IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.
www.ijiset.com
ISSN 2348 – 7968

An Advanced Digital Image Forgery Detection via Local Binary Pattern and Haralick Features

Bini Babu
Department of Computer Science & Engineering
Sree Buddha College of Engineering
Alappuzha, India
binibabu26@gmail.com

Keerthi A. S. Pillai
Department of Computer Science & Engineering
Sree Buddha College of Engineering
Alappuzha, India
keerthias@gmail.com

***Abstract* - Nowadays, authorizing the genuineness of an image is a big challenge. For ensuring the trustworthiness of images, a secure hashing method is developed. This method detects the tampering like addition, removal and replacement of any object from the image, unusual color modifications, resizing, and image compression and especially locates the forged area. A hash sequence is generated by extracting features from reference and test image. Global features are extracted using Zernike moments representing luminance and chrominance characteristics. Texture features are extracted by dividing the image into non-overlapping blocks. Haralick features and Modified Local Binary Patterns are extracted from each block. Secret keys are introduced for hash construction. The hash is sensitive to malicious forgeries. By decomposing the hashes the type and location of forgery can be determined. The proposed method will combat the problem of image forgeries in various domains like legal services, medical images, forensics, intelligence and sports.**

Keywords - Image Forgery Detection; Zernike Moments; Local Binary Pattern; Haralick Features; Image Hash

I. INTRODUCTION

In the age of high performance digital cameras and the Internet, understanding the authenticity and validity of digital images is always a problem and challenge. Nowadays, there are several powerful high-quality image editing tools for editing digital images. Therefore it is possible for non-professional users to use these tools to change contents of digital images.

Since images are an effective and vivid communication medium for people to understand content easily by stimulating their visual system, decreasing serious vulnerabilities and increasing the credibility of digital images is of paramount importance. For humans to visually identify whether the image is original or manipulated is very difficult. Also images which are presented as court evidence must not be manipulated in any way because they lose credibility as acceptable evidence. Fig. 1. Shows two images where (a) is the original image and (b) is the forged image with an object inserted in the original image. Thus, digital image forensics is one of the latest research fields which intend to authorize the genuineness of images.

The proposed method is a robust hashing method. Hashing techniques extracts image sequences to represent

(a) Original Image (b) Tampered Image

Fig.1. An example of Original and Tampered Images to find Forgery

image contents and are suitable for image authentication. Both the global and local features of the images are extracted and combined to form the image hash. The global characteristics are represented using Zernike Moments of the luminance and chrominance components of the image. The local features extracted are the texture and position features. The images are divided into non-overlapping blocks and the local features are extracted from these blocks. By using an encryption method with secret keys hashes are created for detecting tampered images.

Various image forgery detection methods including hashing techniques have been proposed up to the time. Image authentication techniques are classified into active and passive authentication techniques. In active authentication technique prior information of the image is indispensible. While in passive authentication no prior information of the image is required, instead image itself s needed. Passive techniques are also called image forensics.

V. Monga [2] proposed a clustering based approach for image hashing. A histogram based scheme was developed [3] which extracts only global features of the image. A global method of Nonnegative Matrix Factorization [4] was advancement in the field of digital forensics. Digital watermarking was another technique which satisfies the property perceptual robustness [5] through local feature extraction. SIFT Harris detector was proposed [6] to identify various key points under content preserving

ISSN 2348 – 7968

operations. This method was robust against geometric attacks.

(a) Original Image (b) Tampered Image (c) Forgery Detected

Fig. 2. Authenticating a forged image (b) with a reference image (a) in the existing method (c)

II. RELATED WORK

The recent method of authenticating image genuineness was through feature extraction. The global and local features of the image were extracted and calculate the image hash sequence. The local features of the image were extracted through salient region detection. Detecting the saliency map and salient regions of an image is a less accurate method [1], even-though it has various benefits. The saliency region detection method extracts a sequence of image contents as forged area as shown in Fig. 2. Another technique proposed was extracting global, local and histogram features. All these techniques are having own advantages and disadvantages. In this paper, the proposed method is a content preserving authentication technique which is robust.

III. FEATURE EXTRACTION CONCEPTS

A. *Zernike Moments*

Zernike Moments [7], [8] are defined as projections of image function $f(x,y)$ on a class of polynomials called Zernike Polynomials. The Zernike basic function $V_{nm}(\rho,\theta)$ with order n and magnitude m is defined over a unit circle in the polar coordinates as:

$$V_{nm}(\rho,\theta) = R_{nm}(\rho)\, e^{jm\theta}, \text{ for } \rho \geq 1 \qquad (1)$$

where $R_{nm}(\rho)$ are real valued radial polynomials and θ is the azimuth angle.

