A New Method for Robust and Secure Image Hash Improved FJLT

Anna Xiu*, Hyoung Joong Kim*

Abstract

There are some image hash methods, in the paper four image hash methods have been compared: FJLT (Fast Johnson- Lindenstrauss Transform), SVD (Singular Value Decomposition), NMF (Non-Negative Matrix Factorization), FP (Feature Point). From the compared result, FJLT method can't be used in the online. the search time is very slow because of the KNN algorithm. So FJLT method has been improved in the paper.

Keywords: image hash, robustness, improved FJLT, FJLT, SVD, NMF, FP.

I. INTRODUCTION

Mapping an image to a short binary string, it is known as image hashing. In particular, a perceptual image hash function should have the property that the two images look the same to the human eye map to the same hash value, even if the images have different digital representations (e.g., being separated by a large distance in mean squared error)[4]. An image hash function by splitting it into two stages. In the first step, a feature vector, which should capture the important perceptual aspects of the image, is extracted. In the second step, the feature vector is securely compressed. Secure compression by first adding a dither sequence to the feature vector and then compressing the result with a distributed source code. The mutual information between the image and the hash value goes to zero if the dither is drawn, which are content-based compact representation of an image[10] For example, image hash based on Fast Johnson-Lindenstrauss transform (FJLT), dimension reduction based techniques singular value decomposition (SVD), non-negative matrix factorization (NMF), Feature Point (FP).

In general, an ideal image hash should have 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. Visually similar images without significant differences may have hashes with a small distance[3].
- Uniqueness, or anti-collision capability: Probability of two different images having an identical hash value, or very close hash values, should tend to zero[3]
- Sensitivity to visual distinction: Perceptually important changes to an image should lead to a completely different hash. This feature is essential for the image hashing to be useful in image authen- tication and digital forensics[3]
- Key- dependence: The hash must be generated under the control of a secret key or several keys. It should be extremely difficult to estimate the hash without a key[3] The requirement is considered for the security, the security here is mean that it's not easy to forge the original image.

Image hash using feature Points (FP) use hash algorithms [6] to get the image's feature points, then, compare the original image's FP with the others. The method for image hashing has limited utility as it has poor robustness properties.

Non-Negative Matrix (NMF) is distinguished from traditional matrix approximation methods, such as QR and SVD, with its use of non-negativity constraints. These constraints lead to a parts-based representation because they allow only additive, not subtractive, combinations. This is in contrast to SVD which learns holistic and not parts-based representations. An immediate consequence of this property with respect to

접수일자 : 2009년 8월 14일
최종완료 : 2009년 8월 14일

*Korea University Multimedia Security Lab
교신저자, E-mail :khj-@korea.ac.kr

hashing is far less misclassification (perceptually distinct images mapping to the same hash value) when NMF as opposed to SVD is employed for dimensionality reduction. The NMF-based hash possesses excellent robustness under a large class of perceptually insignificant attacks while significantly reducing collision probability for hash values obtained from perceptually distinct images by the experiments[4].

Hashing scheme based on dimension reduction were developed, singular value decomposition (SVD) using low-rank matrix approximations obtained via singular value decomposition for hashing was explored in [5]. It's robustness against geometric attacks motivates other solutions in this direction.

A new robust and secure image hash algorithm based on Fast Johnson-Lindenstrauss transform is coming. It Also use the proposed dimension reduction technique. FJLT hashing provides robustness to various manipulations according to the experimental result. But in [1], they use classifier K-nearest neighbors (KNN) to solve the classification problem about that the distance of hash vectors between the original images and the manipulated images. KNN is the unsupervised learning of machine learning, it cost much time to learning and then set the train samples database, get the train labels, and then use the test samples, which are the Euclidean distance of hash vectors between the original images and geometric deformations images.

