ISSN: 2321-7782 (Online)
Volume 3, Issue 11, November 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Content Authentication and Forge Detection using Perceptual Hash for image database

Gauri Barse
Computer Department
Jayawantrao Sawant College Of Engineering
Pune, India

Abstract: ***Perceptual image hash has been widely investigated in an attempt to solve the problems of image content authentication and content-based image retrieval. This paper presents a perceptual image hashing algorithm which can distinguish maliciously attacked images from content-preserving ones. We combine statistical analysis methods and visual perception theory to develop a real perceptual image hash method for content authentication. To achieve real perceptual robustness and perceptual sensitivity, the proposed method uses Watson's visual model to extract visually sensitive features that play an important role in the process of humans perceiving image content. We then generate robust perceptual hash code by combining image-block-based features and key-point-based features. A secure hashing scheme is developed for image authentication and finding the forgery regions. The hash can be used to find similar, forged, and different images. It can also identify the type of forgery and locate fake regions containing salient contents. The hash is very sensitive to malicious tampering. The hash of a test image is compared with the reference image. The proposed method achieves a tradeoff between perceptual robustness to tolerate content-preserving manipulations and a wide range of geometric distortions and perceptual sensitivity to detect malicious tampering. Furthermore, it has the functionality to detect compromised image regions. Moreover, compared with some other image hashing algorithms, the proposed approach also achieves better performance even in the aspect of robustness, which is more important in some image hashing application***

I. INTRODUCTION

With the widespread use of image editing software, more and more digital media products are easily to distribute illegal copy. With the advances in multimedia and networking technologies, it has become easy to copy original material completely and distribute illegal copies rapidly over the Internet. In order to trace the unauthorized use of digital contents, media hashing technologies have been applied to digital content management. Unfortunately, it is the sensitivity that makes these functions not applicable to digital images. Since images will also be considered as the identical one even if they have undergone some content preserving manipulations, such as image compression, noising, and filtering. Image hashing is a technique that extracts a short sequence from the image to represent its contents, and therefore can be used for image authentication. . Consequence, it is expected that images which look like the same or very similar should have the same or very similar hash codes, while images which differ from each other should have distinct hash codes.

Perceptual image hashing has been therefore presented to provide the content-based authentication, copyright verification and some other protections for digital images. The core idea of perceptual image hashing is to construct the hash by extracting characteristics of human perception in images, and use this constructed hash to authenticate or retrieve an image without considering the various variables or formats of this image. Recently, perceptual image hash has been developed as a frontier research topic in the field of digital media content security and multimedia applications. The generation of a perceptual image hash is based on well-designed image features that are in accordance with the perceptual characteristic of the human visual system. Such features are extracted from the image perceptual content. Image authentication is performed via comparing the

hash value of an original image with the hash value of a doubted image. A perceptual image hash is expected to be able to survive unintentional distortion and reject malicious tampering within an acceptable extend. The process of human cognizing multimedia data is a complex psychological activity. Moreover, unlike cryptographic hash functions, which are highly sensitive to bit changes, perceptual image hash is scalable and tolerates the fuzziness associated with how computers understand image content, although they are similar in form.

II. LITERATURE SURVEY

Currently there is tremendous amount of image data being generated over internet, this data is very vulnerable to tampering, and hence, it is necessary to provide an authentication process for image dataset as images are many times used as proofs. Perceptual image hash, also known as perceptual image signature, has been proposed as a primitive method to solve problems of image content authentication. A perceptual image hash is a short summary of an image's perceptual content. It has many important applications, for example, image content authentication, tampering. Although many existing works refer to "perception hash", they are not really related to human's visual perceptual characteristics. Based on a general survey of the research on image hash technologies, the earliest hash methods answer whether the image content is authentic, but are unable to detect changed image regions. Recent works emphasize robustness to tolerate content-preserving manipulations and geometric distortion such as rotation/scaling and to detect changed image regions. Thanks to the theory and technology of image processing and pattern recognition, many robust image hash methods were developed in the past dozen years. Based on differences in feature extraction, existing methods in the literatures can be classified into four main categories.

Statistics-based methods: these methods extract image features by calculating statistics such as mean, variance, moments of image blocks, histogram.

Relationship-based methods: these methods use the invariant relationships of the image transform coefficients, Such as discrete cosine transform (DCT) and discrete wavelet transform (DWT), to generate image features and hash codes.

Coarse representation or sketch-based approaches: the hash codes are calculated by using the global coarse features of an image, such as the spatial distribution of the wavelet coefficients or the low-frequency coefficients of the Fourier Transform.

Lower-level features based methods: the hash codes are extracted by detecting salient image feature points. These hash values are very sensitive to local distortions that do not cause perceptually significant changes.