The ZMs for a continuous image function is represented by:

$$Z_{nm} = \frac{n+1}{\pi} \sum_x \sum_y f(x,y) V^*_{nm}(x,y) \qquad (2)$$

The chosen value of $n = 0,1,\ldots,5$ and $0 \leq |m| \leq n$.

B. *Haralick Features*

The Haralick texture features are used for image classification [9]. These features extract texture patterns of the image. It is based on the construction of a co-occurrence matrix. This matrix will be a square matrix of dimension Ng, the number of gray levels in the image. The element (i,j) of the matrix is generated by counting the number of times a pixel with value i is adjacent to a pixel with value j. Then the value is calculated by dividing the entire matrix by

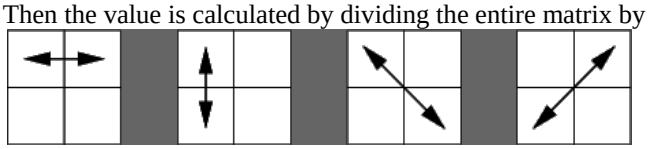

Fig. 3. Directions of adjacency used for calculating Haralick features

the total number of comparisons made. The various texture features extracted are Angular Second Moment, Contrast, Correlation, Sum of Squares, Sum Average, Sum Variance, Entropy etc [10]. The Haralick statistics are calculated for co-occurrence matrices generated using each of the four directions of adjacency which is shown in Fig. 3.

C. *Modified Local Binary Pattern*

The Local Binary Pattern (LBP) code is measured by comparing a pixel with its neighboring pixels [11]. LBP returns the local binary pattern image or LBP histogram of an image.

$$LBP_{P,R} = \sum_{P=0}^{P-1} r(g_P - g_C)2^P \qquad (3)$$

where g_C represents the grey level value of the centre pixel , g_P denotes the value f the neighboring pixels of the centre, P is the total number of neighboring pixels and R is the radius of the neighborhood.

For an image of size $I * J$, the modified LBP is measured for each pixel and histogram is developed to represent texture features.

IV. PROPOSED METHOD

The proposed technique forms the image hashes by concatenating the global and local features. The image hashes are compared for authenticating the genuineness and locating the forged area. The proposed hashing scheme is shown in Fig. 4 and the output obtained is as shown in Fig.5.

A. *Preprocessing*

The image which is stored as the reference image is first rescaled to a fixed size. The rescaling is performed through bilinear interpolation with a size factor of 256. Then the image is converted from RGB to YCbCr and the luminance and chrominance components are calculated. The components Y and $|Cb - Cr|$ are used to generate hash where $C = |Cb - Cr|$.

ISSN 2348 – 7968

B. *Feature Extraction*

In this paper of image forensics the process of image authentication is through feature extraction.

1) Global Feature Extraction:

Zernike Moments of Y and $|Cb - Cr|$ are calculated for global feature extraction. These components are converted

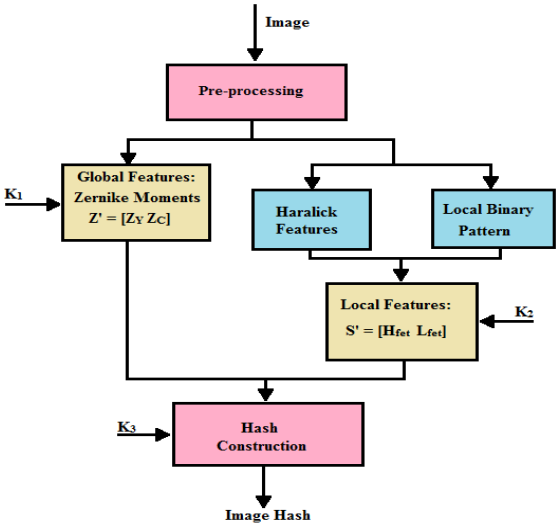

Fig. 4. Proposed Image forgery detection method

into binary by thresholds for extracting shape features exactly. The order of n could be small because shape features can be obtained from small frequency coefficients. The total Zernike moment which represents global vector is calculated as in (4).

$$Z' = [Z_Y\ Z_C] \quad (4)$$

The magnitudes of Zernike moments are rounded. A randomly generated secret key K_1 is used to form a row vector X_1, which is then encrypted to form the encrypted global vector Z.

$$Z = mod(Z' + X_1, 256) \quad (5)$$

2) Local Feature Extraction:

For local features, first the images are converted into gray and then dividing it into non-overlapping blocks. The texture and position features are extracted from each block. Local features are extracted using Haralick features and modified Local Binary Patterns. 14 features of the image are extracted using this method. The local vector is calculated as in (6).

$$S' = [H_{fet}\ L_{fet}] \quad (6)$$

Then a randomly generated secret key K_2 is used to form a row vector X_2 in $[0, 255]$. X_2 is then encrypted to form the encrypted local vector S.

$$S = mod(S' + X_2, 256) \quad (7)$$

The block size chosen is 32 for the dataset.

