IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. III (Sep – Oct. 2014), PP 13-19
www.iosrjournals.org

An Improved Hashing Method for the Detection of Image Forgery

Anupama K. Abraham, Rosna P. Haroon
Dept. of CSE Ilahia College Of Engineering and Technology, Kerala,India
Assistant Professor Dept. of CSE Ilahia College of Engineering and Technology, Kerala, India

***Abstract**: Detection of image forgery is always a crucial factor in image forensic and security applications. Usually this detection is possible with the help of local or global features of an image. We can ensure the credibility of an image with a hashing method by fusing local and global features together. So that it is possible to detect even sensitive image forgeries. Here, we are proposing an improved hashing method for the detection of Copy-move forgery detection and Spliced Image Detection.*
***Key words:** Zernike moments,Local features, Saliency Map,*

I. Introduction

With the development of the Internet and multimedia processing techniques, more and more digital media products become available through different online services and easy to distribute illegal copy. Digital hashing has been introduced as a potential solution for tracing the unauthorized use of digital media since the traditional cryptography hash functions can not satisfy the requirements of content authentication because the cryptographic hash is sensitive to every single bit of input. Image hash should be unique, robust and short in length.

So many techniques are introduced with Image Hashing Development. Image hash is developed as a result of feature extraction and the coding of intermediate result. That hash is useful in image databases, watermarking and authentication [2]. In a robust histogram based image hashing scheme, the robustness of the hash against geometric deformations is achieved by using the histogram shape invariance. Real-world image authentication is not possible with this approach [3].

A perceptual image hashing scheme uses a non-negative matrix factorization to extract image features. This is not good for detection sensitivity against less obvious tampering [4]. A new algorithm is created for generating an image hash based on Fourier transform features and controlled randomization. This method provides excellent security and robustness through the rotation invariance of the Fourier-Mellin transform and controlled randomization during image feature extraction [5]. The security of perceptual image hashing scheme analyzed based on non-negative matrix factorization. This paper theoretically demonstrates that if the technique uses different secret keys in subsequent stages, the first key plays an essential role to secure the hashing system [6].

A new framework is proposed to perform multimedia forensics by using compact side information to reconstruct the processing history of a multimedia document. This method is robust against images that have undergone multiple operations [7]. Forensic hash can be constructed based on visual words representation. This method of hash construction achieves more robust and accurate forensic analysis than prior work. But this is not much reliable on tampering detection capability [8]. These methods are either based on global or local features.

There is another method Robust Hashing for Image Authentication using Zernike moments and Local features. Here the hash is a combination of global and local features of an image. The global features are represented by the Zernike moments representing the luminance and chrominance characterestics of the image. Position and texture information of salient regions in the image represents the local features. Four types of image forgeries, removal, insertion, and replacement of objects, and unusual color changes can be identified by this method. Threshold values determines the authenticity of the image. Hash performance is measured by the distance metrics.

Here we are discussing an Improved Hashing Method for the Detection of Image Forgeries. Apart from the forgeries removal, insertion, replacement of objects and unusual color changes, the different image forgeries copy move attack, splicing attack, and multiple cloning can be identified by this method. The hashing technique is improved by considering multiple texture features and color properties. Authentication of videos can be conducted by the use of this hashing technique is under discussion.

II. Related Works

A robust hashing method is developed for detecting image forgery including removal, insertion, and replacement of objects, and abnormal color modification, and for locating the forged area. Both global and local

features are used in forming the hash sequence. The global features are based on Zernike moments representing luminance and chrominance characteristics of the image as a whole. The local features include position and texture information of salient regions in the image. Secret keys are introduced in feature extraction and hash construction. While being robust against content-preserving image processing, the hash is sensitive to malicious tampering and, therefore, applicable to image authentication. The hash of a test image is compared with that of a reference image.When the hash distance is greater than a threshold and less than , the received image is judged as a fake. By decomposing the hashes, the type of image forgery and location of forged areas can be determined.[1]

A perceptual image hash function maps an image to a short binary string based on an image's appearance to the human eye. Perceptual image hashing is useful in image databases, watermarking, and authentication. Image hashing is decoupled into feature extraction (inter- mediate hash) followed by data clustering. The decision version of this clustering problem is NP complete. Then, for any perceptually significant feature extractor, here proposes a polynomial-time heuristic clustering algorithm that automatically determines the final hash length needed to satisfy a specified distortion. Based on the proposed algorithm, there developed two variations to facilitate perceptual robustness vs. fragility trade-offs. Validates the perceptual significance of this hash by testing under Stirmark attacks. Finally, develop randomized clustering algorithms are developed for the purposes of secure image hashing. This is a scheme for secure hashing. [2]

A robust image hash algorithm is proposed by using the invariance of the image histogram shape to geometric deformations. Robustness and uniqueness of the 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 function has a satisfactory performance to various geometric deformations, and is also robust to most common signal processing operations , the use of Gaussian kernel low-pass filter in the preprocessing phase.

