень, коли людина може сказати, що ці зображення однакові.

Хеш функція зображення $HK(I)$ бере зображення I і визначає короткий вектор $h = HK(I)$, який є в більшості випадковим значенням (індексованим у відповідності з секретним ключем K). Значення хеш функції повинне бути інваріантним до невеликих змін I, які перцептуально незначні, тоді як на введення різних значень хеш функцій вони повинні бути незалежними (і відповідно різними з високою ймовірністю). Така функція буде корисна для ідентифікації зображень в базі даних, можливе проведення різних змін з I (такі як стиснення та зміна формату, алгоритми загальної обробки сигналів, сканування чи створення водяних знаків). Якщо h двійкове, то можна використовувати стандартний пошук та методи сортування для додатків, які працюють з базою даних. Якщо розмір бази даних n, то в цьому випадку пошук скоріше визначався б як логарифм кроків від n. Ця задача значно ускладнюється, якщо необхідно витримати зловмисні атаки на I, які хотять перешкодити ідентифікації зображення.

Алгоритми стійкого хешування зображення можуть використовуватися в додатках захисту мультимедіа для створення водяних знаків та ідентифікації. З точки зору надійності використання одного і того ж ключа для багатьох зображень сприяє послабленню надійності, як наслідок, атакуючий може повернути єдиний секрет багатьох зображень, на яких створювалися водяні знаки одним ключем, так як кожне зображення може видати деяку інформацію про ключ. Можливо уникнути цієї проблеми, якщо замість використання для кожного I залежного ключа зображення $s = HK(I)$ (з K секретом) використовувати алгоритми стійкого хешування зображення. Якщо значення хеш функції при створенні водяних знаків інваріантне та здійснюються невеликі атаки, декодер може вирахувати *S,* якщо відоме *K*. Загалом, значення хеш функції може використовуватися як вказівники, які показують місце знаходження водяного знаку. Такий підхід також забезпечив би додаткову ефективність обчислення, коли розмір вхідного потоку, в якому створені водяні знаки, дуже великий. Ці проблеми були також обговорені в [2, 3].

Хеш функції важливі в різних криптографічних та пошукових додатках баз даних, в тих, що компілюють довгі двійкові рядки в короткі. Вимогами є рівномірний розподіл вихідних даних і парної незалежності (подана пара вихідних даних хеш функцій має бути незалежна одна від одної). Обмеження, що вивід хеш функції має бути інваріантним за невеликих перцепційно неважливих модифікацій (ненавмисних чи злонавмисних) вимагає розробки нових підходів. Два зображення «перцепційно однакові», якщо людське око не може розрізнити їх. Нехай X позначає специфічне зображення, а X' – змінену версію цього зображення, яке «перцепційно схоже на X у всіх практичних цілях». Нехай Y позначає зображення, яке «перцепційно несхоже» на X. Нехай L позначає кінцеву довжину хешування і нехай $HK(:)$ позначає хеш функцію, яка використовує секретний ключ K. Ми використовуємо нормалізовану відстань Хеммінга $D(:;:)$ для того, щоб порівняти два значення хеш функції, яка є відношенням звичайної відстані Хеммінга і розміром введення. Для того, щоб спростити задачу, ми пропонуємо розділити її на 2 стадії:

1. Обчислити проміжне значення хеш функції. В кінці першої стадії отримаємо значення хеш функції, яке має довжину M, і має наступні властивості розподілення:

$$\begin{aligned} D\left(H_K(X), H_K\left(X'\right)\right) < T_1 \\ D\left(H_K(X), H_K(Y)\right) > T_2 \end{aligned}, \quad (1)$$

де $0 < T_1 < T_2 < 0{,}5$.

2. Обчислити кінцеве значення хеш функції. Враховуючи проміжне хешування, необхідно отримати рандомізаційне решіткове векторне квантування, для того щоб отримати кінцеве значення хеш функції.