II. THE ROBUSTNESS HASH PRONCIPLE

1. ast Johnson-Lindenstrauss Transform (FJLT)

FJLT is a random embedding $\Phi = FJLT(n,d,\varepsilon)$ that can be obtained as a product of three real valued matrices: [1]

$$\Phi = PHD \qquad (1)$$

The matrices P and D are random and H is deterministic. [7]

- P is a k-by-d matrix whose elements { P_{ij} } are drawn independentlu according to the following distribution, where $N(0,q$) $^{-1}$ means a Normal distribution with zero-mean and variance q^{-1},

$$\begin{cases} P_{ij} \sim \ N(o,q^{-1}) & \text{with probability q} \\ P_{ij} = 0 & \text{with probability 1-q} \end{cases}$$

Where

$$q = \min\{\frac{c\log^2 n}{d},1\},$$

For a large enough constant C. [1]

- H is a d-by-d normalized Hadamard matrix with the elements as:

$$H_{ij} = d^{\frac{1}{2}}(-1)^{<i-1,j-1>},$$

where <i, j> is the dot-product of the m-bit vectors i, j expressed in binary.[1]

- D is a d-by-d diagonal matrix, where each diagonal element D_{ii} is drawn independently from {1, 1} with probability 0.5. [1]

Therefore, $\Phi = FJLT(n,d,\varepsilon)$ is a k-by-d matrix, where is the original dimension number of data and k is a lower dimension number set to be $c'\varepsilon^{-2}\log n$. Here n is the number of data points, ε is the distortion rate, and c' is a constant.[1] The subimage is actually a point.

2. The Histogram Shape Invariance

The histogram of a gray-level image IH matrix of size k×N with bins of the width M may be described

$$H_M = \{h_M(i) | i = 1,\dots,L\}.$$

Where $h_M(i) \geq 0$ denotes the number of pixels in the i^{th} bin and satisfies

$$\sum_{i=1}^{L} h_M(i) = K * N$$

Suppose that the bit depth of an image is P bits, the relation between the number of the bins L and the bin width M is formulated as

$$\begin{cases} L = 2^P/M & \text{if } \operatorname{mod}(2^P/M) = 0 \\ L = \lfloor 2^P/M \rfloor & \text{ohters} \end{cases}$$

where $h_M(i)$ includes those pixels between (I - 1) ×M and I × M - 1. [2]

The FJLT and histogram algorithms have been explained.. Finally, the key-dependent hash is obtained by randomly permuting the resultant binary sequence.

II. IMAGE HASH VIA FJLT

Given an image, the proposed hashing algorithm consists of three steps: random sampling, dimension reduction by FJLT [1], and compute the histogram.

1. Random Sampling

Color images have to be converted to gray images, a few subimages as original feature by random sampling depending on the key then are selected , which number is N. Each subimage is marked to $S_i \in R^2$, for $1 \leq i \leq N$. Each S_i is a $m^2 \times 1$ vector by concatenating the column of corresponding subimage.

$Feature = \{S_1, S_2, \ldots, S_N\}$ with $m^2 \times N$ (2)

The advantage of forming such a feature is that the global information in the Feature matrix and local information in each component S_i can be captured. Even if some portions of the original image are lost.

2. Dimension Reduction by FJLT

FJLT can capture the essential feature of the original data in low dimension.

$IH = \Phi(Feature) = PHD \times Feature$ with k×N (3)

3. Compute the Histogram

Based on the analysis of 2. , the histogram can be computed

III. EXPERIMENT AND RESULT

The hamming distance has been verified to be an effective discrimination standard to measure the performance of the hash function [8]. For a pair of image hashes, the Hamming distance between them is

$$d(hash_1, hash_2) = \frac{1}{C_L^2} \sum_{k=1}^{C_L^2} \left| hash_1(k) - hash_2(k) \right|$$

so, the Hamming distance is used to find the similar images of the original images in the improved FJLT hash method.

In the experiment, for each color image with size 512 ×512, we generate 50 similar attacked versions . The seven manipulations and attaches considered are: additive Gaussian noise, additive Uniform noise, Gaussian blurring, JPEG Compression, rotation, cropping, and scaling. The details of the corresponding parameters are listed in Table1.

Table 1. The parameters for manipulated images

Manipulation	parameters
Gaussian Noise (8)	5%, 10%, 15%, 20%, 25%, 30%, 35%, 40%
Uniform Noise(8)	5%, 10%, 15%, 20%, 25%, 30%, 35%, 40%
Gaussian Blurring(8)	0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4
JPEG Compression(8)	QF ={ 1,3,5,7,9,10,11,12}
Rotation(7)	5°,10°, 15°, 20°, 25°, 30°, 45°
Cropping(6)	5%,10%,20%,30%,35%, 40%
Scaling(5)	25%,50%,75%,150%,175%

We use the five image hash methods to compute the hashes of the 50 manipulated images and original images, then we get the result as follow

Table 2. Compare 5 methods for robustness

Manipulation	Accuracy Rate(%)				
	NMF	SVD	FP	FJLT	*FJLT
Gaussian Noise	100	100	99	100	100
Uniform Noise	100	100	98	100	100
Gaussian Blurring	100	100	99	100	100
JPEJ Compression	96	100	99	100	100
Rotation*	89	90	0	45	46
Cropping	99	99	0	100	100
Scaling	97	97	0	85	85

***FJLT is the improved FJLT**
Rotation*, when the rotation is less than25°,all the 5 methods can get good results.

From Table 2, we can see the FJLT and improved FJLT hash can both get the similar good result, but let's have a look at the time, which the five method cost.