III. IMPLEMENTATION

a) Framework of Perceptual Image Hash

In general, a perceptual image hash system consists of four stages: image preprocessing and transformation, perceptual Feature extraction and description, compression and coding, and encryption and randomization. The general framework is shown in Fig. 1. The purpose of image preprocessing and transformation is to eliminate irrelevant information, recover useful information and enhance image features that are important in subsequent processing. To ensure perceptual robustness and perceptual sensibility, the selection and extraction of perceptual features are very important. Perceptual feature extraction is based on the human visual perception model that is established by the cognitive science theory. It is accomplished via signal processing methods that remove redundant data but retain perceptually significant features. Moreover, to reduce hash Length and improve convenience for storage and hardware implementation, post-processing such as compression and Coding is necessary. Encryption and randomization are used to reduce hash collisions to improve the security of the algorithm.

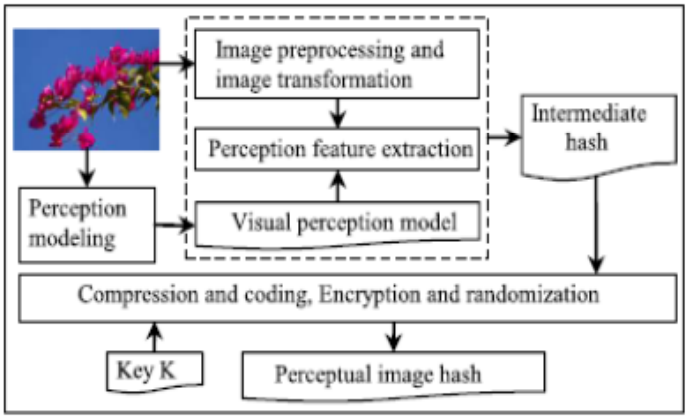


Fig. 1. The framework of perceptual image hash.

The proposed perceptual image hash scheme includes a hash generation algorithm, a tampering detection algorithm, and a tampering localization algorithm. The hash generation algorithm consists of three stages: feature extraction, encryption and randomization, and compression and coding.

b) Hash Generation Algorithm

Considering that the SIFT (Scale Invariant Feature Transform) features are invariant to translation, rotation and scaling transformations in image domain and robust to moderate perspective transformations and illumination variations, we begin our work with the SIFT feature extraction.

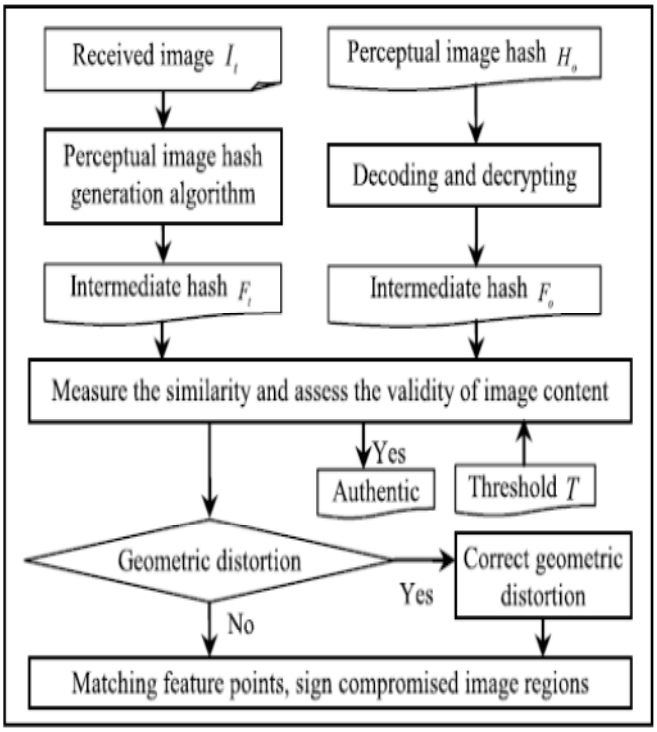


Fig. 2. The schematic diagram of the tampering detection and localization.

c) Tampering Detection and Tampering Localization

Regarding image content changing, it is difficult to define a clear boundary between perceptually insignificant distortion and malicious tampering because some content-preserving manipulations such as JPEG compression are lossy. This results in an intriguing question, that is, the trade-off between robustness to tolerate content-preserving manipulations and sensitivity to malicious tampering. In our work, tampering detection and tampering localization are realized by comparing a distance metric to measure the similarity between hash values. Image tampering will cause the change of feature points, that is, if an image has

been tampered with, then the feature points detected from the compromised regions will be different from the feature points defined in its original version. As a result, the distance between feature points defined in the original version and those detected will be greater. We can use the distance change to detect changed image regions. That is, an image block can be considered as a tampered region if it contains changed feature points, and the change of feature points can be measured via distances between the original feature points and detected feature points in the corresponding image region. Because distance values are clearly distinguishable, we can estimate the cut-off values of the distance change by using the statistical values that are obtained from experimental results

