International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Novel Approach For Image Authentication by Robust Hashing Using Zernike Moments and Local Features

Arunkumar Geddalamari[1], D Basavalingappa[2]

[1]4th Sem, M. Tech, ECE Department, G. M. Institute of Technology, Davangere, India

[2]Professor and HOD of the ECE Department, G. M. Institute of Technology, Davangere, India

Abstract: ***Image hashing maps an image to a short binary sequence representing the image characters. This paper proposes a new image hashing method using Zernike moments that are an effective means for extracting robust features from an image. The method is based on rotation invariance of magnitudes and correct phases of Zernike moments and detecting image forgery including removal, insertion, and replacement of objects, and abnormal color modification, and for locating the forged area. We use Zernike moments of the luminance/chrominance components to reflect the image's global characteristics, and extract local texture features from salient regions in the image to represent contents in the corresponding areas. Distance metrics indicating the degree of similarity between two hashes and defined to measure the hash performance. Two thresholds are used to decide whether a given image is an original/normal-processed or maliciously doctored version of a reference image, or is simply a different image. The method can be used to replacement of objects or abnormal modification of colors. Probability of collision between hashes of different images approaches zero. Experimental results are presented to show effectiveness of the method.***

Keywords: Forgery detection, image hash, perceptual robustness, saliency, Zernike moments.

1. Introduction

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. If the image is modified the hash must be changed significantly. In general, a good image hash should be short, robust to ordinary image manipulations. It should be unique in the sense that different images have different hash values, and secure so that any unauthorized party cannot break the key.

People can now use various image processing tools to change images for different purposes. This leads to problems such as copyright infringement and hostile tampering to the image contents. Recently, image authentication techniques have been developed rapidly to verify content integrity and prevent forgery. Image hashing is an important method for image authentication. The concept of image hashing is derived from cryptographic hashing. A cryptographic hash is extremely sensitive to the input data: even one bit change in the input will change the output has dramatically. For an image, however, after normal manipulations such as brightness/contrast adjustment, small-angle rotation and JPEG compression, it is considered as the same image in terms of human vision, and therefore should have the same (or similar) hash as the original. On the other hand, hashes of two different images should be totally different. In image processing, orthogonal rotation-invariant moments (ORIMs) are important features.

2. Proposed System

The procedure for the proposed hash and image authentication scheme.

A) Image Hash Construction

The image hash generation procedure includes the following steps

1) Pre-processing
2) Global feature extraction
3) Local feature extraction
4) Hash generation

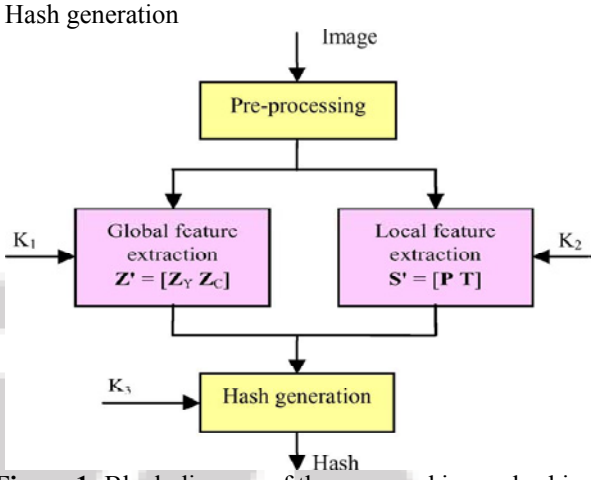

Figure 1: Block diagram of the proposed image hashing method

1) Preprocessing: The image is first rescaled into fixed size image, then it is converted into RGB to the YCbCr representation.
2) Global Feature Extraction: Caluulate the Y Cb and Cr using the Zernike moments to form global feature.
3) Local Feature Extraction: Position and texture of all salient regions to form a local feature. Salient regions includes the coarseness and contrast.
4) Hash Construction: The global and salient local vectors are concatenated to form an intermediate hash, which is

then pseudo-randomly scrambled based on a secret key to produce the final hash sequence.

B. Image Authentication

In image authentication, the reference image is available and the received image is tested and extracted from the hash generation method to form another hash value. These two hash values are compared to determine the test image is same as reference image or different image. The image authentication process is includes the following steps.

1) Feature extraction
2) Hash decomposition
3) Salient regions matching

1) Feature Extraction: The test image is checked from the above method without encryption to produce intermediate hash.
2) Hash Decomposition*:* With the secret keys and, restore the intermediate hash from the reference hash, which is a concatenated feature sequence of the trusted image. Decompose it into global and local features.
3) Salient Region Matching*:* Check the salient regions of tested image and reference image

C. Forgery Classification and Localization

There are four types of image forgery identified as follows

1) If salient regions of reference image is greater than tested image to know the object has been removed.
2) If salient regions of tested image is greater than reference image, the image contains additional image. .
3) If salient regions of both reference and tested images are equal, check the luminance and chrominance components in the Zernike moments if chrominance is greater than luminance, the color changed in the reference image.
4) If salient regions of both reference and tested images are equal, and (ZC - ZY) is less than threshold of chrominance, the test image contains replaced object.

