IEICE TRANS. INF. & SYST., VOL.E93–D, NO.5 MAY 2010

INVITED PAPER *Special Section on Information and Communication System Security*

A Survey on Image Hashing for Image Authentication

Yang OU[†], ***Nonmember and*** **Kyung Hyune RHEE**[††a)], ***Member***

SUMMARY The traditional cryptographic hash functions are sensitive to even one-bit difference of the input message. While multimedia data always undergo compression or other signal processing operations, which lead to the unsuitability of multimedia authentication using cryptographic hash. The image hashing has emerged recently which captures visual essentials for robust image authentication. In this paper, we give a comprehensive survey of image hashing. We present an overview of various image hashing schemes and discuss their advantages and limitations in terms of security, robustness, and discrimination under different types of operations on the image.

key words: *image hashing, image authentication, feature extraction, perceptibility*

1. Introduction

With the spreading use of multimedia information, security of media contents has become an important concern by attracting large research attentions. Multimedia authentication techniques have emerged to verify content integrity and prevent forgery. Traditional data integrity issues are addressed by cryptographic hash functions (e.g. MD5, SHA-1) or message authentication code, which are very sensitive to every bit of the input message. However, the multimedia data, such as digital images, always undergo various acceptable manipulations such as compression, image enhancement or other common signal processing operations. The sensitivity of traditional hash functions could not satisfy these perceptual insignificant changes. Nowadays, image hashing, which takes into account changes in the visual domain, is emerging rapidly [1], [2].

Similar as traditional cryptographic hash functions, an image hash is a compact representation used to verify the integrity of image content. The randomness should be introduced in the hash value by using a secret key, in order to ensure that an unauthorized user cannot forge a valid hash of the image without the key. Different from traditional hash, an image hash captures the essential perceptual attributes of the image. An ideal image hash function should be tolerant enough to visually acceptable manipulations, rather than bit-by-bit comparisons, whereas the discrimination to the visual content changes should be also ensured.

Due to the particularity of image hashing functions, a wide application scenarios are found currently, among which the main application is content-based authentication. A key dependent image hashing function can ensure the content integrity and source authentication of an image. Besides, the applications in digital watermarking, content-based image retrieval, and image matching are also promoted. Note that the robust hash values are not only generated from images, but also from other multimedia formats, such as audio hashing [3], [4] and video hashing [5], [6]. While we focus on the image hashing since it is the most widely researched with the longest developing history.

There are many other academic terms used for image hashing in literature: robust hashing, perceptual hashing, perceptual image hashing, robust image hashing, robust perceptual hash, soft hash, etc. We use the term "image hashing" in a broad sense to include all the foregoing technologies. Moreover, regarding to the two popular changes on image content, visually acceptable manipulations and visual content changes, the terms "Content Preserving Operations (CPOs)" and "Content Changing Operations (CCOs)" are used in our paper for the sake of simplicity. While some other denominations are: perceptual insignificant attacks and perceptual significant attacks, incidental distortions and intentional distortions, content preserving modifications and malicious tampering, etc.

A number of proposals for image hashing have been put forward to data. The approaches differ significantly in their application field, their levels of security, the functionalities they provide and their robust and discriminative capabilities. In this paper, our aim is to give a comprehensive survey of the existing approaches. For this purpose, we firstly present different categories for the classification of image hashing schemes. We systematically describe, discuss, evaluate, and compare the various techniques, especially with respect to their robustness and discrimination, concerning their security, and regarding the research trends in the future.

In Sect. 2 a general framework of image hashing is given. Section 3 discusses the evaluation criteria for image hashing schemes, especially for the security evaluation. The representative schemes are classified and discussed in Sect. 4, followed by comprehensive comparisons. In Sect. 5, several open issues are discussed. Finally, Sect. 6 concludes this paper.

Manuscript received October 31, 2009.

[†]The author is with the Department of Information Security, Pukyong National University, Republic of Korea.

[††]The author is with the Division of Electronic, Computer & Telecommunication Engineering, Pukyong National University, Republic of Korea.

a) E-mail: khrhee@pknu.ac.kr

DOI: 10.1587/transinf.E93.D.1020

2. General Framework of Image Hashing

Generally, an image hash is constructed through three main procedures as shown in Fig. 1: preprocessing, feature extraction and postprocessing. While the pre- and postprocessing are not mandatory but necessary to get a more robust hash value. The randomness can be cooperated into one of the three steps by using a secret key.

The preprocessing aims to decrease the sensitivity of feature extraction against minor distortions on an image, such as noises, lossy compression or transcoding. The common preprocessing operations include image downsampling [7], low-pass filtering for reducing high frequency signals [8], resizing for image rescaling, order statistic filtering for denoising [9], and Gaussian blurring [10]. As such, all above operations serve for the next essential attributes extraction stage.

Achieving the robustness against content preserving operations is the fundamental goal of image hashing. The robustness is largely relies on the essential features extracted from an image. The features selected should be tolerant to content preserving distortions, while the discriminative capability to content changing operations or other different images should be also provided at the same time. Hence, the feature extraction stage is significantly important in order to achieve robustness, discrimination and security. Some of the robust feature extraction methods exploited in literature include image histogram [10], feature points [11] or image edge information, significant DWT or DCT coefficients, Fourier transform [8], and dimensionality reduction with linear transforms [12].

On the other hand, since most feature extraction methods are publicly known, one can forgery an image hash easily from a different image or maliciously create another image to cheat the authentication systems. Therefore, key-based randomization should be incorporated into feature extraction to make the hash unpredictable and resist these threats. Another merit of randomization stated in [12] is in enhancing the scalability of the hash algorithm, i.e., the ability to work with large data sets while avoiding the collision for distinct inputs. This step also ensures source authentication of image data. The randomization approaches can be achieved via random pattern projection, image random blocking, and random weighted sum of feature parameters.