Для вирішення поставленої задачі пропонується два алгоритми: алгоритм *А* і алгоритм *Б*. Алгоритм *А* є детермінований і формує основу для першого та другого алгоритму, який використовує рандомізацію, щоб збільшити вивід ентропії та надійності. Задача розглядається як безповоротне стиснення, яке зменшує введення при збереженні сутності вхідного зображення, а також використовується дискретне перетворення Уолта [4], так як воно стисло фіксує характеристики зображення через час та частоту локалізації. Далі ми піднімаємо суттєві області за допомогою порогової класифікації. Щоб отримати надійність проти модифікацій, пропонується проста ітераційна методика фільтрації, яка зменшує наявність «геометрично слабких компонентів» і збільшує «геометрично сильні компоненти» за допомогою засобу росту області. Число потенційних меж більшості зображень досить велике, так як вивід заснований на геометричній структурі введеного зображення. Вивід запропонованої ітераційної системи фільтрації – стійка приваблива точка для області більш можливих малих модифікацій.

Розглянемо покроковий опис алгоритму *А*.

Алгоритм *А*.

1. Обчислити дискретне перетворення Уолта X до рівня L, де L – число рівнів дискретного перетворення Уолта. Нехай X' - результат піддіапазону прямого потоку.

2. Виконати операцію порогової обробки X_A, щоб отримати двійкове зображення M:

$$M(i,j) = \begin{cases} 1 \; if \;\; X_A(i,j) \geq T \\ 0 \;\; inakше \end{cases}, \tag{2}$$

T – вибраний таким чином, що $W(M) \approx q$, де $0 < q < 1$ параметр алгоритму, $W(M)$ – нормалізована вага Хеммінга.

3. Обчислити геометричний ріст області. $M1 = M$, $ctr = 1$.

3.1. Виконати порядково-статистичне фільтрування $M1$. $M2 = S[m;n]; p(M1)$, де m,n і p параметри алгоритму.

3.2.Провести двомірне інваріантне фільтрування $M3$ через фільтр f, де $M3\ (i;\ j) = AM2\ (i;\ j);\ f$ і A параметри алгоритму. Нехай вихідним параметром буде $M4$.

3.3.Виконати операцію порогової обробки $M4$. Нехай $M5$ вихідний параметр, так як $W(M5) \approx q$.

3.4.Якщо $ctr \geq C$, то закінчити ітерацію і перейти до кроку 4. Якщо це не так, знайти $D(M5;M1)$; якщо його значення менше T, то закінчити ітерацію та перейти до кроку 4; якщо ні, то $M1 = M5$, $ctr = ctr + 1$ і перейти до кроку 3.1.

4.$H\ (X) = M5$.

5. Кінець алгоритму.

Підхід розглянутий в алгоритмі *А,* є загальним, дозволяє використовувати різні зміни зображення, фіксує характеристики зображення і при цьому досягається надійність. Використання рандомізації (отриманої із секретного ключа) важливе не тільки для надійності та захисту проти атак, а також для масштабності. Як було зазначено раніше, мета полягає в тому, щоб отримати однорідне розповсюдження значень хешування і значень вхідних параметрів, які будуть попарно незалежні. Алгоритм *А* не використовує секретного ключа, тому ми використовуємо $H(:)$ замість $HK(:)$.

Розглянемо покрокове описання алгоритму *Б*. Введемо основні позначення. Нехай N буде кількістю прямокутників зображення; нехай R_i буде i-й прямокутник і нехай w_i і h_i будуть відповідно шириною і висотою R_i, де $i \in \{1,2,...,N\}$. Нехай X_1 буде підзображення, яке сформовано за допомогою частини X, що знаходиться в R_i, $i \leq N$.. Секретний ключ буде використовуватися як початок генератора випадкових чисел, який буде використатися для рандомізації всіх нижче зазначених кроків. Тепер переходимо до покрокового описання алгоритму *Б*.

Алгоритм *Б*.

1. Для кожного i випадковим чином знайти встановлений прямокутник R_i, таким чином щоб $w_s \leq w_i \leq w_l$ і $h_s \leq h_i \leq h_l$, де w_s, w_l, h_s, h_l параметри алгоритму.

