An Improved Forgery Detection Method for Images

Tiss Tom¹, D.Usha Nandini², S.Princemary³, B.Ankayarkanni⁴

School of Computing, Sathyabama Institute of Science and Technology, Chennai, India
tisskayathinkara@gmail.com ushaduraisamy@yahoo.co.in, princemary26@gmail.com, ankayarkanni@gmail.com

Abstract: A forgery image detection system is introduced to detect the forgery in images using global, local and pixel based features. Global features will consider the whole images which include luminance and chrominance features. These global features can be extracted by using Zernike moments. The local feature consists of descriptors of multiple interest points. Image authentication is done by using hash method. The set of images will be trained in the database earlier itself. Then the test image and reference image will be compared based on pixels. By analyzing the hash distance the system can identify the test image is forged or not. As an improvement, pixel based feature extraction is used. Pixel based feature extraction is carried out by using supervised classification algorithm.

Keywords: forgery detection, global, local and pixel features, supervised classification algorithm

1. Introduction

We are indubitably having life in an age where we are exposed to a eminent array of visual imagery. In earlier days images may have trustworthy. But now a days the powerful digital image editing software undermine our trust in images. Even though the image editing software becomes powerful the more becomes the forgery detection systems. The image editing software will carry out the manipulations such as deleting some objects from the images, inserting some objects into the images or replacing some objects. In this system introducing global, local and pixel based features.

The system [1] proposes mapping of an image function onto a set of orthogonal basis functions over the unit circle has been developed on the basis of Zernike moments. To make the image reconstruction from its moment simple the orthogonal property of Zernike moments used. The image representation ability of each order moment and in addition its contribution to the reconstruction process can be enabled by using Zernike moments. The highest order moment is used to yields a reconstructed image which will be close to the original one. The features are tested.
with series of experiments on two different data sets. And also Zernike features can be performed well in moderate level of noise.

In this system [2], proposed two contrast enhancement based forensic algorithms through histogram peak/gap artifacts analysis. First, to detect the global contrast enhancement for both uncompressed and previously JPEG-compressed images extends it. To identify features, exploit zero-height gap bins in gray level histograms. This contrast enhancement detector accomplished high performance, i.e., \( P_d = 100\% \) at \( P_{fa} = 1\% \). Second, the system proposed a novel method to expose source-enhanced composite image, which vitiated the prior detection methods. The composition boundary was precisely located by detecting the disproportionateness between detected block wise peak/gap positional distributions.

The system[3]proposed a method for embedding and detecting chaotic watermarks for large images. Adaptive clustering method is used in order to obtain robust region representation of original image. Ellipsoids are used to approximate robust regions. To avoid annoying artifacts from the embedded watermark a visual masking technique is used.

The images and videos on the social networks which would be edited and misused will affect trustworthiness of online information. To estimate the parameters of geometric transforms and to detect local tampering Radon transform and scale theory is used in [4] this system. The alignment component of forensic hash can provide correct calculation of parameters of geometric transforms.

In a wireless multimedia sensor network (WMSN)for secure image transmission and storageImage authentication is critical. A perceptual hashing-based robust image authentication scheme issued in the system [5]which uses the distributed processing strategy for perceptual image hashes and can provide visual fragility, compactness, security in digital image authentication and perceptual robustnessfor WMSN. A secure pseudorandom chaotic sequence with keys will be generated by cluster head node and dispatch it to the image capturing node. By using this received sequence, several overlapping rectangles will be derived and then calculate the gravity centers and binary distance of two gravity centersin each of the general cluster member node.

The system [6] analyze the log spectrum of input image then extract spectral residual of the image in spectral domain and constructing saliency map in spatial domain. But it can apply only to static images.

In the system [7] hash method is based on Fourier transform features and controlled randomization. It specifies the security issues of existing image hashing scheme. Multimedia hashes will use in content authentication and content based retrieval from databases.
2. Existing System

The global features which include luminance and chrominance extract using Zernike moments representing the characteristics of the images as a whole. Position and texture information of salient regions in the image includes the local features. Image authentication carried out using hash method. Disadvantage of the existing system is that it analyzes only local and global features and also the secret key is complicated.

3. Proposed System

Initially the global and local features of the given input image are extracted. The extracted global features are group to form the hash. The hash is constructed by using Zernike moments. Zernike moment features from order 1 to order 5. Magnitudes of the Zernike moments are rounded and used to form a global vector. Thus the global features are extracted from the image. The local features are extracted by using k-element vector values.

The extracted images are compared with the trained image which is already stored in the database. During the comparison, the image needs not to have the identical pixel values. However, either both image or one of the images may have small modification like contrast, brightness, etc. In addition, to find the similarity our system calculates the distance between the hashes. To compute the distance both the global features vector values and local features vector values are combined by using Euclidean distance calculation.

If the tested image in fake or mismatched with the trained image then it said to be forged image. Four types of forgery can be identified. They are removal, insertion and replacement of objects, and unusual color changes. The performance of proposed system is very high in detecting the forged image. This is because of using hash methods.

Finally the pixel features are extracted from the image. Supervised classification algorithms are applied in pixel-based classification. This technique is used find the exact location of forgery and also the type of forgery. It also includes the features of local and global from the image.

The performance of the proposed system will be high. This is due to the pixel based feature extraction which is more accurate to identify the location and type of forgery.