The feature vector extracted after the second stage is an intermediate hash, which still contains some redundancy and sensitivity. The postprocessing stage concerns about quantization, compaction and binarization of features. The clustering techniques [1], [13], decoding step of a proper Error Correcting Code (ECC) [9] have been exploited for compacting an intermediate hash. Furthermore, a key-based permutation can be applied to hash vectors for randomization [10]. However, the security is not as strong as in previous feature extraction stage, also the accuracy will be varied with the changes of key inserting [12]. The binary representation of hash vectors is expected to use Gray Code [14] in order to avoid the bit error caused by natural binary code.

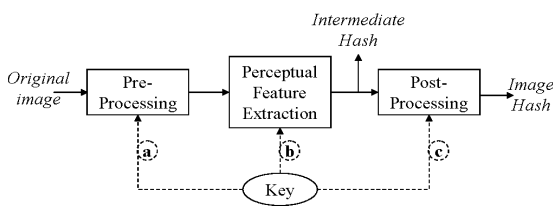


Fig. 1 The general framework of image hashing.

3. Evaluation Criteria for Image Hashing

3.1 Requirements of Image Hashing

An image hash should capture the essential attributes of the image so that insignificant changes to the human eyes will not substantially alter the hash value. The following notations are used to describe the requirements of image hashing:

- X: the input image;
- X_s: a similar version of X distorted under CPOs;
- X_d: a different version of X tampered under CCOs;
- k: a key involved in image hash generation;
- $\psi(\cdot)$: an image hash function;
- $P(\cdot)$: a certain probability;
- θ_1, θ_2: two given parameters where $\theta_1, \theta_2 \in (0, 1)$;
- τ: a given threshold.

Generally, a good image hash should satisfy the following requirements which have been given in [1], [11], [15]:

(1) Randomization (Unpredictability):

$$P(\psi(X, k) = h) \approx \frac{1}{2^q}, \forall\, h \in \{0, 1\}^q$$

where q is the length of the binary hash sequence. This property indicates that with a secret key k varying in an available range, the image hash value should be approximately uniformly distributed among all possible q-bit outputs.

(2) Robustness against CPOs:

$$P(\| \psi(X, k) - \psi(X_s, k) \| < \tau) \geq 1 - \theta_1$$

for a given θ_1 and predefined τ. X_s is a perceptually similar or identical image of X. The hash value of X_s should be close to the hash of X by using same k.

(3) Discrimination to CCOs:

$$P(\| \psi(X, k) - \psi(X_d, k) \| > \tau) \geq 1 - \theta_2$$

for a given θ_2 and predefined τ. X_d is a perceptually different image from X. This property implicates that a good image hash function should be discriminative to perceptual different images.

(4) Onewayness:
Given the hash value h and hash function $\psi(X, k)$, it is difficult or impossible to get information related to original X.
(5) Compactness:
On the premise of satisfying the above properties, the hash sequence should be as short as possible to save on storage space.

3.2 Measurement Metrics

The metrics reviewed in this subsection are mainly applied to evaluate the robustness and discriminative capability which are the fundamental properties of image hashing.

Euclidean Distance (ED). Given two image hash vectors, $\boldsymbol{h} = (h_1, h_2, \ldots, h_n)$ and $\boldsymbol{h}' = (h'_1, h'_2, \ldots, h'_n)$, $\boldsymbol{h}$ is the hash value of original image, while $\boldsymbol{h}'$ is the hash of a modified version or a totally different image. The Euclidean distance between them is defined as:

$$ED(\boldsymbol{h}, \boldsymbol{h}') = \sqrt{\sum_{i=1}^{n}(h_i - h'_i)^2}$$

The Euclidean distance (2-norm distance) is suitable for non-binary hash vectors such as float or integer arithmetic numbers. The lower the Euclidean distance is, the closer the two hash values. In other words, a lower Euclidean distance indicates two images are perceptually identical and vice versa. A limitation of Euclidean distance is that there is no uniformed boundary or threshold that can be applied to evaluate most of image hashing systems. The threshold should be determined based upon different hash generation models and applications.

Normalized Hamming Distance (NHD). For a pair of image binary hashes $\boldsymbol{h}$ and $\boldsymbol{h}'$, both of which contain n-bit length, the normalized Hamming distance between them is defined as

$$NHD(\boldsymbol{h}, \boldsymbol{h}') = \frac{1}{n}\sum_{i=1}^{n}|\boldsymbol{h}_i - \boldsymbol{h}'_i|$$

The normalized Hamming distance is calculated firstly by bit-by-bit comparisons of two hash vectors, then normalized in the range $[0, 1]$. The two images are regarded as perceptually same if the distance is close to 0, whereas the distance is expected to be close to 0.5 for two perceptually different images. Due to its simplicity and efficiency, the normalized Hamming distance is the most widely used measurement metric in image hashing systems, especially for those with the postprocessing containing one-bit quantization or relationship-based bit generation, such as the approaches in [10], [16].

ROC Curves. Both the Euclidean distance and the normalized Hamming distance directly compare two image hash sequences and calculate the distance between them. The Receiver Operating Characteristics (ROC) curves [17] make use of one of the above results to evaluate the robustness and discriminative capability through statistical analysis. Generally, given the reference images sets $\boldsymbol{X}$, two image sets are firstly constructed:

- $\boldsymbol{X}_s$ contains the similar versions of $\boldsymbol{X}$ (distorted under CPOs)
- $\boldsymbol{X}_d$ contains the different versions of $\boldsymbol{X}$ (attacked under CCOs)

Let X, X_s and X_d are the reference image and its corresponding versions in two different sets, denoting as $X \in \boldsymbol{X}$, $X_s \in \boldsymbol{X}_s$ and $X_d \in \boldsymbol{X}_d$. Given two predefined thresholds τ_1 and τ_2 ($\tau_2 = a\tau_1$, where a is a constant value satisfying $\frac{1}{\tau_1} \geq a \geq 1$), the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are recorded as follows:

- $P_{frr}(\tau_1) = Pro(D(\psi(X, k), \psi(X_s, k)) < \tau_1)$
- $P_{far}(\tau_2) = Pro(D(\psi(X, k), \psi(X_d, k)) > \tau_2)$

where D is the distance between two hash values. With the varying of both thresholds, the ROC curve is drawn, which reflects a visual characterization of the tradeoff between FAR and FRR.

