Content Based Image Hashing Using Companding and Gray Code

Lei Yang
Department of Electrical and
Computer Engineering
University of Florida
Gainesville, Florida, 32611
Email: {leiyang}@ufl.edu

Qian Chen
University of Florida
Gainesville, Florida, 32611
Email: {qiantrue}@ufl.edu

Jun Tian
Futurewei Technologies Inc.
Hazlet, NJ, 07730
Email: jtian@huawei.com

Dapeng Wu
University of Florida
Gainesville, Florida, 32611
Telephone: (352) 392–4954
Fax: (352) 392–0044
Email: wu@ece.ufl.edu

Abstract

Easily processing, storing and propagating of digital images demand efficient and automatic techniques to identify and verify image contents. Image hashing is such a promising technique to represent and authenticate images without changing the content of images. The new robust image feature we use is the Morlet wavelet coefficients at feature points with the k-largest local total variations in images. The Morlet wavelet coefficients are pseudo randomly permutated such that image hashes have a small collision rate and are difficult to analyze by attackers. The Morlet wavelet coefficients are further quantized using companding technique and binarily coded using Gray code to form the final hash. Experimental results show the effectiveness and robustness of our method. The proposed image hash could have applications in image authentication and video signature.

Index Terms

Image hashing, image authentication, video signature, companding, Gray code, Morlet wavelet.

I. Introduction

Digital images are in an exponential increase due to proliferation of digital cameras and image applications. The huge number of digital images requires efficient classification and retrieval of images [1]. Digital images facilitate multimedia processing, and at the mean time, make fabricating and copying of digital contents easy. To protect the copyright of the images, efficient and automatic techniques are needed to identify and verify the content of digital multimedia. Besides the long-time established copy right protection tool — image watermarking [2], image hashing emerges as an effective tool to represent images and automatically identify whether the query image is a fabrication or a copy of the original one.

As an alternative to image watermarking, image hashing can be applied to many applications previously accomplished by watermarking, such as copyright protection, image authentication. It can also be used for image indexing and retrieval as well as video signature. Unlike watermarking, image hashing need not change the image by inserting watermarks into the image. Image hash is a short binary string, mapped from an image by an image hash function. The image hash function has such a property that perceptually identical images should have the same or similar hash values with high probability, while perceptually different images should have quite different hash values. In addition, the hash function should be secure, so that an attacker cannot predict the hash value of a known image.

Many techniques for image hashing have been proposed in the literature. These algorithms are typically based on statistics [3], relations [4], low-level image features [5], [6], non-negative matrix factorizations [7], and so on. Fridrich and Goljan [8] proposed a robust visual hashing method. Their hash digests of digital images are created by projections of DCT coefficients to zero-mean random smooth patterns, generated using a secrete key. Roy *et al.* [9] proposed content-hashing, which consists consists of a compact representation of some image features. The resulting image hash is robust to image filtering, but surrenders to geometric attacks and may not be collision free. The image hash based on Scale Invariant Feature Transform(SIFT) algorithm [10] and compressive sensing technique [11] could solve geometric attacks in certain degree, but it is computationally expensive. Lin and Chang [4] created the mutual relationship of pairwise block DCT coefficients to distinguish JPEG compression from malicious modifications. But the block based method is unreliable, since possible shifting and cropping operations may change hash values. Venkatesan *et al.* [3] proposed an image hashing technique. Their hashes are generated from statistical features extracted from random tiling of wavelet coefficients. However, it only allows limited resistance to geometric distortions, and is susceptible to some manipulations, such as luminance change and object insertion.

To address these problems, we propose content based image hashing using companding and Gray code. Content based image hashing is more robust to content preserving image processing like geometric and illuminance attacks, and more sensitive to malicious content tampering attacks than statistics based image hashing. Our method combines robust feature point detector and robust content singularity descriptor at these feature points. The feature points are chosen from cross points of lines, with the k-largest local total variations [12] in images. The local total variations are determined by the structure of images, and robust to geometric attacks and luminance attacks. Therefore, it will obtain stable similar feature points in perceptual identical images and is resistant to content-preserving attacks. Morlet wavelet [13] is good at describing the singularity of signals. The Morlet wavelet coefficients at feature points are obtained to represent images. The Morlet wavelet coefficients are pseudo randomly permuted with a secrete key, which enhances the security of the image hashing system. Morlet wavelet coefficients are computationally efficiently quantized using companding technique according to the probability distribution of the coefficients. Thus, the proposed image hashing is robust to contrast changing and gamma correction of images. Gray code is used to binarily code the quantized coefficients, which increases discriminability of image hashes.

The rest of the paper is organized as following. In Section II, we present an overview of the proposed image hashing system. In Section III, we describe how to extract the robust feature of images, which is the Morlet wavelet coefficients at feature points with the k-largest local total variations. Then the Morlet wavelet coefficients are quantized and binarily coded with Gray code as shown in Section IV. Section V shows the experimental results that demonstrate the effectiveness and robustness of the proposed image hashing system. Finally, we conclude our paper in Section VI.