3. Result Analysis

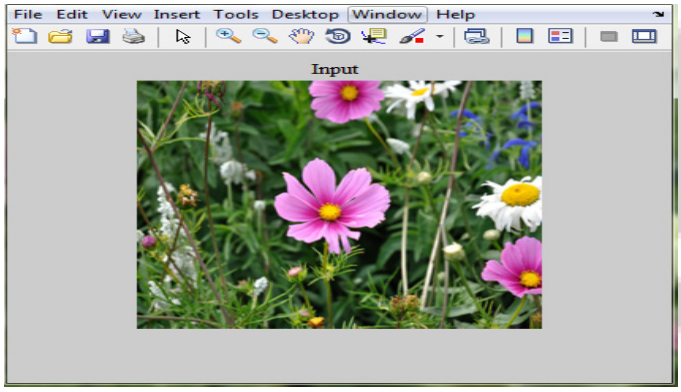

Figure 2: Input image

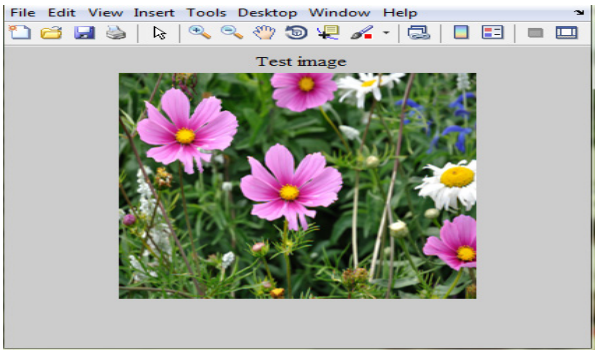

Figure 3: Test image

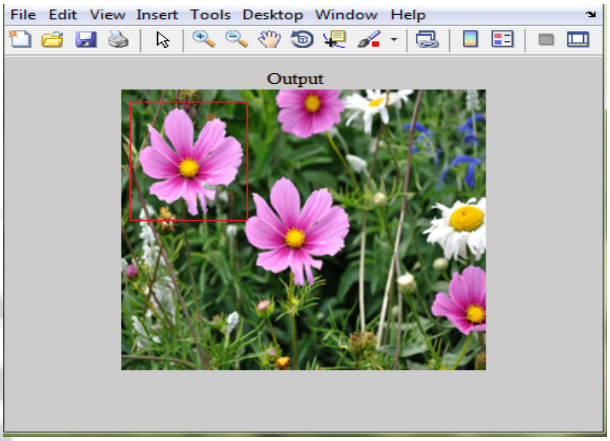

Figure 4: Output image

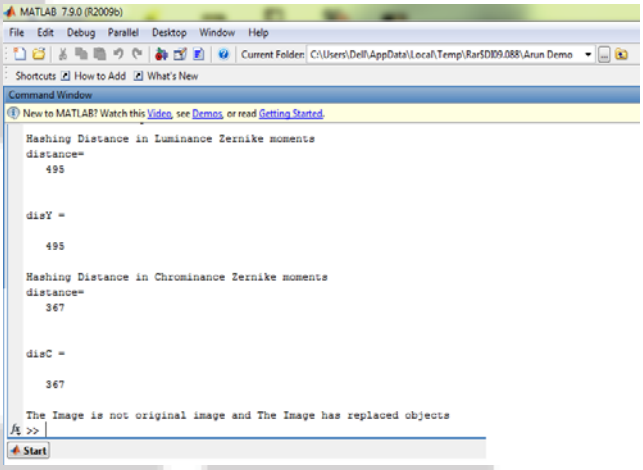

Figure 5: Simulation result

There are four salient regions in the reference image and the six salient regions in tested image. Fig 4 shows the forged image and forged area and Fig 5 shows the simulation result.

4. Conclusion

The method described in this paper is aimed at image authentication. The hash can be used to differentiate similar, forged, and different images. . In the image authentication, a hash of a test image is generated and compared with a hash of the reference image and salient regions of test image is compared with the salient regions of reference image to identify the type of forgery and locate fake regions containing salient contents. Future study is desired to find features that better represent the image contents so as to enhance the hash's sensitivity to small area tampering while

maintaining short hash length and good robustness against normal image processing.

5. Acknowledgment

The authors would like to say thanks to Professor D Basavalingappa who is a Head Of the Department of ECE, GMIT, Davangere. for providing the all facility used in the experiments.

References

[1] V. Monga, A. Banerjee, and B. L. Evans, "A clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 68–79, Mar. 2006.
[2] S. Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," in Proc. ACM Multimedia and Security Workshop, New York, 2007, pp. 121–128.
[3] Z. Tang, S.Wang,X. Zhang, W.Wei, and S. Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18–26, May 2008.
[4] Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.
[5] Y. Lei, Y.Wang, and J. Huang, "Robust image hash inRadon transform domain for authentication," Signal Process.: Image Commun., vol. 26, no. 6, pp. 280–288, 2011.
[6] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection," IEEE Trans. Image Process., vol. 19, no. 4, pp. 981–994, Apr. 2010.