The above measurement metrics have been widely used in literature. Whereas the development of benchmark platforms to provide a more convenient comparison is also emerged recently. The early works have been done by the Watermarking Virtual Lab of ECRYPT [18], [19]. H. Zhang *et al.* [20] have analyzed the problems of traditional metrics and proposed a new benchmark based on human subjective identification to provide a more comprehensive and fairer evaluation for image hash functions.

3.3 Security Evaluation

We separately discuss the security evaluation of image hashing in a new subsection because of its uncertainty and complexity. The security of an image hash function depends on key-based randomization. Hence, the goal of randomization is to make the defeat of the hash algorithm much harder. Ideally, the adversary should have to solve a hard problem to generate collision or failure cases for the hashes. In particular, there are two major malicious attacks can be tried by an adversary:

- The adversary may try to make a perceptual different image as the input, but the same hash value is generated.
- The adversary may attempt to forge a perceptual identical image which yet leads to the hash algorithm generates a different hash value.

The security of image hash functions is usually evaluated under Kerckhoffs principle [21] in which it is assumed that an adversary knows all information about hash functions except the secret key. The security can be evaluated by

either experiment-oriented analysis or information theory-oriented analysis. In the following, some of popular approaches related to security evaluation are reviewed.

Confusion and Diffusion. The confusion and diffusion are firstly proposed by Shannon [22]. They have been used to evaluate the security of cryptographic systems. Coskun *et al.* [23] present a new notion of confusion and diffusion for image hash functions. The confusion is the complexity of the relation between the key and the hash value, i.e., for hash functions which have relatively strong confusion capabilities can generate totally different hash values for the very similar input keys. Whereas weak confusion capability implicates that the key-space is certainly narrow and the hash function can not resistant against brute-force attacks. The diffusion is originally defined as the complexity of the relation between plaintext and ciphertext. For image hash functions, it is newly defined as the irrelevance or complex relationship between the perceptual information of the input and the hash value. An image hash function which has good diffusion capability can be expected to generate a hash value containing significant difference when only slight changes occur in the input image. However, the conclusion in [23] drawn from the tests of some practical hashing algorithms comes to that these algorithms are not recommended to applied for multimedia authentication due to their low diffusion capability.

Differential Entropy. Swaminathan *et al.* [8] firstly suggest using the differential entropy for security evaluation of image hashing. It is assumed that the adversary knows the hashing algorithm $\psi(\cdot)$ and the image X, and tries to estimate the hash value without knowing the secret key. The degree of success that can be attained by the adversary depends on the amount of randomness in the hash values, which can be evaluated by the differential entropy. For a continuous random variable X, the definition of differential entropy is given as [24]:

$$H(X) = \int_{\Omega} f(x) \log_2 \left(\frac{1}{f(x)} \right) dx$$

where $f(x)$ is the probability density function of X, and Ω is the range of support of $f(x)$. The higher the entropy of the hash value, the more difficult the adversary would estimate or forgery the hash without knowing the key. Nevertheless, it is stated in [12] that high differential entropy is certainly a necessary property of secure image hashes, but it is not adequate for completely quantifying security. In another word, a secure image hash should generate a hash value with high differential entropy, but not vice-versa.

Unicity Distance. The unicity distance was firstly proposed in [22] to investigate encryption systems. The basic idea is that using the same secret key to produce an increased number of plain/ciphertext pairs would reduces the uncertainty of the encryption key. When the number of the produced plain/ciphertext pairs is large enough, one can almost estimate the secrete key. Mao *et al.* [25] adapts the unicity distance to evaluate the security of robust image hashing algorithms. The new definition of unicity distance of an image hashing algorithm is defined as the minimum number of observed image hash pairs needed to uniquely determine the hashing key. In detail, given an image hash function $\psi(\cdot)$, the input image X, the secret key k and the output hash value $\boldsymbol{h}$, when the same key k is used to generate n image hashes, the conditional entropy of k is $H(k|(X_1, \boldsymbol{h}_1), (X_2, \boldsymbol{h}_2), \ldots, (X_n, \boldsymbol{h}_n)) = H(k|\{X_j, \boldsymbol{h}_j\}_{j=1}^n)$. The conditional entropy is generally decreased with the increase of n. Hence, the goal becomes to how the uncertainty in the secret key decreases with more observed image hash pairs. Based upon the simulation results in [25], a secret key can be gradually refined and gained by increasing the number of image hash pairs.

Shannon Equivocation. Under the Kerckhoffs security principle, Koval *et al.* address the issue of estimation of the complexity to reveal a particular secret key k when only *a single pair* of the image X and the hash function $\psi(\cdot)$ is available [15]. The security evaluation is formulated in terms of equivocation, which is also based on Shannon's theory [22]. The equivocation is cryptographically defined as the ambiguity about the secret that remains after observing the ciphertexts. In the case of image hashing, equivocation is redefined as:

$$H(k|\psi(X,k)) = H(k) - I(k; \psi(X,k))$$

where $H(k)$ and $H(k|\psi(X,k))$ are entropy of the secret key k and conditional entropy of k given an input image X and its hash function $\psi(X,k)$, respectively. $I(k;\psi(X,k))$ is the mutual information [24] between k and $\psi(X,k)$, which is also the auxiliary information potentially obtained by the adversary. The estimation of the complexity to obtain the secret key is applied to two particular image hashing algorithms, and it is demonstrated that both algorithms provide certain auxiliary information to the adversary.

As we reviewed above, the security analysis of image hashing is generally based on information theory. Because of the special properties of image hashing, whether the cryptographic analysis can be investigated, and whether the same attacking scenario can be formed to image hashing systems are still being considered. Further information about security evaluation of image hashing can be referred in [26]–[28].

4. Image Hashing Methods

Depending upon extraction procedures and feature types, the image hashing methods can be classified as the following approaches:

- Approaches based on statistic information;
- Approaches based on low level features;
- Approaches based on dimensionality reductions;
- Approaches based on invariant properties in transformed domains.