II. System Overview

Image hashes should have small collision probability, and high discriminability. From two input images I and $I^{'}$, a image hashing system ϕ extracts two corresponding binary hashes h and h' using a secrete key K as shown in Equation (1). The distance function such as normalized Hamming distance is denoted by $d(\cdot,\cdot)$, and discriminative thresholds are denoted by ζ_1 and ζ_2.

$$\begin{cases} h = \phi(I, K) \\ h^{'} = \phi(I^{'}, K) \end{cases} \tag{1}$$

For the design of image hashing system, three objectives should be considered.

1) $\forall I, I^{'}$, if $I \neq I^{'}$ then $d(h, h^{'}) \geq \zeta_1$;
2) $\forall I, I^{'}$, if $I = I^{'}$ then $d(h, h^{'}) < \zeta_2$;
3) $\forall I$, $P(h(i) = 1) = P(h(i) = 0) = 0.5$,
   where $h(i)$ is the i-th element of hash h, $P(h(i) = j)$ is the probability of $h(i) = j$, (j = 0 or 1).

The first objective indicates that distances between different images should be larger than a threshold ζ_1, which guarantees that the discriminability of image hashing system. The second objective implies that the distances between similar images should be smaller than a threshold ζ_2, where $\zeta_2 \leq \zeta_1$, which ensures the robustness of image hashing under intentional or unintentional attacks. For similar images, it is expected that the image hash is able to discriminate images under intentional and unintentional attacks using a threshold for image authentication purpose. The third objective provides the unpredictability of image hashes whose binary values are distributed with equal probability.

Our proposed image hashing system is shown in Fig. 1. First, feature points in images are extracted. The feature points are expected to be similar for similar images, such that distances between hashes of similar images are small and that image hashes are robust against perceptually preserving attacks. We extract feature points with the k-largest local total variations, which capture the structure of images. Second, we obtain the Morlet wavelet coefficients at feature points to describe the degree of singularity at feature points. Third, pseudo random permutation of the Morlet wavelet coefficients with a secrete key increases the security and reduces the collision probability of image hashes. Forth, the coefficients are quantized with companding technique and binarily coded with Gray code to form the final image hashes. Inverse Error Correction Coding to compress image hashes is optional in our system.

III. Robust Descriptor of Images

Most information of signals is conveyed by irregular structures and transient phenomena of signals. Feature points such as corners are salient content descriptors of images. There are three stages to extract the robust descriptor of images in our proposed method.

- Image preprocessing;
- Finding the locations of feature points;
- Evaluating the singularity of image signals at feature points by continuous wavelet transform.

A. Preprocessing

Preprocessing will change image pixels and may influence the detection and description of feature points. We try to avoid any changes to images and extract the original information from images. Therefore, the only preprocessing in our method is resizing images into the same size to facilitate later algorithm steps.

B. Feature Point Extraction

For different applications and corresponding performance requirements, different techniques to extract feature points are explored in the literature [14]. Since image hashes should be invariant to content-preserving processing, robust repeatable feature point detectors with small computations are desired. Jaroslav *et al.* [15] proposed a **f**eature **p**oint detector in **b**lurred images, which we call BFP in the paper. BFP can yield high repetition rate on differently distorted images. We will propose a more robust feature point detector based on BFP. BFP is to efficiently detect points which belong to two edges regardless their orientations. It selects points with the k-largest local variances. The local variance (LV) is defined on the image block in Equation (2).

$$LV = \sum_{X \in \Omega} (I(X) - \bar{I}_{\Omega})^2 \tag{2}$$

where Ω is the image block centered at a feature point, X is a vector representing the pixel coordinates, $I(X)$ is the pixel value, $\bar{I}_{\Omega}$ is the mean of the pixel values in the block. LV depends on pixel values, thus, is easily changed by any image processing.

Therefore, we propose to select feature points with the k-largest local total variations (LTV) [12]. LTV is defined as:

$$LTV = \sum_{X \in \Omega} |I^{'}(X)|^2 \tag{3}$$

where Ω is the image block centered at the current feature point, $I^{'}(X)$ is the gradient of pixel values at coordinate $X = (x_1, x_2)$

$$|I^{'}(X)| = \sqrt{(\frac{\partial I(X)}{\partial x_1})^2 + (\frac{\partial I(X)}{\partial x_2})^2} \tag{4}$$

LTV depends on local structure in images. It is robust against content-preserving image processing.

Therefore, our modified feature point extraction algorithm is more robust than BFP. We use this method to determine the coordinates of the most salient feature points with the k-largest local total variations in images, as shown in Fig 2.

Feature points are extracted in the high repetition rate. Coordinates of feature points are not invariant to the geometric transforms of images, but the singularity of feature points is invariant to the geometric transforms of images. Therefore, after locating the most salient feature points in images, we use Morlet wavelet to evaluate the degree of singularity at the feature points.

C. Feature Point Description

Harmonic analysis [16] of signals can detect and locate the singularity of signals. Wavelet bases have good localization ability in both time and frequency domain. Therefore, they can locate and characterize the singularity of signals very well. The local singularity of functions is measured by Lipschitz exponent mathematically. A function $f(x)$ is with singularity of Lipschitz α, at point x_0, if and only if there exists a constant A such that all the points x in a neighborhood of x_0 satisfy $|f(x) - f(x_0)| \leq A|x - x_0|^{\alpha}$. The wavelet coefficients $Wf(s, x_0)$ of $f(x)$ at x_0 and scale s has relation with Lipschitz exponents α shown in Equation (5).

$$|Wf(s, x_0)| \leq A_{\epsilon} s^{\alpha} \tag{5}$$

where A_{ϵ} is a constant.