2. Використати алгоритм *А* на всі X1; вихідними є $H(X_i), i \leq N$

3. Перетворити кожну матрицю $H(X_i)$ в одномірний вектор $\hat{H}_i$ в вибірковому порядку. Об'єднати $\{\hat{H}_i\}, i \leq N$, щоб отримати $\hat{H}$.

4. Виконати випадкове планування $\hat{H}$. Нехай M буде довжиною $\hat{H}$. Випадково вибрати $\{i_1, i_2, ..., i_M\} \subseteq \{1,2,..., M\}$. Обчислити $H_K(X) = \left[\hat{H}(i_1), ..., \hat{H}(i_M)\right]$. Якщо N достатньо велике і R_i також, то геометричні стійкості алгоритму *А* зберігаються для алгоритму *Б*.

5. Кінець алгоритму.

Подальшою перевагою використання алгоритмів *А* і *Б* є зменшення колізійної ймовірності і підвищення стійкості проти атак через рандомізацію, але за рахунок складності, як наслідок, алгоритм *А* використовується для кожного зображення індивідуально.

Висновки

Запропонований ітераційно-геометричний метод хешування зображення використовує перцепційно суттєві компоненти зображень через методи ітеративного фільтрування. Метод базується на емпірично проглянутих фактах, які, у випадку атак, виробляють перцепційно схожі зображення. Алгоритми рандомізаційної векторно-решітчастої квантизації можливо використовувати на проміжне хешування, щоб провести заключне хешування. Даний підхід буде корисним для ідентифікації зображень в базах даних, при якому можливе проведення різних змін з зображенням, таких як стиснення та зміна формату, алгоритми загальної обробки сигналів, сканування чи створення водяних знаків. Розроблено базову кластеризацію, що дає можливість кластерам не зазнавати жодних втрат. Для не згрупованих векторів, що залишились, було представлено два підходи, що полегшують баланси стійкості та слабкості.

Література

1. Бабаш А.В. Криптографические методы защиты информации : учебник для студ. вузов / А. В. Бабаш, Е. К. Баранова. – М. : КНОРУС, 2016. – 190 с.

2. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзинский. – М. : Юридическая литература, 2006. – 160 с.

3. Борисов М.А. Основы программно-аппаратной защиты информации : учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. – 4-е изд., перераб. и доп. – М. : ЛЕНАНД, 2016. – 416 с.

4. Нестеров С.А. Основы информационной безопасности : учебник / С. А. Нестеров. – СПб : Лань, 2017. – 423 с.

5. Шаньгин В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М. : ДМК Пресс, 2017. – 702 с.

6. Нетравалі А. Н. Цифрові зображення: Представлення і компрессія / А. Н. Нетравалі, Б.Г. Хаскель. – Нью-Йорк, 2002. – 430 с.

References

1. Babash A.V. Kriptograficheskie metody zashity informacii : uchebnik dlya stud. vuzov / A. V. Babash, E. K. Baranova. – M. : KNORUS, 2016. – 190 s.

2. Baturin Yu.M. Kompyuternaya prestupnost i kompyuternaya bezopasnost / Yu.M. Baturin, A.M. Zhodzinskij. – M. : Yuridicheskaya literatura, 2006. – 160 s.

3. Borisov M.A. Osnovy programmno-apparatnoj zashity informacii : ucheb. posobie dlya vuzov / M. A. Borisov, I. V. Zavodcev, I. V. Chizhov. – 4-e izd., pererab. i dop. – M. : LENAND, 2016. – 416 s.

4. Nesterov S.A. Osnovy informacionnoj bezopasnosti : uchebnik / S. A. Nesterov. – SPb : Lan, 2017. – 423 s.

5. Shangin V. F. Informacionnaya bezopasnost i zashita informacii / V.F. Shangin. – M. : DMK Press, 2017. – 702 s.

6. Netravali A. N. Tsyfrovi zobrazhennia: Predstavlennia i kompressiia / A. N. Netravali, B.H. Khaskel – Niu-York, 2002. – 430 s.

Рецензія/Peer review : 3.1.2020 р. Надрукована/Printed :14.2.2020 р.
Стаття рецензована редакційною колегією