Different approaches have their own properties and advantages, as well as the related limitations. In this section, we review and discuss these four categories in detail with representative methods for each category.

4.1 Approaches Based on Statistic Information

The statistic information, such as image intensity, mean and variance, is generally invariant under small perturbations to the image. Several image hashing algorithms are proposed by employing this robust principle.

In the early works, Schneider *et al.* [29] suggest to use intensity histogram from image blocks to create image hash, where the local information is captured by image blocking. The histograms are pubic key encrypted for the final image signature which needs to be stored and decrypted again for verification. The Euclidean distances between intensity histograms are used as a measure to verify the image. The biggest limitation of the scheme is that it is easy to attack the image but maintain the same histogram hash.

Venkatesan *et al.* [30] propose an image hashing scheme based on image statistic vectors extracted from random blocks in the variant subbands in a wavelet decomposition of the image. The mean values from coarse subband and variances from other subbands are extracted and probabilistic quantized as the statistic vectors. The vectors are finally input in to the decoding stage of a Reed-Muller Error correcting code [31] to generate the final hash value. A similar scheme based on K-means segmentation [32] is proposed to extract the statistics such as mean, variance, and other higher order moments from image blocks or image segments for image hashing. Both of the two schemes have the same limitation as [29].

Recently, the image histogram is concerned again due to its invariance to the positions of image pixels. Xiang *et al.* [10] propose an image hashing scheme based on histogram shape and apply it to invariant image watermarking [33]. It is investigated that the histogram shape, i.e. the relative relations in the number of pixels among groups of two different bins, is invariant to both basic and challenging geometric operations. By comparing the population among each two different bins from a Gaussian blurred image, a binary string is obtained and then key-based permuted to generate the final hash value. The scheme achieves an excellent robustness to geometric operations, even for the challenged operations, such as strong shearing, bending, and warping. However, the local structure of the image is totally lost during the hash construction.

Remarks. The biggest merit of statistic information based methods is the robustness against perturbations to the image, so that the scheme in [10] achieves a very well robust capability to geometric deformations. Additionally, in order to capture local information, blocking or segmentation [29], [30], [32] are exploited, in which case the robustness almost depends on the invariance of image partition under geometric operations. However, the previous image partitions do not have a bright result under these operations. On the other hand, the security of this kind of methods is very weak, since the adversary can easily disturb the image content but generate an acceptable hash value. Random partition may solve the security problem under the assumption that the sizes and the positions of image blocks are secure enough against attackers.

4.2 Approaches Based on Low Level Features

The low level features are edges, interest points, or blobs information in the image. Robust low level feature extraction is the major task for this kind of approaches. The related algorithms are proposed recently and gain lots of valid results.

Monga *et al.* [11], [34] propose an image hashing scheme based on end-stopped wavelet cells. Through the evaluation and comparison results of several famous feature points detectors, end-stopped wavelet gains the most satisfactory robustness to CPOs. In this scheme, the feature points are firstly extracted by using end-stopped wavelet transform. Then an iterative algorithm similar as [9] is employed to obtain an optimistic hash value. Alternatively, key-based random partitioning of the image can be also applied in advance for random hash generation. However, the feature points detection may be failed in the case of smooth texture in image blocks. An extending approach is proposed in [1] which aims to find a proper affine transform that best approximates the geometric distortions on the input image. As a result of approximation, which will decrease the efficiency, the robustness against geometric operations can be largely increased.

A mesh-based geometric distortion resilient image hashing scheme is proposed by Lu *et al.* [35], [36] for copy detection and tracing images. The Harris detector is firstly applied on the downsampled image to detect robust points. Following, Delaunay tessellation is performed using the obtained points to generate the set of meshes. Each mesh is normalized and a threshold-based binary hash string is generated. A coarse-to-fine indexing is also suggested for fast image tracing in large scale databases. There is no key injection in the scheme thus the security cannot be evaluated. Moreover, the mesh normalization during hash generation is complex and time cost.

The image hashing scheme for detecting and localizing image tampering is presented in [37], where the localization of the tampering is a special functionality of image hashing. The hash consists of two parts: the first part is used for authentication only, based on the Scale-Invariant Feature Transform (SIFT) [38], which have been shown to be robust to several geometric transformations; the second part for tampering localization is based on local quantized histograms of edge directions. The performance of both robustness and collision resistance, as well as the choice of parameters, are analyzed in [39] through theoretical modeling and experiments.

Remarks. The low level features reflect a rough contour

of the image, which can be employed to generate the image hash. The properties of the image hashing algorithms based on low level features mainly depend on the performance of low level feature detectors. Ideally, if the detector is robust enough against CPOs, and has sufficient discriminative capability to CCOs, an image hashing function with satisfactory performance would be constructed under a suitable key projection. On the other hand, the parameters used to constructing hash, such as the number of feature points selected, the number of meshes or the edges, should be selected carefully in order to avoid unnecessary costs. And also, the parameter defining may be different from various image types.

4.3 Approaches Based on Dimension Reduction

The generalized definition of dimension reduction is the process of reducing a high dimensional datasets into a relative low dimensional datasets as well as maintaining the properties of the original data [40]. Generally, in the dimension reduction based image hashing approaches, the images are regarded as matrices and the hashes is generated based on the retaining coefficients in a low-rank matrix approximation of the image.

Kozat *et al.* [41] choose the Singular Value Decomposition (SVD) to generate the low-rank approximation due to some of its provable optimality properties. Intermediate features are firstly generated by applying SVD on the image. Following, a secondary image is constructed from the intermediate features and decomposed by SVD again for the final hash. The SVD-based image hashing algorithm gains a certain robustness to severe geometric operations on images, but it has a relative low discriminative capability to different images.

Motivated by [41], Monga *et al.* [12] propose to use Non-negative Matrix Factorization (NMF) for image hashing because of its non-negativity constraints. The NMF is also applied twice on the image, in conjunction with pseudo-randomization to generate the secure hash sequence. The two-stage cascade application of NMF on images obtains a higher robustness under CPOs while reducing the misclassification rate for the images under CCOs.