Continuous wavelet transform [17] is designed to detect the singularity of signals better than discrete wavelet transform. The locations of singularity found by continuous wavelet transform [13] may be influenced by the noise in images. False positive may happen at points which are not at corners but close to straight lines. False negative may happen at points which are at corners but with small variation of gray levels. But the degree of singularity is less influenced. Therefore, based on robustly extracted feature points, we calculate the continuous wavelet coefficients row-by-row and column-by-column, and use the magnitudes of the coefficients to represent feature points.

Morlet wavelet is a continuous wavelet with single frequency and Sine modulated Gaussian function. Morlet wavelet is used to detect linear structures perpendicular to the orientation of the wavelet. 2D Morlet wavelet is defined as

$$\varphi_M(X) = (e^{iK_0X} - e^{-1/2|K_0|^2})e^{-1/2|X|^2} \tag{6}$$

where $X = (x_1, x_2)$ is the 2D spatial coordinates, and $K_0 = (k_1, k_2)$ is the wave-vector of the mother wavelet, which determines the scale-resolving power and angular resolving power of the wavelet.

Because the directions of the strongest responses of Morlet wavelet filter at feature points may be perturbed by noise. Only horizontal and vertical directions of Morlet wavelet are considered. Although the magnitudes of Morlet wavelet coefficients in horizontal and vertical directions will be slightly perturbed by a small degree of rotation of images, it will be normalized in the later quantization step.

IV. Hash Generation

After extracting salient feature in images, we will further generate the binary hash sequences from the obtained Morlet wavelet coefficients in this section.

A. Pseudo Random Permutation of Morlet Wavelet Coefficients

To enhance the security of image hashes, i.e., to avoid the forgery inputs designed by an adversary resulting in the same hashes, we use a secrete key K to pseudo randomly permute the Morlet wavelet coefficients. The random permutation can also decrease the collision probability for different inputs by using different secrete keys.

B. Quantization Using Companding

Quantization using companding is efficient and unbiased for coefficients with different probability. Quantization can obtain discrete representation of image hash, normalize the range of output hash, as well as weight different parts of hashes with different values. Vector quantization with Lloyd-Max algorithm is classical, but is dependent on the initial configuration and computationally expensive. Therefore, we propose to use companding technique [18] to quantize the float-point Morlet wavelet coefficients to finite level binaries. The algorithm of companding for discrete values is similar to the algorithm of histogram equalization. The computational complexity of the algorithm is $O(n)$, where n is the number of coefficients. Quantization using companding technique assumes that the shape of distribution of Morlet wavelet coefficients of similar images are similar which is in line with the fact. It is a kind of probabilistic quantization. It tries to be fair to every coefficients, i.e., coefficient values with large probability will be quantized with small stepsizes, while coefficient values with small probability will be quantized with large stepsizes. A compandor consists of a compressor, a uniform quantizer, and an expandor. The compressor is a nonlinear transformation and designed to convert the distribution into the uniform distribution. The expandor is an inverse of the compressor, which is used for recovery of original coefficients and thus disregarded in our image hashing system. Using the companding technique, we quantize the data into L levels. The coefficient probability of each level is the same, i.e., $\frac{1}{L}$. L should be 2^m ($m \in Z^+$) for easy binarization of coefficients.

C. Binary Coding Using Gray Code

We propose to use Gray code [19] to code the quantized coefficients. Gray code, also known as the reflection binary code, is a binary code, in which two successive values differ in only one bit. Thus the hamming distance between two successive values is one, and the hamming distance between any two nonsuccessive values is proportional to their difference. However, it does not hold for ordinary binary code. In this way, the distances between similar images decrease and those between dissimilar images increase. This helps increase the discriminant capability of the system. Since the length of a hash is 5 in our experiments, a 32 byte array is used as a lookup table for constructing hash with Gray Code. For arbitrary length, Gray code may be constructed recursively.

V. Experimental Results

In our experiments, the image block Ω is 15x15 to calculate LTV; 40 points with largest LTVs are chosen as feature points; the quantization level L is 32, i.e. 2^5; the length of image hash N is 200.

The distances between different hashes are evaluated by the normalized Hamming distance.

$$d(h, h') = \frac{1}{N} \sum_{i=1}^{n} \delta(h(i), h'(i)) \tag{7}$$

where

$$\delta(h(i), h'(i)) = \begin{cases} 1, & h(i) = h'(i) \\ 0, & h(i) \neq h'(i) \end{cases} \tag{8}$$

h and h' are two hash vectors, their the ith values are denoted as $h(i)$ and $h'(i)$, and N is the length of an image hash.

These parameters could be tuned for better performance in specific applications.