d) Experimental Results and Performance Analysis

Sensitivity Analysis and Performance Comparison

In general, for perceptual image hash, perceptual robustness and perceptual sensitivity are in opposition. The former requires good stability under slight perturbation, whereas the latter requires that the algorithm is sensitive to small malicious modifications. Therefore, the trade-off between perceptual robustness and perceptual sensitivity must be considered in practical applications. To analyze these characteristics ,In the experiment, 1000 tested images with different sizes come from the Ground truth Database. The tampering manipulations include adding image objects, copy-move attack, object replacement attack, hiding image object attack, among others. We examine the perceptual robustness and perceptual sensitivity of the proposed method in terms of the receiver operating characteristics (ROC). For each original image *Io* and corresponding manipulated image, we compare the hash values. We repeat this process with different *T* thresholds and finally arrive at the ROC, the sensitivity becomes weaker when threshold *T* is higher. This means that a smaller threshold will lead to a higher sensitivity. Conversely, to obtain higher sensitivity, threshold *T* should be as small as possible. However, a smaller threshold will lead to a weaker robustness. In practice, an applicable threshold *T* should be selected according to specific application requirements.

Visual Effect of Tampering Localization

For a perceptual image hash scheme, the tampering localization functionality is of crucial importance. This functionality refers to a capability to identify compromised image regions. This functionality can be visually demonstrated via visual effect. We also investigated this functionality of the proposed method via quantitative assessment

Original Image ***Tampered Image*** ***Detected Result***

Fig. 3. Detection results for object replacement attack.

The detected results are indicated by white color regions.

As shown by the experimental results, the proposed method can detect the locations of compromised image regions. It is valid for detecting compromised images that have undergone geometric distortions. To assess the detection performance quantitatively, we estimate the tampering rate and detection rate at the pixel level. Here, the tampering rate and the detection rate are defined as follows:

Tr = Tampering rate

$$= \frac{\text{The size of tampered regions}}{\text{The size of tested image}} \times 100\%$$

Dr = Detection rate

$$= \frac{\text{The size of detectioned regions}}{\text{The size of tested image}} \times 100\%$$

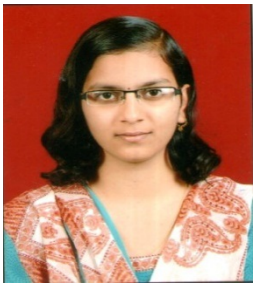
IV. CONCLUSION

In this paper, a real perceptual image hash method is proposed. Based on this hash, an image tampering detection and tampering localization method is presented. As a tool for image content authentication, the proposed method is robust to geometric deformations and content-preserving manipulations such as JPEG compression, adding noise, filtering, and others. It is sensitive to changes caused by malicious attacks, and it achieves a trade-off between robustness against geometric distortion and tampering localization. The experimental results show the effectiveness and the availability of the proposed algorithm for different tampering attacks at three performance levels: image-tampering detection (detection accuracy), compromised region localization (visual effect), and localization accuracy (detection rate at the pixel level). The proposed method can be used for content-based image authentication and for image retrieval and matching in large-scale image databases. Many companies can secure their image database like employees images for cards. Police networks can use this application to secure criminal images so they can detect modifications by attackers.

References

1. Deepa, Nagajothi ,'a secure hashing scheme for image authentication using zernike moments and local features with histogram features', American International Journal of Research in Science, Technology, Engineering & Mathematics,2014
2. X. Si, J. Feng, and J. Zhou, "A Model-based Image Steganography Method Using Watson's Visual Model," in Proc. IEEE Int. Workshop Inf. Forensics Security, 2012, pp. 1–6.
3. Y.-H. Kuo, K.-T. Chen, C.-H. Chiang, and W. H. Hsu, "Query expansion for hash-based image object retrieval," in Proc. 17th ACM Int. Conf. Multimedia, 2009, pp. 65–74.
4. Fang Liu and Lee-Ming Cheng, "Wave Atom-Based Perceptual Image Hashing Against Content-Preserving and Content-Altering Attacks" © Springer-Verlag Berlin Heidelberg 2015 Y.Q. Shi (Ed.): Transactions on DHMS X, LNCS 8948, pp. 21–37, 2015.
5. R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," in Proc. Int. Conf. Image Process., 2000, pp. 664–666.
6. H. G. Schaathun, "On watermarking/fingerprinting for copyright protection,"in Proc. 1st Int. Conf. Innov. Comput., Inf., Control (ICICIC),Aug./Sep. 2006, pp. 50–53
7. R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin,"Robust image hashing," in Proc. Int. Conf. Image Process., 2000,pp. 664–666.
8. 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, Dec. 2005.

AUTHOR(S) PROFILE



Gauri Barse, received the B.E degree in Information Technology and pursuing M.E degree from Jayawantrao Sawant College of Engineering.