A Fast Johnson-Lindenstrauss Transform (FJLT) based image hashing scheme [42] is suggested since the FJLT shares the low distortion characteristics of a random projection but requires a lower complexity. This approach experimentally achieves comparable robust capability as NMF-based scheme, but needs less computation cost. Moreover, the discrimination to tiny changes on the image is not covered in the scheme.

Remarks. The image hash generated by dimension reduction approaches actually depends on the creation of an image adaptive basis, which is an unsupervised learning process. Generally, the learning procedures require much more computational costs due to its iterative calculations. However, as introduced above, this kind of approaches obtains a satisfactory robustness against the strong geometric operations, meanwhile, the discriminative capability is also ensured in [12]. Therefore, a good tradeoff between the efficiency and classification performance would be the major objective when designing an image hashing function via dimension reduction techniques.

4.4 Approaches Based on Invariant Properties in Transformed Domains

We classify the image hashing algorithms, that transform the image from the spatial domain into other domains such as DCT/DWT or Fourier domain, as transformed domains based approaches. Different algorithms utilize different invariant properties in various domains to construct the image hashes.

One of the early work is proposed by Fridrich *et al.* [16] that constructs the image hash by projecting its each DCT block on the zero-mean random patterns independently, which depends on the resistance of the low frequency DCT coefficients from an image under slight CPOs. Mihçak *et al.* [9] develop a wavelet based image hashing algorithm by using an iterative approach to binarize the DC-subband (LL subband) of a wavelet decomposition of the image. During the iterations, the significant features are preserved whereas the unstable features are eliminated.

The robust properties of Radon transform are exploited and applied for the construction of image hash in [43]–[45]. The image is firstly projected in Radon domain, then the median point of each projection of each angle [43], the PCA features on Radon vectors [44], and the low frequency DCT coefficients of radial variance vectors [45] are extracted separately for hash generations. While all the above Radon based hashing approaches are no key combined. Swaminathan *et al.* [8] propose an image hashing scheme by maintaining the rotation invariant coefficients of Fourier-Mellin Transform (FMT). The scheme achieves a good robustness under CPOs but a vulnerable discriminative capability to local tampering.

A special image hashing scheme generating the hash value in compressed domain is proposed in [46]. The hash construction is based on JPEG2000 compression which is the latest still image compression standard [47]. The secret key is embedded by means of employing a parameterized lifting scheme in the wavelet decomposition stage, whereas the hash is extracted from the compressed bitstream.

Remarks. The robustness and discrimination of this kind of approaches mainly depends on the properties of the applied transforms, while some of the algorithms are still sensitive to geometric operations [16] or not distinguishable to content changing manipulations [8]. Concerning the security aspect, since most of the transformations are not new, the coefficients or parameters in the transformed domain can be easily attacked as simulated in [48]. However, improving the security may sacrifice somewhat of the robustness to CPOs. Furthermore, while constructing image hashing in

Table 1 Comparisons of the robustness of image hashing approaches.

Image Hashing Schemes	Compression	Cropping	Rotation	Rescaling	Noise	Blurring	Mean Filter
Statistic Information							
Schneider et al. [29]	++++	+	+	+	+	++	+
Venkatesan et al. [30]	+++++	++	+	+++	+++	+++	+++
Kailasanathan et al. [32]	+++++	+	+	+	+	+++	+++
Xiang et al. [10]	+++++	+++++	+++++	+++++	++++	++++	++++
Low Level Features							
Monga et al. A [11]	+++++	+++	++	+++++	+++	++++	++++
Lu et al. [36]	+++++	+++	+++	++++	++++	+++	+++
Roy et al. [37]	+++++	+++	++++	++++	+++	+++	+++
Dimension Reduction							
Kozat et al. [41]	++++	+++	++++	++++	+++	++++	++++
Monga et al. B [12]	+++++	++++	++++	++++	+++++	+++++	+++++
Lv et al. [42]	+++++	++++	+++++	++++	+++++	+++++	+++++
Invariant Properties in Transformed Domains							
Fridrich et al. [16]	+++++	+	+	+	++++	+	+++
Mihçak et al. [9]	+++++	++	++	++++	++++	+++	+++
Lefebvre et al. [45]	+++	+	+	++++	+	++	+++
Swaminathan et al. [8]	+++++	+++	+++	++++	++	++++	++++
Laimer et al. [46]	++	+	+	+	+	+	+

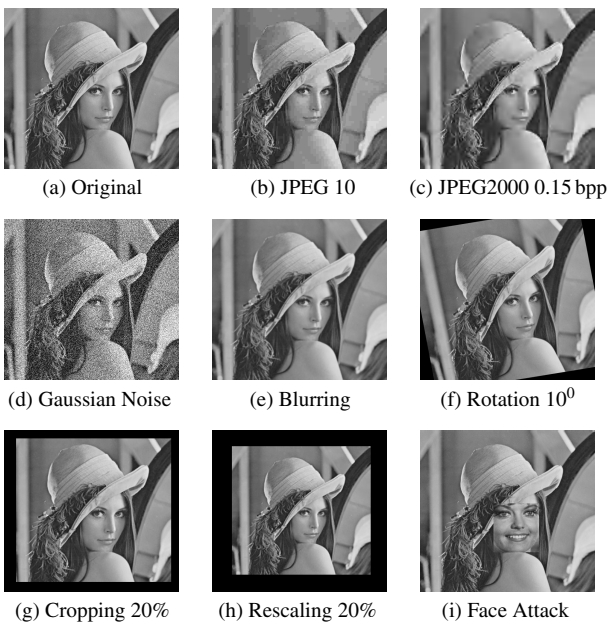
compressed domain, the effect on the compression performance caused by the secret key should be considered delicately.

4.5 Discussions

Numerous and diverse image hashing schemes have been proposed in literature as we discussed above. One of the basic design principles of image hashing functions is the robustness against CPOs. Depending on the simulation results and evaluations from their original works, a concise estimation is given in Table 1 about the robustness of the reviewed image hashing schemes under some typical content preserving operations, such as compression, rotation and noise. We observe that it is much easier to gain robustness against compression than other signal processing operations, whereas more difficult to geometric modifications.