A. The Robustness of Feature Point Detector

The robustness of proposed feature point detector is shown in Fig. 2. The image ‘Lena’ is tampered, rotated, contrast enhanced with histogram equalization as shown in Fig. 2(b) (c) (d), respectively. In Fig. 2, the extracted feature points are denoted by red ‘o’. The feature points extracted from the original image, the tampered image, the rotated image and the image after histogram equalization are almost the same. It indicates high correct detection rate of the proposed feature point detector. Hence, the proposed feature point detector is robust against tampering, rotation and histogram equalization.

B. Parameter Determination of Singularity Descriptor

Besides the elegance of Morlet wavelet, the reason why we use Morlet wavelet is due to its strong discriminability in the proposed image hashing system, which we will show in this subsection.

The optimal scale of Morlet wavelet is determined by using 24 frames of two shots in the video sequence *big_buck_bunny _480p_h264.mov* [20]. Each shot has 12 frames. The reference image randomly selected is the 7th frame in the first shot. The 7th frame and the 17th frame among 24 frames are shown in Fig. 3. The frames in the first shot are similar to Fig. 3(a), and the frames in the second shot are similar to Fig. 3(b).

From Fig. 4, we can see that the distance between the 7th frame and the reference image, i.e., itself, is 0. The distances between similar frames in the same shot are much smaller than the distances between different frames in different shots.

Fig. 4(a) compares the discriminability of image hashes with Morlet wavelet at different scales. The gaps between the average distances of the first shot and the average distances of the second shot are 0.2342, 0.2704, 0.2628, 0.2645 at scale 6, 8, 10, 12, respectively. The largest gap 0.2704 at scale 8 indicates that the strongest discriminability of Morlet wavelet at scale 8 for video signals. Fig. 4(b) compares the discriminability of image hashes with different wavelets at scale 8. The gaps between the average distances of the first shot and the average distances of the second shot are 0.2704, 0.2335, 0.2083, 0.2582 for Morlet wavelet, Spline wavelet, Haar wavelet, Symmetric wavelet respectively. Morlet wavelet has the strongest discriminability.

C. Discriminability and Robustness of Image Hashes

We also test the robustness of proposed image hashing system on natural images under various attacks. The six test images are 512x512 gray images shown in Fig. 5.

1) Discriminability between Different Images: The normalized Hamming distances of six test images are shown in Table I. They are relatively large. It indicates that the discriminability of the proposed image hashing system is good.

2) Non-predictability of Image Hashes: A desirable property of an image hash function is that the distance between the hash of an image and any random sequence with the same length is large. If this property is achieved, it is unlikely for an attacker to generate an imposter of the hash of an image by using a random sequence.

We evaluate the distance between an image hash and a random binary sequence. We generate 50 different random sequences; each random sequence is a binary random vector with probability $p(0) = p(1) = 0.5$ and has the same length as the image hash. The normalized Hamming distances between the hash of Lena and the 50 different random sequences are illustrated in Fig. 6. The distances are relatively large and constant, which implies the non-predictability of image hashes.

3) Robustness to Content-preserving Attacks: We make the following types of attacks on these images: scaling images to 0.5 and 1.5 of their sizes, compressing images using JPEG with quality factor 50 [21], rotating images by 5 degrees, cropping 20% of images, adding white Gaussian noise (variance $\sigma^2 = 20$) to images, filtering images with Gaussian and Median filters. The normalized Hamming distances between the attacked images and the original test images are listed in Table II. The hash distances are small under these content-preserving image processing, showing the robustness of the proposed image hashing system.

4) Robustness to Tampering: We make several tampered versions of image 'Lena' as shown in Fig. 7. The tampered areas are indicated by red rectangles. The normalized Hamming distances between the hash of Lena and those of the tampered Lena are shown in Table III. The normalized Hamming distances between the hash of Lena and those of the tampered Lena are larger than the normalized Hamming distances between the hash of Lena and those of the content-preserving processed Lena, and are smaller than the normalized Hamming distances between the hashes of different images. Thus, the proposed image hashing system has the ability to identify tampering.

5) Discriminative Thresholds: Based on the experiments above, the discriminative thresholds in our system are determined as $\zeta_1 = \zeta_2 = 0.26$. With the thresholds, the false positive and false negative rate on the test images are both 0.

VI. Conclusions

In this paper, we proposed a new method to generate robust image hashes. The feature points are extracted from images with the k-largest local total variations. Morlet wavelet coefficients are calculated at the feature points. They are pseudo random permutated, quantized with companding technique and binarily coded with Gray code. The generated image hashes are robust to content-preserving image processing. The normalized Hamming distances between the hashes of Lena and those of the tampered Lena are larger than the normalized Hamming distances between the hash of Lena and those of the content-preserving processed Lena, and are smaller than the normalized Hamming distances between the hashes of different images. Our future research will be exploring its applications on image authentication and video signature, since our proposed image hash has good discriminability between different images and different video shots, and strong ability to recognize similar images.

REFERENCES

[1] R. Datta, D. Joshi, J. Li, and J. Wang, "Image retrieval: Ideas, influences, and trends of the new age," *ACM Computing Surveys (CSUR)*, vol. 40, no. 2, pp. 1–60, 2008.

[2] P. Wong and N. Memon, "Secret and public key image watermarking schemes for imageauthentication and ownership verification," *IEEE Transactions on Image processing*, vol. 10, no. 10, pp. 1593–1601, 2001.

