The Development of Perceptual Image Hashing

*Xiu Anna **Li Kun ***Kim Hyoung-Joong
Seoul Graduate School of Information Security
*19840317xiu@korea.ac.kr

Abstract

In this paper, we show that methods of perceptual image hashing which have been proposed recent years. And the disadvantages of them. Perceptual robustness, security and fragility are properties what we always discuss. Then we propose some ideas which we will do the research later.

1. Introduction

With the development of Internet and multimedia technology, the amount of image information that is conveyed, broadcast or browsed vis digital devices has grown dramatically. Simultaneously, digital forgery and unauthorized use have reached a significant level that makes digital image security very challenging and demanding.

Based on human visual system, perceptual image hash was been presented. In general an ideal perceptual image hash should habe the following desirable properties.

Perceptual robustness: The hash function should map visually identical images to the same hash even if their digital representations are not exactly the same.

Security: To avoid the forgery, the security of image hashing requires that the hash values as well as the secret key should be difficult to guess.

Fragility: In order to distinguish perceptually different images, the fragility of image to be as large as possible.

Nowadays, perceptual image hash towards a joint signal-cryptographic approach since the traditional cryptography hash functions (such as MD5) can not satisfy the requirements of multimedia content authentication. Because the cryptographic hash is sensitive to every single bit of input. Robustness and uniqueness of media hashing are two desired aspects.

It can be appled for audio or video authentication, audio watermarking or video watermarking, and image database or website indexing.

Perceptual image hash can be stepped two stages simply. the first stage is feature extraction, the second stage is hash generation, see Figure 1.

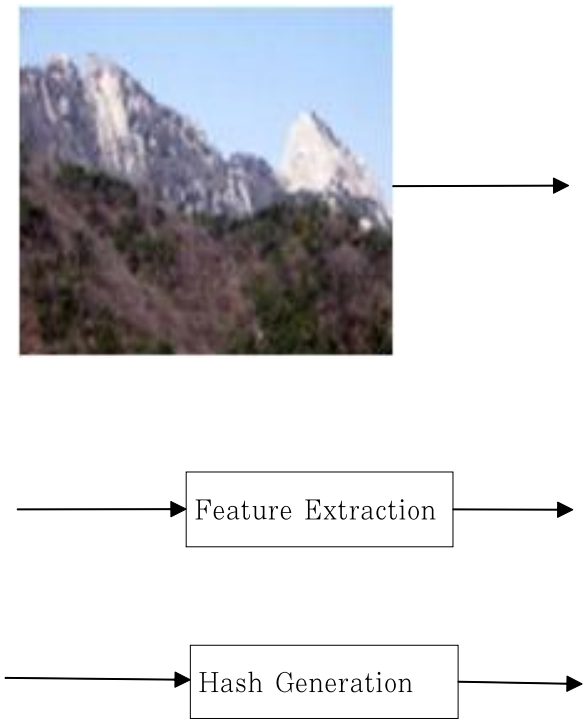

Figure 1: Two stages of image hashing

2. Hashing Algorithms

In order to achieve robust image authentication tolerant to legitimate image manipulations, the so-called perceptual image hashing schemes were proposed so that images with perceptually insignificant differences will still result in similar hashes, and therefore, will be treated as authenticated. To this end, Monga and

Evans designed a perceptual image hashing scheme through extracting significant geometry-preserving feature points and applying probabilistic quantization[1].

In [2], a clustering algorithm was employed to generate the hash vector based on a pre-determined intermediate hash vector.

Aiming at providing a perceptual image hashing scheme with better performance against geometric attack, Monga and Mihcak proposed to conduct two rounds of non-negative matrix factorization (NMF) to some randomly selected overlapping blocks, and generate the hash vector by applying random projection on the concatenation of columns and rows of the two resulting matrices from NMF [3].

More recently, Khelifi and Jiang designed a perceptual image hashing scheme based on virtual watermark detection [4]. For every image to be hashed, its high frequency content will be extracted to form the feature vector, which will be treated as possibly watermarked sequence.

3. Discusses

In [2], a clustering approach has been proposed as a trade-off between the perceptual robustness to attacks and the fragility to visual dissimilarities across distinct images. However, the major drawback of this approach is the requirement of intermediate hashes to be clustered in an optimized way. Such a requirement limites the application of image hashing to specific areas such as registration and retrieval where the number of images in the database is known a priori.

In [3], the use of one single independent key to generate various hashes could make it estimable by observing a number of hashes extracted from different images, and renders hashing techniques vulnerable to malicious manipulation. the secret key used to secure NMF-based hashing can be disclosed.

In [4], under the known-hash attack where the opponent has access to several pairs of images and their corresponding hash vectors, estimating the virtual watermark sequences serving as the secret key can be formulated as a simple convex optimization problem, and can be solved efficiently.

4. Conclusions

In this paper, we show the popular image hashing schemes recently. But all of them are not perfect in security property. We are doing the research to find one scheme which is satisfy the three properties of perceptual image hashing.

What we will do is that using prewitt filter to construct the image hashing algorithm.

References

〔1〕 V. Monga and B. L. Evans, Perceptual Image Hashing via Feature Points: Performance Evaluation and Tradeoffs, IEEE TIP, vol. 15, pp. 3452-3465, 2006.
〔2〕 V. Monga, et. al. A Clustering based Approach to Perceptual Image Hashing, IEEE TIFS, vol. 1, pp. 68-79,2006.
〔3〕 F. Khelifi and J.M. Jiang, Perceptual Image Hashing Based on Virtual Watermark Dectection, IEEE TIP, vol. 19, pp. 981-994, 2010.
〔4〕 A. Menezes, et. al., Handbook of Applied Cryptography, CRC Press, 1996.