A simulation is performed to evaluate the robust and discriminative capabilities of several representative approaches with the results shown in Fig. 3, where the corresponding modified images are listed in Fig. 2. Note that Fig. 2 (b)–(h) are the images modified under CPOs, and Fig. 2 (i) is the attacked image under CCO. In the desired case, the distance between the face attacked image and original image should be distinguishable from other images under CPO. However, there is no distinguishability gained between CCO and CPO as shown in Fig. 3, especially the statistic information based schemes. The feature point based scheme [11] seems to be most sensitive to the attack, but the robustness against rotation and cropping is unsatisfactory.

Table 2 gives a summary of the approaches including the hash construction techniques and their various properties. It can be observed that there is no perfect scheme that satisfies all desirable requirements. A high robustness may couple with some other sacrifices, such as the high complexity in [12], [41], [42], low discrimination to CCOs [8], [10]. Accordingly, in some cases [8], [10], [46], the discrimination to CCOs seems to be conflicted with robustness. A good tradeoff between both is significant important. The hash length is an intuitive representation of the compactness of hash functions, while from the summary table we see that having a long hash sequence does not mean possessing a good performance. The secret key can be combined (a) before, (b) during, or (c) after feature extraction stage as shown in Fig. 1. However, key combining in stage-c would cause the scheme vulnerable to attacks, since the adversary can easily generate an intermediate hash value without any accessorial information. The localization actually is not a mandatory requirement but can be an attractive feature for image hashing if the related application requires to localize malicious tampering. Concerning the security, here we only list a rough estimation of the security levels since exact eval-



(a) Original (b) JPEG 10 (c) JPEG2000 0.15 bpp

(d) Gaussian Noise (e) Blurring (f) Rotation 10^0

(g) Cropping 20% (h) Rescaling 20% (i) Face Attack

Fig. 2 Different operations on Lena.

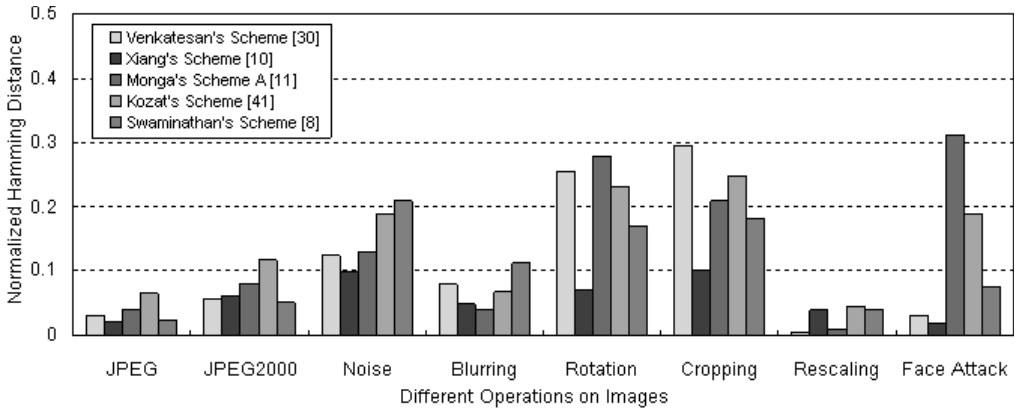


Fig. 3 Robustness and discrimination performances of several approaches via NHD.

uation of the security is still somewhat intractable. Further discussions will be shown in next subsection.

5. Open Issues

Diffusion vs. perceptibility. For an image hashing with a good diffusion capability, slight modifications on the image content should lead to significant difference in the hash value. However, the diffusion of most approaches is not satisfied. A discriminative image hashing scheme based on region of interests is proposed [49] aiming to solve the diffusion problem. Once one ROI is modified, the hash value would totally changed to ensure the diffusion capability, while it is not robust to geometric operations. On the other hand, the image hash is established based on the image content, i.e. the perceptual information. Small changes on the image, such as blocks replacing in [23], certainly cause the corresponding slight changes in the image hash. Therefore, whether the image hashing should comply with the diffusion capability is a little questionable.

Security analysis: Theoretical vs. experimental. There are several metrics or benchmarks proposed to evaluate the security of image hashing functions as we discussed in Sect. 3.3. An information theory oriented framework seems to be more persuasive to prove the security, such as the differential entropy, unicity distance. However, it may be plausible from the experimental point of view. The FMT-based hashing scheme [8] is a typical case, which has a relative high differential entropy and a high unicity distance than some other schemes. Nevertheless, a different hash generated from a similar image or a meaningless image having the same hash can be easily obtained by changing Fourier coefficients [2]. The example gives a result that an image hashing scheme which is provable secure may be vulnerable under simple experimental oriented attacks. Fair and objective security evaluation methods, either theoretical or experimental oriented, or both, are required.

Hashing for other media formats. The images actually have the least amount data comparing with other media formats, such as audio, video. Even though there are several approaches proposed for audio hashing and video hashing, developing a desirable hashing functions for other media formats is much more challengeable and difficult.

Hashing in the compressed domain. As we reviewed, the performance of JPEG2000-based hashing scheme [46] is not as good as other approaches due to various compression parameters and restriction, even though it is one of the latest schemes. The multimedia contents generally are firstly compressed then transmitted or stored. Generating the hash value during compression would be more attractive and applicable than hashing in raw data.

Hashing in the encrypted domain. Generating the image hash from a plain image is under the assumption that one who generate the hash is trusted by the image creator. While if the one can not be trusted, i.e., an untrusted third party, the hash should be generated from a cipher image which is encrypted for confidentiality. Hashing in the encrypted domain would solve the problem, however, it is just at the beginning and staying in theoretical research [50].

6. Conclusion

This paper reviewed the developments and research trends on image hashing. A general framework and the evaluation criteria for image hash functions are firstly provided, particularly to the security evaluation methods. We pay most attention on the construction of image hashing and various approaches are discussed and compared. Different approaches have their own properties and limitations, while there is no perfect scheme satisfying all desirable requirements. A good tradeoff among robustness, discrimination and security should be considered delicately when designing an image hash function. Furthermore, objective measure metrics are urgently needed to provide a fair and effective security analysis.