[3] R. Venkatesan, S. Koon, M. Jakubowski, and P. Moulin, "Robust image hashing," in *Image Processing, 2000. Proceedings. 2000 International Conference on*, vol. 3, 2000.

[4] C. Lin and S. Chang, "A robust image authentication method distinguishing JPEGcompression from malicious manipulation," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 2, pp. 153–168, 2001.

[5] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*, vol. 1, 1998.

[6] V. Monga and B. Evans, "Perceptual image hashing via feature points: performance evaluation and tradeoffs," *IEEE Transactions on Image Processing*, vol. 15, no. 11, pp. 3452–3465, 2006.

[7] V. Monga and M. Mihcak, "Robust image hashing via non-negative matrix factorizations," in *2006 IEEE International Conference on Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings*, vol. 2, 2006.

[8] J. Fridrich, "Visual hash for oblivious watermarking," in *PROC SPIE INT SOC OPT ENG*, vol. 3971, 2000, pp. 286–294.

[9] S. Roy and Q. Sun, "Robust hash for detecting and localizing image tampering," in *IEEE International Conference on Image Processing, 2007. ICIP 2007*, vol. 6, 2007.

[10] X. Di Wu, "A Self-Synchronized Image Hash Algorithm," in *2010 International Conference on Communications and Mobile Computing*. IEEE, 2010, pp. 13–15.

[11] M. Tagliasacchi, G. Valenzise, and S. Tubaro, "Hash-based identification of sparse image tampering," *IEEE Transactions on Image Processing*, vol. 18, no. 11, pp. 2491–2504, 2009.

[12] G. Aubert and P. Kornprobst, "Mathematical problems in image processing," 2006.

[13] S. Bhattacharjee and P. Vandergheynst, "End-stopped wavelets for detecting low-level features," in *Proceedings of SPIE*, vol. 3813, 1999, p. 732.

[14] T. Tuytelaars and K. Mikolajczyk, "Local invariant feature detectors: A survey." *Foundations and Trends in Computer Graphics and Vision*, vol. 3, no. 3, pp. 177–280, 2007. [Online]. Available: http://dblp.uni-trier.de/db/journals/ftcgv/ftcgv3.html#TuytelaarsM07

[15] J. Kautsky, B. Zitová, J. Flusser, and G. Peters, "Feature point detection in blurred images," in *IVCNZ*, 1998, pp. 103–108.

[16] Y. Katznelson, *An introduction to harmonic analysis*. Cambridge Univ Pr, 2004.

[17] S. Mallat and W. Hwang, "Singularity detection and processing with wavelets," *IEEE transactions on information theory*, vol. 38, no. 2 Part 2, pp. 617–643, 1992.

[18] R. M. Gray and D. L. Neuhoff, "Quantization," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2325–2383, 1998.

[19] C. Savage, "A survey of combinatorial Gray codes," *SIAM review*, vol. 39, no. 4, pp. 605–629, 1997.

[20] http://www.bigbuckbunny.org.

[21] T. Recommendation, "Information technology - digital compression and coding of continuous-tone still images - requirments and guidelines," in *Recommendation T.81*, 1993.

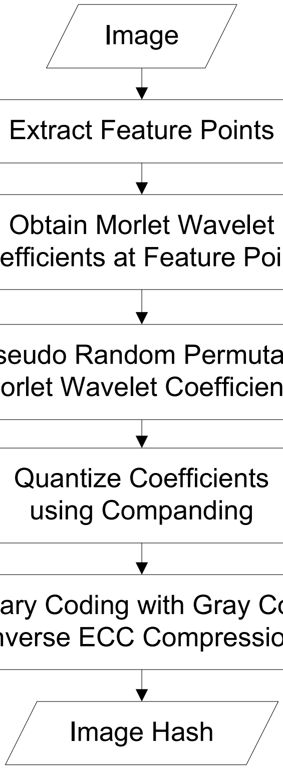


Image
Extract Feature Points
Obtain Morlet Wavelet Coefficients at Feature Points
Pseudo Random Permutate Morlet Wavelet Coefficients
Quantize Coefficients using Companding
Binary Coding with Gray Code (Inverse ECC Compression)
Image Hash

Fig. 1. Flow chart of image hash generation.

TABLE I
HAMMING DISTANCE BETWEEN DIFFERENT TEST IMAGES.

