International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON IMAGE FORGERY DETECTION AND REMOVAL

Radika Krishnan[1], Annamariya K S[2], Blessy M D[3], Neenu George[4], Teena Davis[5]

[1]Assistant Professor, Department of Computer Science, Depaul Institute of Science and Technology Angamaly, Kerala, India
[2,3,4,5]Student of MCA, Department of Computer Science, Depaul Institute of Science and Technology Angamaly, Kerala, India

---

Abstract - *In this paper, a survey is performed to study more about different techniques used to detect the image forgery. These methods are either based on global or local features. There is another method Robust Hashing for Image Authentication using P# and Local features. Here the hash is a combination of global and local features of an image. Four types of image forgeries, removal, insertion, and replacement of objects, and unusual color changes can be identified by this method. Threshold value determines the authenticity of the image. Hash performance is measured by the distance metrics. This method can be used to detect tampering image.*

Key Words: image forgery, hashing, authentication.

1. INTRODUCTION

Today most of the people began to use different image processing techniques to make changes in the images for different purposes. Since it is not easy to differentiate with original image and processed images. The processing of images are called image forging. To identify such images different methods are developed. Image hashing is one of the methods for image authentication. In this method a hash value is developed for every image we created. If an image is processed, even one bit of change in the input will change the output hash. The original image and processed image cannot be easily differentiated by humans but they will have small difference in the hash value generated. Hence the changes occurred can be identified. If one image has large difference in the hash value of another image, then they are not related. Sometimes image forgery leads to cybercrimes. So it is important to detect and avoid image forging.

2. LITERATURE REVIEW

In recent years, many researchers have proposed many image hashing methods. These methods can be classified into two types: space domain methods and transform domain methods. Methods used in the space domain include histogram [1], singular value decomposition(SVD) [2], non-negative matrix factorization(NMF) [3-4] and random projections[5].Transforms used for generating image hashes include discrete wavelet transform (DWT) [6-7], discrete cosine transform (DCT) [8], Radon transform [9], Fourier-Mellin transform [10].

Xiang et al. [1] propose a robust image hashing method based on the fact that the shape of an image histogram is invariant to geometric deformation. Robustness and uniqueness of proposed hash function are investigated in detail by representing the histogram shape as the relative relations in the number of pixels among groups of two different bins. It is found from extensive testing that the histogram based hash functions has a satisfactory performance to various geometric deformation, and is also robust to most common signal processing operations thanks to the use of Gaussian kernel low-pass filter in the preprocessing phase.

In [2],Kozat et al. propose a new hashing algorithm employing transforms that are based on SVD (singular value decomposition).This algorithm construct a secondary image derived from the input image. From the secondary image we extract the final features which can be used as a hash value. In this paper we use spectral matrix invariants as embodied by singular value decomposition.

In [3], V.Monga et al. propose the use of non-negative matrix factorization(NMF)for image hashing. This work is motivated by the fact that standard-rank reduction technique such as QR, and SVD, produce low rang bases which don't respect the structure of original data.

In [4], Tang et al. firstly the image re-scaled to fixed size and low-pass filtering is performed to produce a normalized matrix. The normalized matrix are pseudo randomly re-arranged to generate a secondary image, and then NMF is performed on it to generate robust image hash. Similarity between hashes is measured by hamming distance tampering can be detected by comparing hamming distance with predetermined threshold.

In [5] M. Tagliasacchi et al, propose an image hashing algorithm based on compressive sensing principles which solves both the authentication and the tampering identification problems. The content user receives the image and uses the hash to estimate the mean square error distortion between the original and the received image.

In [6], propose a method of decouple image hashing into feature extraction (intermediate hash) followed by data clustering (final hash). For any perceptually significant feature extractor, we propose polynomial-time heuristic clustering algorithm that automatically determine the final hash length needed to satisfy the distortion.

In [7], a wavelet-based hashing scheme is proposed, which can tackle robustness, security and tamper detection issues.

In [8], digital watermarks have been proposed for authentication of both audio data and still images and for integrity verification of visual multimedia. The watermark depends on a secret key and the original image. A special image digest functions are used that return same bit for the images derived from an original image and different bit for completely different images.

Wu et al. [9] propose a print-scan resistant image hashing method based on Radon and wavelet transform. The Radon transforms an image to its luminance distribution, before the wavelet extracts the relationship of the different areas from luminance distribution.

In [10], propose a new algorithm for generating image hash based on Fourier transform features and controlled randomization. The robustness of image hashing is considered as hypothesis testing problem and to evaluate the performance under various image processing operations.