It efficiently identifies the forgery image which is inserted or removed or replaced and can be used in the real-time image detection applications.
3.1 Implementation

Trained Dataset

The number of images can be trained and stored in the database. The images may be taken from the internet or can be captured using cameras.

Preprocessing

Rescaled the image to a fixed size and converted from RGB values to YCbCr representation.

Feature Extraction

Global Feature Extraction

The Zernike moment of order 'n' and repetition 'm' of an image \( f(x,y) \) can explain as follows:

\[
A_{nm} = \frac{n+1}{\pi} \sum_{x} \sum_{y} f(x,y) V_{nm}(x,y)
\]

Where \( x^2 + y^2 \leq 1 \)

The image \( V(n,m,x,y) \) is the Zernike basis images of order 'n' and repetition 'm'. These basis images are complex and orthogonal. The Zernike moments are essentially the projections of the input image onto these basis images.

Zernike moments has been employed for reconstruction of the original image. The N-th order approximation is given by

\[
f(x,y) = \sum_{n=0}^{N} \sum_{m} A(n,m)V(n,m,x,y)
\]

The information content of the n\textsuperscript{th} order moments is

\[
I(x,y,n) = \sum_{m} A(n,m)V(n,m,x,y)
\]

The moments are returned in the order of (0,0)(1,1)(2,0)(2,2)(3,1)(3,3) and so on, where \( m \leq n \) and \( n = 0 \)

Local Feature Extraction

Local features will be extracted using an image descriptor called surf that combines interest points with visual words.

Pixel Based Feature Extraction

For extracting pixel based features the system uses supervised classification algorithm.

In supervised classification algorithm, it can differentiate one class of other, usually by providing samples of pixels already knows that should be assigned to a specific class. To classify the other pixels on the image, the algorithm use the information already provided. The task is to identify, for each pixel in one image, which class should be assigned to that pixel.
Pseudo code:

Input: Image A and Image B

Steps 1: Select File RefImage=new File("Image A");
Steps 2: Select File TestImage=new File("Image B");
Steps 3: File gh[]=RefImage.listFiles();
Steps 4: File f9 = TestImage.listFiles();
Steps 5: for(i=0;i<f9.length();i++)
   {
      int width=cimage.getWidth();
      int height=cimage.getHeight();
      for(w=0;w<width;w++)
         {
            for(h=0;h<height;h++)
               {
                  if(inimage.getRGB(pixelshash(w,h), h)!=pixelshash(cimage.getRGB(w,h), h))
                     {
                        Flag=false;
                        endif;
                     }
               }
            }
         }
Steps 6: Stop

Output: Comparison Result – Image A and Image B (Matched or Fraud will be detected)

Hash Value Generation

For the above features hash values are generated using randomkey.

Forgery Identification

The calculated pixel values of reference image and tested are compared. If there is no difference with pixels then the reference image and tested image are same. If the reference hash key value is less than test hash key value then the forged type is inserted. Otherwise forged type is removed.

4. Conclusion & Future Enhancement

The proposed system is implemented to find the forged image which is inserted or removed or replaced with new objects. This is achieved by using pixel based features extraction which includes
the supervised classification algorithm. The pixel based features are extracted and then compared with reference image which is already trained in the database. By decomposing the hash values used to find the type of forgery and location of forgery. As an enhancement the pixel based feature extraction is used along with local and global feature extraction method in order to identify the forgery image in an effective way. In Future, the 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.

References

[1] Alireza Khotanzad and Yawhua Hong, “Invariant Image Recognition by Zernike Moments”, IEEE Transactions On Pattern Analysis And Machine Intelligence. Vol. 12. No. 5. May 1990
[2] Remya S, “Digital Image Forgery Detection by contrast Enhancement”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN:2278-8727, volume 16, issue 5, Ver.IX (Sep-Oct. 2014), PP 01-07
[3] Athanasios Nikolaidis and Ioannis Pitas, “Region Based Image Watermarking”, IEEE Transactions on Image Processing, vol.10, No.11, November 2001
[4] Wenjun Lu, Avinash L Varna and Min Wu, “Forensic Hash for Multimedia Information”, IEEE Transactions of Information Forensics and Security, vol. 1, No. 2, pp. 93-116, 2009
[5] Hongxia Wang and Bangxu Yin, “Perceptual Hashing-Based Robust Image Authentication Scheme for Wireless Multimedia Sensor Networks”, International Journal of Distributed Sensor Networks, Volume 2013, Article ID 791814, 9 pages.
[6] Xiaodi Hou and Liqing Zhang, “Saliency Detection: A Spectral Residual Approach”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(11):1255–1259, 1998.
[7] A. Swaminathan, Y. Mao, and M. Wu, “Robust and secure image hashing,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp.216–230, Jun. 2006.
[8] Ankayarkanni, B., and A. Ezil Sam Leni. "A new statistical rule model for image retrieval system of remote sensing images." In Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on, pp. 1-5. IEEE, 2016.
[9] D. Usha Nandini, Dr. Ezil Sam Leni, “Shadow Identification using Ant Colony Optimization”, Journal of Theoretical and Applied Information Technology, vol. 78, no. 2, pp.195-200, 2015.
[10] S. Prince Mary, Dr. E. Baburaj, “Performance Enhancement in Session Identification”, Conducted by ICCICCT, Noorul Islam University, on July 10 & 11, 2014. Published in IEEE Xplore, pgs: 837 – 840, ISBN: 978-1-4799-4191-9.