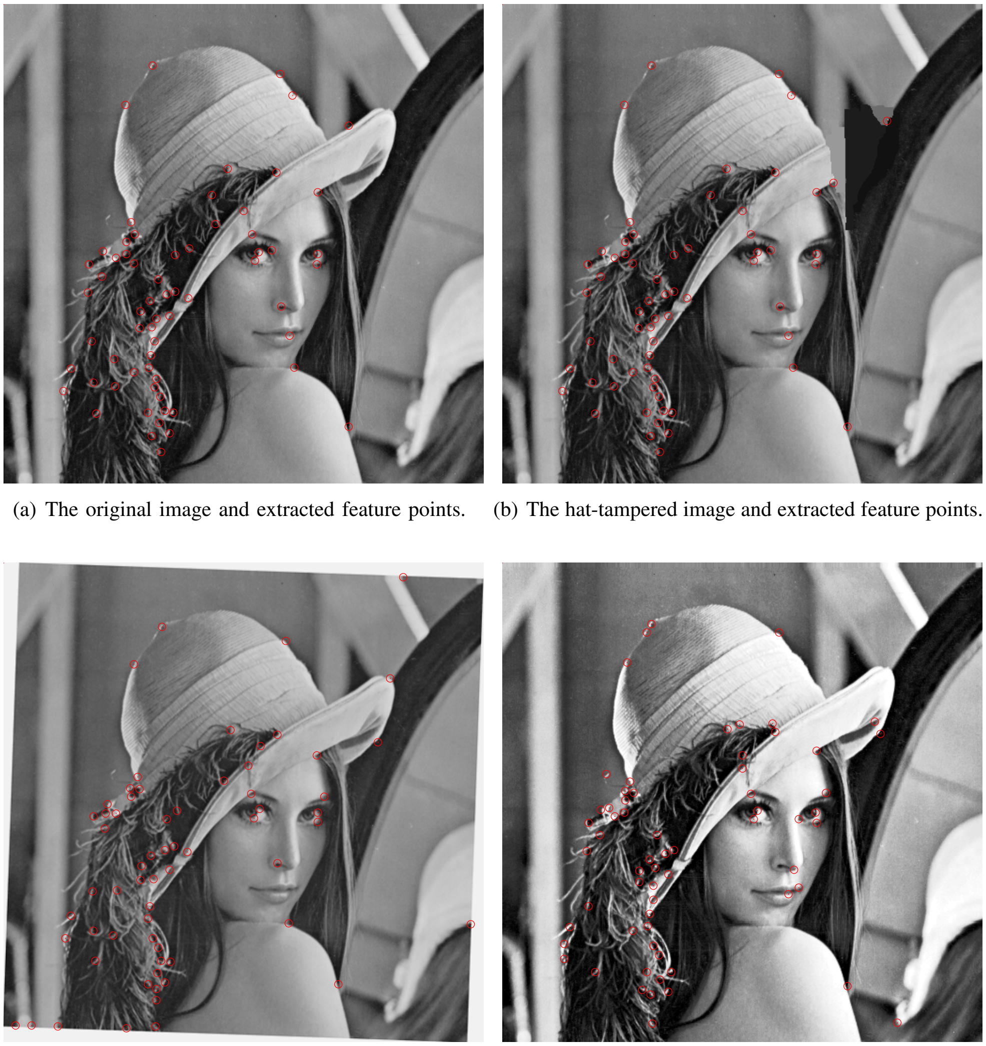
	(Lena, Barbara)	(Lena, Boat)	(Lena, Mandrill)	(Lena, Jet)	(Lena, Pepper)
Distance	0.44	0.39	0.42	0.35	0.39
	(Barbara,Boat)	(Barbara,Mandrill)	(Barbara,Jet)	(Barbara,Pepper)	(Boat,Mandrill)
Distance	0.39	0.48	0.41	0.39	0.41
	(Boat,Jet)	(Boat,Pepper)	(Mandrill,Jet)	(Mandrill,Pepper)	(Jet,Pepper)
Distance	0.37	0.37	0.41	0.40	0.36

TABLE II
HAMMING DISTANCE BETWEEN ATTACKED IMAGES AND TEST IMAGES.

Attacks	Lena	Barbara	Boat	Mandrill	Jet	Pepper
Scale 0.5	0.05	0.03	0.25	0.08	0.25	0.03
Scale 1.5	0.03	0.03	0.05	0.08	0.05	0.03
JPEG 50	0.05	0.30	0.15	0.03	0.03	0.03
Rotate 5^o	0.03	0.34	0.25	0.03	0.23	0.17
Crop 20%	0.03	0.33	0.25	0.08	0.25	0.25
AWGN σ^2=20	0.03	0.12	0.03	0.03	0.04	0.03
Gaussian Filtering	0.12	0.03	0.03	0.12	0.06	0.06
Median Filtering	0.06	0.12	0.25	0.12	0.03	0.15

TABLE III
HAMMING DISTANCE BETWEEN LENA AND ITS TAMPERED VERSION.

	(Lena, Tamper 1)	(Lena, Tamper 2)	(Lena, Tamper 3)
Distance	0.28	0.32	0.33
	(Lena, Tamper 4)	(Lena, Tamper 5)	(Lena, Tamper 6)
Distance	0.26	0.35	0.29



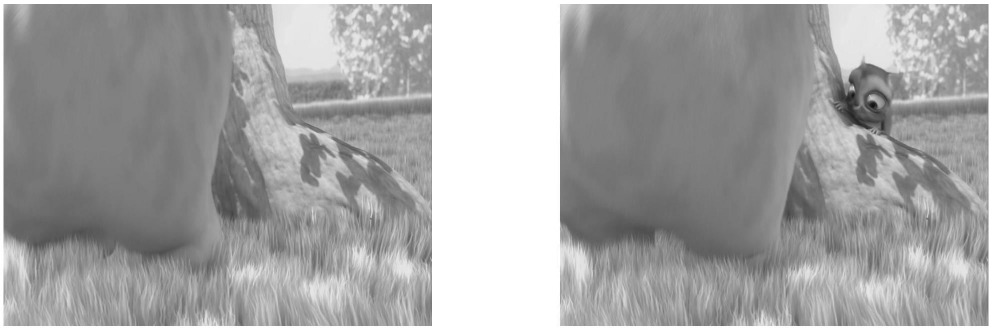
(a) The original image and extracted feature points.

