Robust Image Hashing

Daniela Coltuc
University Politehnica Bucharest, Romania

INTRODUCTION

By robust image hashing (RIH), a digital image is transformed into a short binary string, of fixed length, called hash value, hash code or simply *hash*. Other terms used occasionally for the hash are digital signature, fingerprint, message digest or label. The hash is attached to the image, inserted by watermarking or transmitted by side channels. The hash is robust to image low distortion, fragile to image tempering and have low collision probability.

The main applications of RIH are in image copyright protection, content authentication and database indexing. The goal of copyright protections is to prevent possible illegal usage of digital images by identifying the image even when its pixels are distorted by small tempering or by common manipulation (transmission, lossy compression etc.). In such cases, the image is still identifiable by the hash, which is robust to low distortions (Khelifi & Jiang, 2010). The content authentication is today, one of the main issues in digital image security. The image content can be easily modified by using commercial image software. A common example is the object insertion or removal. Although visually undetectable, such modifications are put into evidence by the hash, which is fragile to image tempering (Zhao & al., 2013). Finally, in large databases management, the RIH can be an effective solution for image efficient retrieval, by replacing the manual annotation with the hash, which is automated extracted (Lin & al., 2001). The properties that recommend the hash for indexing are the low collision probability and the content-based features.

The origins of the hash lay in computer science, where one of the earliest applications was the efficient search of large tables. Here, the hash – calculated by a hash function – serves as index for the data recorded in the table. Since, in general, such functions map more data strings to the same hash, the hash designates in fact a bucket of records, helping to narrow the search. Although very efficient in table searching, these hashes are not appropriate for file authentication, where the low collision probability is of high concern. The use in authentication applications has led to the development of the cryptographic hashing, a branch including hash functions with the following special properties: preimage resistance (by knowing the hash it is very difficult to find out the file that generated it), second image resistance (given a file, it is very difficult to find another with the same hash) and collision resistance (it is very difficult to find two files with the same hash). They allow the hash to withstand the cryptanalytic attacks.

The development of multimedia applications in the last two decades has brought central stage the digital images. The indexing or authentication of these data has been a new challenge for hashing because of a property that might be called *perceptible identity*. It could be defined as follows: although the image pixels undergo slight modification during ordinary operations, the image is perceived as being the same. The perceptual similar images must have similar hashes. The hashing complying with this demand is called robust or perceptual. Specific methods have had to be developed in order to obtain hashes tolerant to distortions, inherent to image conventional handling like archiving, scaling, rotation, cropping, noise filtering, print-and-scan etc., called in one word non malicious attacks. These methods are grouped under the generic name of RIH.

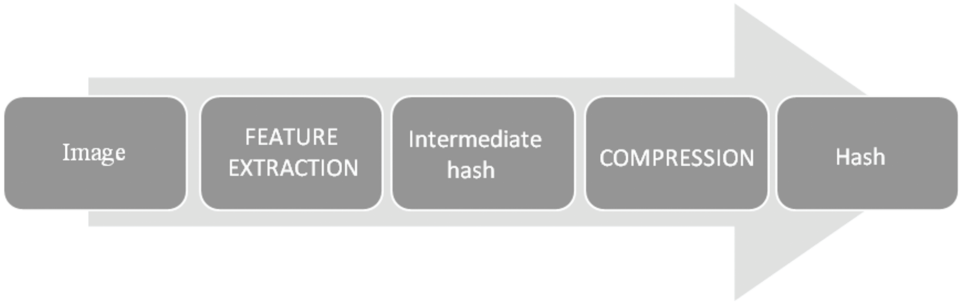
In this article, we define the main terms used in RIH and discuss the solutions commonly used for designing a RIH scheme. The presentation will be done in the light of robust hash inherent properties: randomness, independence and robustness.

BACKGROUND

The hash calculation follows the two steps scheme in Figure 1, consisting in feature extraction and compression. At the end of the first step, the image is reduced

DOI: 10.4018/978-1-4666-5888-2.ch592

Figure 1. RIH general scheme



at a *feature vector* called *intermediate hash*. The intermediate hash is transformed into a robust hash by quantization, binarization and compression. In RIH, the term compression is used purely to designate a significant reduction in the dimensionality of the feature vector. The techniques for obtaining compression in RIH are different from those used in traditional image compression, where the processing chain is quasi reversible in order to allow also the image decompression. In RIH, the reversibility is not necessary.

The following particular concerns guide the design of a RIH scheme: the hash must be short, robust and fragile, and with low collision probability. The shortness is imposed by the fact that the hash must be attached, inserted by watermarking or transmitted on side channels. In all these cases, there are capacity limitations. The robustness is the hash property to remain unchanged or almost, when the image undergoes slight modifications caused by non malicious attacks. The robustness must be doubled by fragility, which is the hash capability to change when the image content is forged. The collision defines the situation when, for two perceptually different images, a same hash is obtained. Since the hashes are very short, the collision probability can be significant if there is redundancy inside or among hashes.

The shortness, the robustness/fragility and the low collision probability represent a must in any RIH application. In authentication, there is a supplementary task: image securing by involving a secret key in the process of hashing.

Mathematically, these demands are resumed by the following three hash properties (Mıhçak & Venkatesan, 2001):

1. **Randomness:**

$$P[\mathcal{H}(I)] \approx \frac{1}{2^n} \tag{1}$$

where P denotes the probability, I the image, $\mathcal{H}(I)$ the hash and n the hash bitlength. From the point of view of Shannon's Information Theory, the equation (1) is the condition for maximum entropy memoryless sources.

2. **Pairwise independence:**

$$P[\mathcal{H}(I) = a \mid \mathcal{H}(I_{diff}) = b] \approx P[\mathcal{H}(I) = a] \tag{2}$$

where I and I_{diff} denote two perceptually different images. The Equations (1) and (2) define the condition of minimum collision probability.

3. **Robustness:**

$$P[\mathcal{H}(I) = \mathcal{H}(I_{sim})] \approx 1 \tag{3}$$

where I and I_{sim} denote the image before and after a non malicious attack.

The properties (1-3) distinguish the hash from the common signatures used in image recognition. The robustness and fragility are obtained by selecting appropriate image features, while the minimum collision probability results from their processing. In the next, we present the main solutions for generating image hashes with these properties.