Table 2 An overview of image hashing approaches.

Image Hashing Schemes	Pre-Processing	Hash Construction	Hash Length	Key Combination	Evaluation Metrics	Complexity	Security	Robustness	Discrimination	Localization
Statistic Information										
Schneider et al. [29]	Image blocking	Intensity histogram	256 vector	No key	ED	Low	Low	Low	Low	Yes
Venkatesan et al. [30]	Wavelet decomposition, Random partition	Mean, Variance	805 bits	a	NHD, Unicity distance	Low	Low	Median	Median	No
Kailasanathan et al. [32]	K-means segmentation	Mean, Variance, Kurtosis, Skewness	≥ 178 bytes	No key	ED	Low-Median	Low	Low	Low	No
Xiang et al. [10]	Gaussian Blurring	Histogram shape	435 bits	c	NHD	Low	Low	High	Low	No
Low Level Features										
Monga et al. [11] A	Random partition	End-stopped wavelet feature points	512 bits	a	ROC, NHD	Median	Median	Median	Median-High	No
Lu et al. [36]	Wavelet decomposition	Harris corners Delauney tessellation	≥ 640 bits	No key	NHD	High	Low	Median-High	High	Yes
Roy et al. [37]	Downsampling Anisotropic blurring	SIFT Edge detection	920 bits	b	ROC	Median-High	Median-High	Median-High	High	Yes
Dimension Reduction										
Kozat et al. [41]	Random partition	SVD-SVD	150 vector	a, b	ED	High	Median-High	High	Median	No
Monga et al. [12] B	Random partition	NMF-NMF	64 vector	a, b	ROC, Differential entropy	High	Median-High	High	Median-High	No
Lv et al. [42]	Random partition	FJLT	20 vector	a	ROC	High	Median	High	Median	No
Invariant Properties in Transformed Domains										
Fridrich et al. [16]	Image blocking	Projections of DCT blocks on random patterns	420 bits	b	NHD Unicity Distance Equivocation	Low	Median-High	Low	Median-High	No
Mihçak et al. [9]	Order statistic filter	DWT iterative thresholding	1000 bits	a	NHD	Low-Median	Low-Median	Median	Low	No
Lefebvre et al. [45]	-	Radon transform DCT on radial variance vectors	40 vector	No key	Peak of Cross Correlation	Median	Low	Low	Median	No
Swaminathan et al. [8]	Low-pass filter, Downsampling	FMT	420 bits	b	ROC, Differential entropy, Unicity Distance	Low	Median	High	Low	No
Laimer et al. [46]	-	JPEG2000 bitstream parsing Byte extraction	≥ 50 bytes	b	NHD Unicity Distance	Median	Median	Low	High	No