(b) The hat-tampered image and extracted feature points.

(c) The rotated image and extracted feature points.

(d) The image after histogram equalization and extracted feature points.

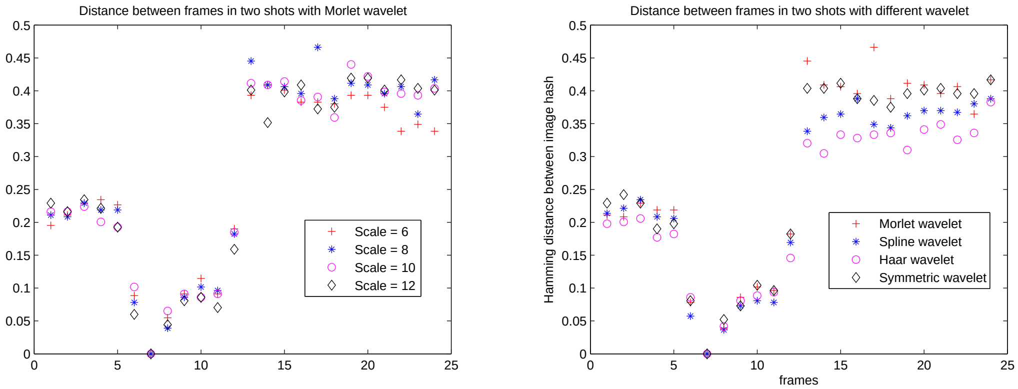
Fig. 2. The stable feature point detector.



(a) The 7th frame.

(b) The 17th frame.

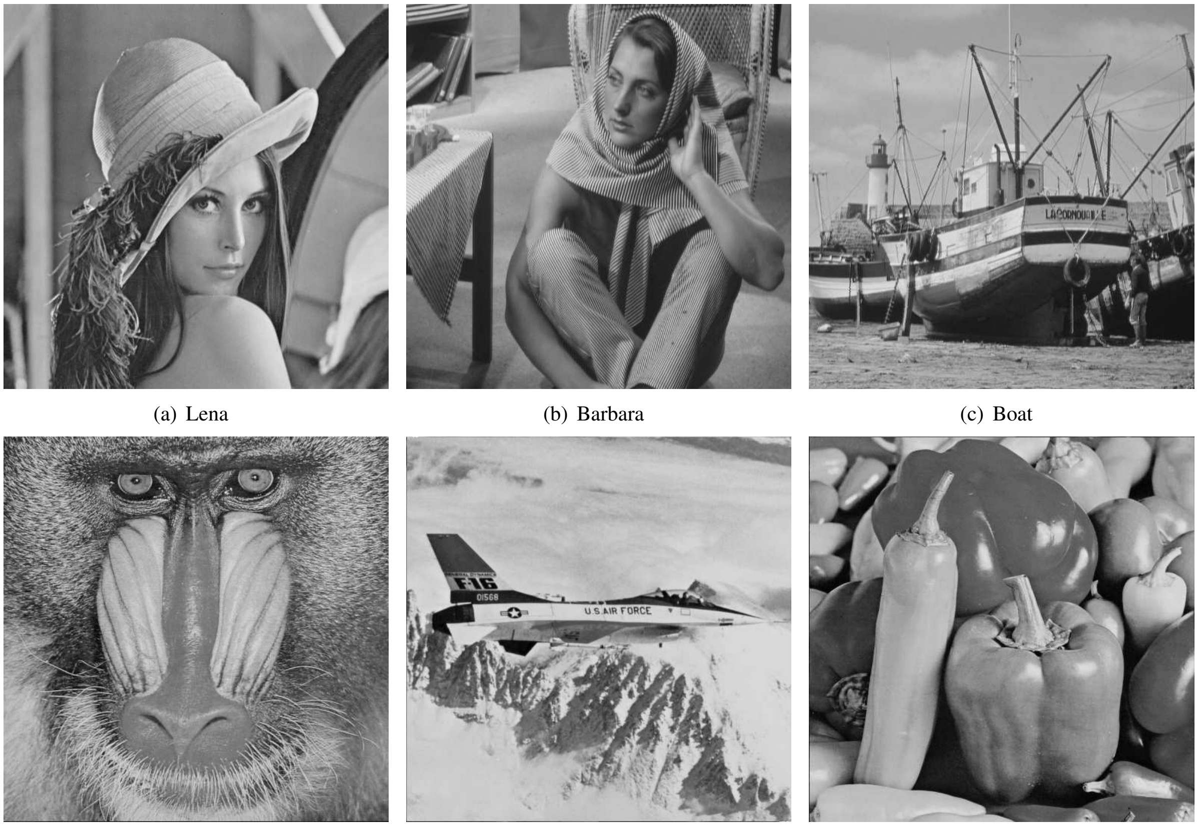
Fig. 3. The 7th frame and the 17th frame in the test video frames BUNNY.