Table 3. Compare the implement time

5 methods	NMF	SVD	FP	FJLT*	FJLT*
Compared time(s)	3.8015	2.4844	64.6406	90.3593	2.4983

From the Table 3, we can get the result that the improved FJLT method is more faster than FJLT method.

From the experiment result, we can get the result: The improved FJLT hash method is better than the FJLT hash method, because they both have good robustness, but the improved one costs less time to get the result, finds the similar images.

FJLT image hash method use classifier K-nearest neighbors (KNN) to solve the classification problem about that the distance of hash vectors between the original images and the manipulated images. KNN is the unsupervised learning of machine learning, it cost much time to learning. And it can't be used in the website. But the improved FJLT can save the searching time, and can be used for our daily life. For example , search some similar images from the website, after we give the website the original image.

IV .Reference

[1] Xudong Lv, Z. Jane Wang, "Fast Johnson-lindenstrauss Transform for Robust and Secure Image Hashing", *MMSP 2008*, pp. 725-729.

[2] Shijun Xiang, Hyoung-Joong Kim, Jiwu Huang, "Histogram-Based Image Hashing Scheme Robust Against Geometric Deformations", pp. 121-128, MM&Sec'07, September 20-21, 2007, Dallas, Texas, USA.

[3] Zhenjun Tang, Shouzhong Wang, Xinpeng Zhang, Weimin Wei, and Shengjun Su, "Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization", *Journal of Ubiquitous Convergence and Technology*, vol 2, no.1, pp. 18-26, MAY 2008.

[4] Vishal Monga, M.Kivanc Mihcak, "Robust and Secure Image hashing via Non-Negative Matrix Factorizations", *IEEE Transactions of Information Forensics and Security*, vol .2, no. 3, pp.376-390, Sep.2007.

[5] Suleyman S. Kozat, Ramarathnam Venkatesan, M.Kivanc Mihcak, "Robust Perceptual Image Hashing via Matrix Invariants", *2004 International Conference on Image Processing (ICIP)*, pp. 3443-3446.

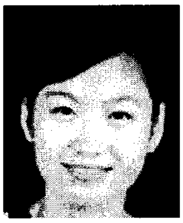
[6] Vishal Monga and Brian L. Evans, "Robust Ferceotual Image Hashing using Featrre Points", *2004 International Conference on Imge Processing(ICIP)*, pp. 677-680.

[7] N. Ailon and B. Chazelle, "Approximate nearest neighbors and the fast Johnson-Lindenstrauss transform", *in Proceedings of the 38th Annual Symposium on the Theory if Computing (STOC)*, pp. 557-563, Seattle WA, 2006.

[8] A. Swaminathan, Y. Mao, and M. Wu. "Image hashing resilient to geometric and filtering operations", *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp.215-230, 2006.

[9] R. Venkatesan, S. W. Koon, M. H. Jakubowski, and P. Moulin. "Robust Image Hashing", *in IEEE International Conference Image Processing*, pp. 664-666, Vancouver, BC, Canada, Sep. 2000.

[10] Mark Johnson, http://www.eecs.berkeley.edu/~mjohnson/ abstracts /hashing.htm



Anna Xiu, B.E. in Electrical Engineering and Automation , Qingdao University of Technology, Qindao, China. 2004-2008, and she is currently pursuing M.S. and PhD in Information Management and Security Lab, Korea University, Korea. Her research interests focus on Image Hash, Image Process, and Security.

Hyoung Joong Kim,received the B.S. degree in Electrical Engineering from Seoul National University, Korea (ROK), in 1978. Healso received M.S., and PHD in Control and Instrumentation Engineering from Seoul National University, Korea (ROK) in 1986, and in 1989 respectively. Currently he is a full professor in the Graduate School of Information Management and Security, Korea University, Korea (ROK). His research interests Multimedia Computing, Multimedia Security, Semantic Analysis, and e-learning applications.