References

[1] V. Monga, Perceptually based methods for robust image hashing, Ph.D. thesis, University of Texas, 2005.
[2] S. Wang and X. Zhang, "Recent development of perceptual image hashing," J. Shanghai University (English Edition), vol.11, no.4, pp.323–331, 2007.
[3] M.K. Mihçak and R. Venkatesan, "A perceptual audio hashing algorithm: A tool for robust audio identification and information hiding," IHW '01: Proc. 4th International Workshop on Information Hiding, pp.51–65, 2001.
[4] H. Özer, B. Sankur, N. Memon, and E. Anarim, "Perceptual audio hashing functions," EURASIP J. Applied Signal Processing, vol.2005, pp.1780–1793, 2005.
[5] J.C. Oostveen, T. Kalker, and J. Haitsma, "Visual hashing of digital video: Applications and techniques," Applications of Digital Image Processing XXIV, pp.121–131, SPIE, 2001.
[6] A. Mucedero, R. Lancini, and F. Mapelli, "A novel hashing algorithm for video sequences," IEEE International Conference on Image Processing (ICIP '04), pp.2239–2242, 2004.
[7] X.C. Guo and D. Hatzinakos, "Content based image hashing via wavelet and radon transform," PCM 2007, LNCS 4810, pp.755–764, 2007.
[8] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Information Forensics and Security, vol.1, no.2, pp.215–230, 2006.
[9] M.K. Mihçak and R. Venkatesan, "New iterative geometric technique for robust image hashing," ACM Workshop on Security and Privacy in Digital Rights Management, pp.13–21, 2001.
[10] S. Xiang, H. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," MM&Sec '07: Proc. 9th Workshop on Multimedia & Security, pp.121–128, 2007.
[11] V. Monga and B.L. Evans, "Perceptual image hashing via feature points: Performance evaluation and tradeoffs," IEEE Trans. Image Process., vol.15, no.11, pp.3453–3466, 2006.
[12] V. Monga and M.K. Mihçak, "Robust and secure image hashing via non-negative matrix factorizations," IEEE Trans. Information Forensics and Security, vol.2, no.3-1, pp.376–390, 2007.
[13] V. Monga, A. Banerjee, and B.L. Evans, "A clustering based approach to perceptual image hashing," IEEE Trans. Information Forensics and Security, vol.1, no.1, pp.68–79, 2006.
[14] C. Savage, "A survey of combinatorial Gray codes," SIAM Review, vol.39, no.4, pp.605–629, 1997.
[15] O. Koval, S. Voloshynovskiy, F. Beekhof, and T. Pun, "Security analysis of robust perceptual hashing," Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE, vol.6819, 2008.
[16] J. Fridrich and M. Goljan, "Robust hash functions for digital watermarking," IEEE International Conference on Information Technology: Coding and Computing (ITCC '00), pp.178–183, 2000.
[17] T. Fawcett, "ROC graphs: Notes and practical considerations for researchers," Technical Report, HP Laboratories, USA, 2004.
[18] M. Schmucker and H. Zhang, "Benchmarking metrics and concepts for perceptual hashing," Technical Report, ECRYPT European Network of Excellence in Cryptology, 2006.
[19] H. Zhang, M. Schmucker, and X. Niu, "The design and application of phabs: A novel benchmark platform for perceptual hashing algorithms," IEEE International Conference on Multimedia and Expo (ICME '04), pp.887–890, 2007.
[20] H. Zhang, Q. Li, H. Zhang, and X. Niu, "A benchmark for perceptual hashing based on human subjective identification," Information Technology J., vol.8, pp.544–550, 2009.
[21] A. Kerckhoffs, "La cryptographie militaire," Journal des sciences militaires, vol.IX, pp.5–83, 1883.
[22] C.E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol.28, pp.656–715, 1949.
[23] B. Coskun and N. Memon, "Confusion/diffusion capabilities of some robust hash functions," Proc. 40th Annual Conference on Information Sciences and Systems (CISS '06), 2006.
[24] T. Cover and J. Thomas, Elements of information theory, John Wiley & Sons, NY, 1991.
[25] Y. Mao and M. Wu, "Unicity distance of robust image hashing," IEEE Trans. Information Forensics and Security, vol.2, no.3-1, pp.462–467, 2007.
[26] S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Robust perceptual hashing as classification problem: Decision-theoretic and practical considerations," IEEE Workshop on Multimedia Signal Processing (MMSP '07), pp.345–348, 2007.
[27] O. Koval, S. Voloshynovskiy, F. Beekhof, and T. Pun, "Security analysis of robust perceptual hashing," SPIE, 2008.
[28] S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Conception and limits of robust perceptual hashing: Towards side information assisted hash functions," SPIE, 2009.
[29] M. Schneider and S.F. Chang, "A robust content based digital signature for image authentication," IEEE International Conference on Image Processing (ICIP '96), pp.227–230, 1996.
[30] R. Venkatesan, S.M. Koon, M.H. Jakubowski, and P. Moulin, "Robust image hashing," IEEE International Conference on Image Processing (ICIP '00), pp.664–666, 2000.
[31] R.E. Blahut, Theory of practive of error control codes, Addison-Wesley, 1983.
[32] C. Kailasanathan and R.S. Naini, "Image authentication surviving acceptable modifications using statistical measures and k-mean segmentation," IEEE EURASIP Workshop at Nonlinear Signal and Image, 2001.
[33] S. Xiang, H.J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," IEEE Trans. Circuits Syst. Video Technol., vol.18, no.6, pp.777–790, 2008.
[34] V. Monga and B.L. Evans, "Robust perceptual image hashing using feature points," IEEE International Conference on Image Processing (ICIP '04), pp.677–680, 2004.
[35] C.S. Lu, C.Y. Hsu, S.W. Sun, and P.C. Chang, "Robust mesh-based hashing for copy detection and tracing of images," IEEE International Conference on Multimedia and Expo (ICME '04), pp.731–734, 2004.
[36] C.S. Lu and C.Y. Hsu, "Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication," Multimedia Syst., vol.11, no.2, pp.159–173, 2005.
[37] S. Roy and Q. Sun, "Robust hash for detecting and localizing image tampering," IEEE International Conference on Image Processing (ICIP '07), pp.117–120, 2007.
[38] D.G. Lowe, "Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vis., vol.60, pp.91–110, 2004.
[39] S. Roy, Q. Sun, and T. Kalker, "Performance analysis of locality preserving image hash," IEEE International Conference on Image Processing (ICIP '08), pp.1268–1271, 2008.
[40] I.K. Fodor, "A survey of dimension reduction techniques," Tech. Rep., US DOE Office of Scientific and Technical Information, 2002.
[41] S.S. Kozat, R. Venkatesan, and M.K. Mihçak, "Robust perceptual image hashing via matrix invariants," IEEE International Conference on Image Processing (ICIP '04), pp.3443–3446, 2004.
[42] X. Lv and Z.J. Wang, "Fast Johnson-Lindenstrauss transform for robust and secure image hashing," International Workshop on Multimedia Signal Processing (MMSP '08), pp.725–729, 2008.
[43] F. Lefebvre, B. Macq, and J. Legat, "Robust image hashing based on radial variance of pixels," EURASIP, 2002.
[44] F. Lefebvre, J. Czyz, and B. Macq, "A robust soft hash algorithm for digital image signature," IEEE International Conference on Image Processing (ICIP '03), pp.495–498, 2003.
[45] C.D. Roover, C.D. Vleeschouwer, F. Lefebvre, and B. Macq, "Robust image hashing based on radial variance of pixels," IEEE International Conference on Image Processing (ICIP '05), pp.77–80, 2005.

[46] G. Laimer and A. Uhl, "Key-dependent JPEG2000-based robust hashing for secure image authentication," EURASIP J. Information Security, vol.2008, pp.1–18, 2008.
[47] C. Christopoulos and A. Skodras, "The JPEG2000 still image coding system: An overview," IEEE Trans. Consum. Electron., vol.46, no.4, pp.1103–1127, 2000.
[48] F. Ahmed and M.Y. Siyal, "A secure and robust wavelet-based hashing scheme for image authentication," MMM 2007, LNCS 4352, pp.51–62, 2007.
[49] Y. Ou, C. Sur, and K.H. Rhee, "Discriminative image hashing based on region of interest," MMM 2010, LNCS 5916, pp.701–706, 2010.
[50] SPEED, "Signal processing in the encrypted domain," http://www.speedproject.eu/, 2006–2009.

Yang Ou received the B.E. degree in computer science from University of Science and Technology Liaoning, China, in 2004 and M.E. degree from Gyeongsang National University, Korea, in 2006. She is currently a Ph.D. candidate in the Department of information security, Pukyong National University, Korea. Her research interests include image processing, image encryption and authentication.

Kyung Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Daejon Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Daejon Korea from 1985 to 1993. He also worked as a visiting scholar in University of Adelaide, University of Tokyo, and University of California, Irvine, respectively. He is currently a professor in the Division of Electronic, Computer and Telecommunication Engineering of Pukyong National University, Republic of Korea. His research interests are related to cryptography and its applications, wireless communication security and digital rights management.