In image processing, Zernike moments (ZMs) are widely used in many occasions because of their orthogonal rotation invariant features. Zernike moments are proposed by Zernike firstly in [11], and has been studied extensively ever since.

Zernike moments have been most widely used in extracting the region based shape features of an image. In most of the research the magnitude of Zernike moments are used and the phase is ignored. In [12], Li et al. propose a new shape descriptor combining bolt magnitude and phase coefficients of ZMs, which is invariant to rotation

3. COMPARISON TABLE

Advantages and disadvantages of different algorithm

sl no	Matching Algorithm	Advantages	Disadvantages
1	Histogram based image hashing	Robust and secure	Misclassification,
2	SVD	Robustness and security	2
3	NMF	Robust	Moderate noise contamination
4	Polynomial time heuristic clustering algorithm	Authentication	Insensitivity to relative scaling
5	Random projection	Authentication	Random projection
6	DWT	Security	High cost of computing,
7	Wavelet based hashing	Robustness , security, tamper detection	Complex in mathematical formulas
8	DCT	Used for misleading tool for hiding facts and evidence	Not produce well results in image blurring and video frame reconstruction
9	Random transform	Robust, common content preserving processing, discriminable to changes	Less speed because of number of comparison required
10	Fourier-mellin	Security, robustness	Difference in image properties cause limitations
11	Zernike moments	Orthogonal rotation invariant	Less retrival accuracy
12	Zernike moments	Retrival accuracy, robust	Object based approach

4. CONCLUSION

Image forgery is one of the major problems in nowadays. There are different techniques to identify the original image from two similar images by using image hashing. It is necessary to produce robust and secure image hashes. For that different techniques like wavelet based hashing, Zernike moments, Polynomial time heuristic clustering algorithm etc. are used. In addition, further study is needed to enhance the robustness to more content-preserving manipulation and sensitivity of hashes to tampering in small regions involving fine details.

REFERENCES

[1] S. Xiang, H. J. Kim and J. Huang, Histogram-based image hashing scheme robust against geometric deformations, Proc. of the ACM Multimedia and Security Workshop, ACM Press, 2007, pp. 121-128.

[2] S. S. Kozat, K. Mihcak and R. Venkatesan, Robust perceptual image hashing via matrix invariants, Proc. of IEEE Conference on Image Processing (lCIP'04), Singapore, Oct. 24-27, 2004, pp. 3443-3446

. [3] V. Monga and M. K. Mihcak, Robust and secure image hashing via nonnegative matrix factorizations, IEEE Transactions on Information Forensics and Security, 2007, 2(3): 376-390.

[4] Z. Tang, S. Wang, X. Zhang, W. Wei and S. Su, Robust image hashing for tamper detection using non-negative matrix factorization. Journal of Ubiquitous Convergence and Technology, 2008, 2(\): 18-26.

[5] M. Tagliasacchi, G. Valenzise and S. Tubaro. Hash-based identification of sparse image tampering. IEEE Transactions on Image Process. 2009, 18(\ 1):2491-504.

[6] V. Monga, A. Banerjee and B. L. Evans, A clustering based approach to perceptual image hashing, IEEE Transactions on Information Forensics and Security, 2006,1(\): 68-79.

[7] F. Ahmed, M.Y. Siyal and V. U. Abbas, A secure and robust hash-based scheme for image authentication, Signal Processing, 2010, 90(5): 14561470.

[8] J. Fridrich and M. Goljan, Robust hash functions for digital watermarking, Proc. of IEEE International Conference on Information Technology: Coding and Computing (ITCC'OO), Las Vergas, USA, Mar. 27-29,2000, pp. 178-183.

[9] D. Wu, X. Zhou and X. Niu. A novel image hash algorithm resistant to print-scan, Signal Processing, 2009,89(\2): 2415-2424.

[10] A. Swaminathan, Y. Mao and M. Wu, Robust and secure image hashing, IEEE Transactions on Information Forensics and Security, 2006, 1 (2): 215-230.

[11] F. Zernike, Beugungstheorie des schneidenverfahres und seiner verbesserten form, der phasenkontrastmethode, Physica, 1934, 1, pp.689-704.

[12] S. Li, M.C. Lee, C.M. Pun, Complex Zernike moments features for shape-based image retrieval, IEEE Transactions On Systems, Ma, and Cybernetics-part A: Systems and Humans, 2009, 39(\): 227-237.