C. *Hash Generation:*

The global and local vectors are concatenated to form the intermediate hash

$$H' = [Z\ S] \quad (8)$$

(a) Original Image (b) Tampered Image (c) Forgery Detected

Fig. 5. Detecting forgery in the reference image in proposed method

The final hash sequence H is generated using a third pseudo randomly generated secret key K_3. The key is scrambled to form the row vector X_3. H is then calculated by performing an encryption operation.

$$H = mod(H' + X_3, 256) \quad (9)$$

An image hash without encryption is also generated as: $H" = [Z'\ S']$.

D. *Image Authentication*

In image forensics, the pre-existing image is called the reference image and the image to be authenticated is test image. For ensuring the authentication of test image, hashes have to be created for both reference and test images using above described methods. The hashes are decomposed using the secret keys and performing decryptions using Mod operators.

At the first level, the final hash H is decomposed using the secret key K_3 and the row vector X_3.While obtaining the global and local vectors through decomposition, further decompositions are made using K_2 and X_2 for local features and K_1 and X_1 for global features of each blocks. Then the regions are matched for detecting tampering. The Haralick and modified LBP features of both the images are differentiated and absolute value is calculated for determining the blocks which are tampered. For determining the exact region of forgery the images are converted into binary by removing small regions below some pixels.

The forged areas are represented by drawing the bounding boxes around the regions of tempering. Fig 4 shows the original image, tampered image and the image obtained after applying the proposed technique. This

ISSN 2348 – 7968

proposed method is a content preserving forensics method for forgery detection.

V. PERFORMANCE ANALYSIS

Performance of the proposed method is due to the combination of local and global features. The proposed technique is robust for any content preserving modifications. The method has been tested with many other images and result obtained was accurate and with less computational complexity. Since LBP gives excellent results in terms of accuracy and computational complexity. Some of the outputs obtained in Fig. 6 and Fig. 7.

(a) Original Image (b) Tampered Image (c) Forgery Detected

Fig. 6. Authenticating a forged image with a reference image in proposed method

(a) Original Image (b) Tampered Image (c) Forgery Detected

Fig. 7. Authenticating a forged image with a reference image in proposed method

VI. CONCLUSION

The proposed image forensics technique develops an imaging hashing method by extracting local and global features. Zernike Moments are used to form global vector. The local vector is formed using Haralick Features and Modified Local Binary Pattern (MLBP). The hash formed by concatenating these vectors is used for authenticating the genuineness of images. The proposed technique is a content preserving authentication technique. This method detects image resizing, compression, the tampering which changes the contents of the image etc. The method accurately determines the specific area of forgery. Performance analysis of this technique, to which amount of content preserving modification, the proposed technique is robust.

Acknowledgment

At first, we are grateful to the Almighty for giving us idea, brave and intelligence to select an interesting and realistic work. We take this opportunity to thank everyone who directly or indirectly helped us throughout this work. Also we would like to thank all the technological experts who researches in digital image forensics for helping us in implementing new methods.

References

[1] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao," Robust Hashing for Image Authentication Using Zernike Moments and Local Features,"IEEE Trans.Inf.Forensics Security, vol, no.8, January 2013.

[2] 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.

[3] 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.

[4] K. Fouad and J. Jianmin, "Analysis of the security of perceptual image hashing based on non-negative matrix factorization," IEEE Signal Process. Lett., vol. 17, no. 1, pp. 43–46, Jan. 2010.

[5] 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.

[6] X.Lv and Z.J. Wang, "Perceptual image hashing based on shape contexts and local feature points", IEEE Trans. Inf. Forensics Security, vol.7, no.3, Jun,2012

[7] S. Li, M. C. Lee, and C. M. Pun, "Complex Zernike moments features for shape-based image retrieval," IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 39, no. 1, pp. 227–237, Jan. 2009.

[8] Z. Chen and S. K. Sun, "A Zernike moment phase based descriptor for local image representation and matching," IEEE Trans. Image Process., vol. 19, no. 1, pp. 205–219, Jan. 2010.

[9] Eizan Miyamoto and Thomas Merryman Jr.,"Fast Calculation of Haralick Texture Features".

[10] Robert M. Haralick, K, Shanmugam and, Itshak Dinstein, "Texture features for Image Classification", IEEE Trans. on Systems, Man and Cybernetics, vol. SMC-3, No. 6, November 1973, pp 610-621.

[11] Brian O'Connor and Kaushik Roy,"Facial Recognition using Modified Local Binary Pattern and Random Forest ", International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 4, No. 6, November 2013