(a) Hash distance with Morlet wavelet at different scales.

(b) Hash distance with different wavelets at scale 8.

Fig. 4. Hash distance with different wavelets at different scales.



(a) Lena

(b) Barbara

(c) Boat

(d) Mandrill

(e) Jet

(f) Pepper

Fig. 5. Six test images for image hashing.

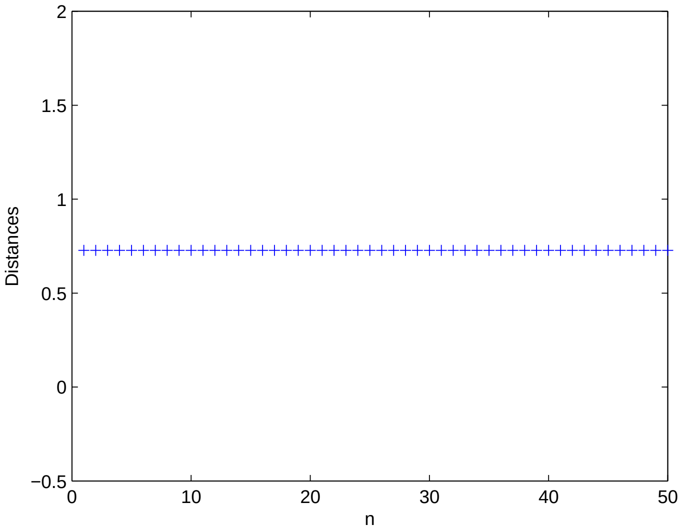
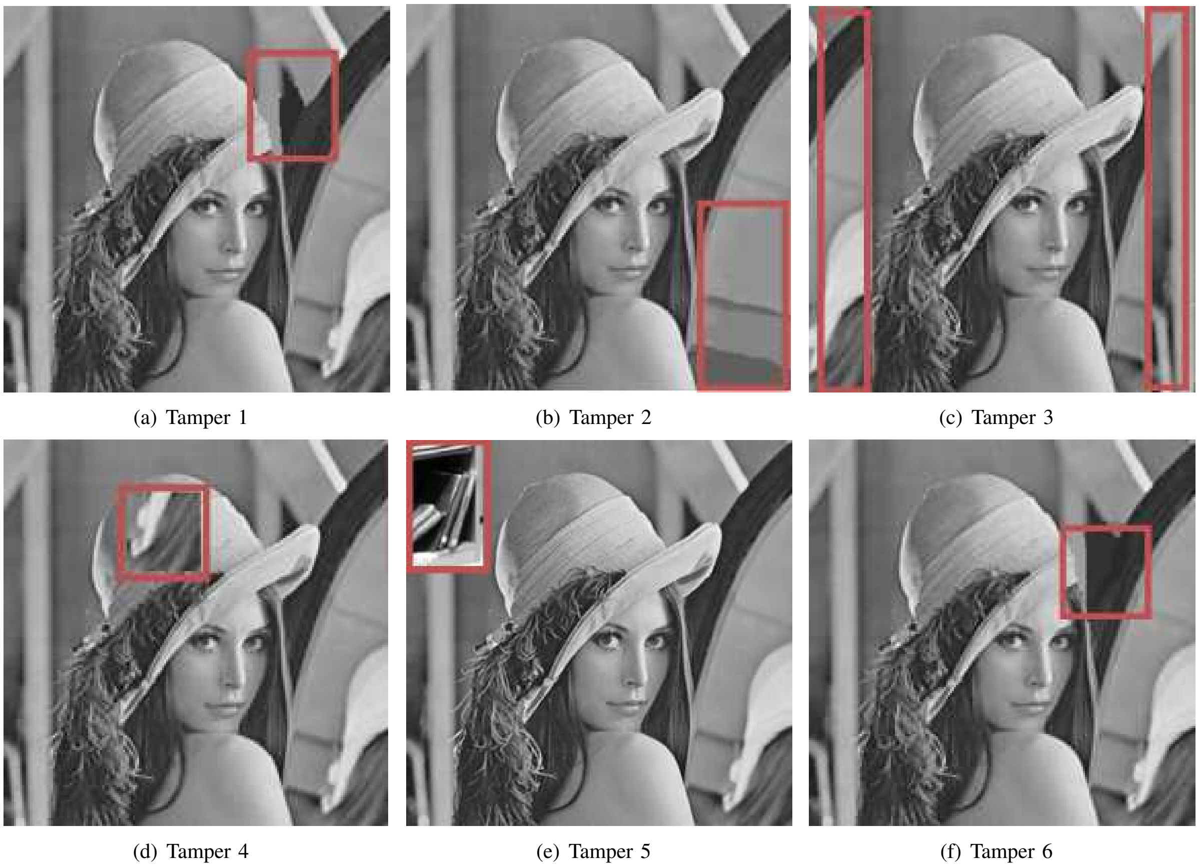


Fig. 6. Distance between the hash of Lena and the n-th random sequence ($n = 1, 2, \cdots, 50$).



(a) Tamper 1

(b) Tamper 2

(c) Tamper 3

(d) Tamper 4

(e) Tamper 5

(f) Tamper 6

Fig. 7. Six tampered images of Lena.