The histogram-based hash function has a satisfactory performance to various geometric deformations and robust to most common signal processing operations. The hash function is simple to estimate the first key based on the observation of image/hash pairs. The key has been shown to be accurately estimable when it is reused several times on images with different visual content. As pointed out in the literature, this key disclosure problem is associated with all perceptual image hashing techniques due to the design requirements on robustness. The use of a secret key combined with image-dependent keys can enhance security in the sense that the information leakage about the final key will be smaller due to its dependence on the image content [6].

Digital multimedia such as images and videos are prevalent on today's internet and cause significant social impact, which can be evidenced by the proliferation of social networking sites with user generated contents. Due to the ease of generating and modifying images and videos, it is critical to establish trustworthiness for online multimedia information. This paper proposes a new framework to perform multimedia forensics by using compact side information to reconstruct the processing history of a multimedia document. This framework is referred as FASHION, standing for Forensic HASH for informatION assurance. As a first step in the modular design for FASHION, new algorithms are proposed based on Radon transform and scale space theory to effectively estimate the parameters of geometric transforms and detect local tampering that an image may have undergone. The FASHION framework is designed to answer a much broader range of questions regarding the processing history of multimedia data than simple binary decision from robust image hashing, and also offers more efficient and accurate forensic analysis than multimedia forensic techniques that do not use any side information [7]. This analysis can provide accurate estimates of the parameters of geometric transforms that the image has undergone.

Forensic hash is a short signature attached to an image before transmission and acts as side information for analyzing the processing history and trustworthiness of the received image. Forensic hash can be constructed based on visual words representation. Here encodes SIFT features into a compact visual words representation for robust estimation of geometric transformations and propose a hybrid construction using both SIFT and block-based features to detect and localize image tampering. This hash construction achieves more robust and accurate forensic analysis than prior work [8].

Shape is a fundamental image feature used in content-based image-retrieval systems. A robust and effective shape feature, which is based on a set of orthogonal complex moments of images known as Zernike moments (ZMs). As the rotation of an image has an impact on the ZM phase coefficients of the image, existing proposals normally use magnitude-only ZM as the image feature. This paper compares, by using a mathematical form of analysis, the amount of visual information captured by ZM phase and the amount captured by ZM magnitude. This analysis shows that the ZM phase captures significant information for image reconstruction. Therefore propose combining both the magnitude and phase coefficients to form a new shape descriptor, referred to as invariant ZM descriptor (IZMD). The scale and translation invariance of IZMD could be obtained by pre normalizing the image using the geometrical moments. To make the phase invariant to rotation, here performs a phase correction while extracting the IZMD features. Experiment results show that the proposed

shape feature is, in general, robust to changes caused by image shape rotation, translation, and/or scaling. The proposed IZMD feature also outperforms the commonly used magnitude-only ZMD in terms of noise robustness and object discriminability.

Tries to find out the relative importance of the phase and magnitude of ZM in representing an image by comparing the distortion of reconstructed images introduced by a small perturbation of a phase coefficient, with the distortion introduced by an equivalent small perturbation of a magnitude coefficient. As phase is not rotation invariant, here proposes a method to perform phase correction to produce rotation invariant phase coefficients. By combining the ZM magnitude and the corrected phase, we form an invariant ZMD (IZMD). The scale and translation invariance of IZMD could be obtained by pre normalizing the image using the geometrical moments. As demonstrated in the experiments, IZMD is more robust than ZMD to changes caused by image scaling and rotation; it could represent images more accurately and is also
more robust to image noise [9].

The representation and matching power of region descriptors are to be evaluated. A common set of elliptical interest regions is used to evaluate the performance. The elliptical regions are further normalized to be circular with a fixed size. The normalized circular regions will become affine invariant up to a rotational ambiguity. Here, a new distinctive image descriptor to represent the normalized region is proposed, which primarily comprises the Zernike moment (ZM) phase information. An accurate and robust estimation of the rotation angle between a pair of normalized regions is then described and used to measure the similarity between two matching regions. The discriminative power of the new ZM phase descriptor is compared with five major existing region descriptors (SIFT, GLOH, PCA-SIFT, complex moments, and steerable filters) based on the precision-recall criterion. The experimental results, involving more than 15 million region pairs, indicate the proposed ZM phase descriptor has, generally speaking, the best performance under the common photometric and geometric transformations. Both quantitative and qualitative analyses on the descriptor performances are given to account for the performance discrepancy. First, the key factor for its striking performance is due to the fact that the ZM phase has accurate estimation accuracy of the rotation angle between two matching regions. Second, the feature dimensionality and feature orthogonality also affect the descriptor performance. Third, the ZM phase is more robust under the nonuniform image intensity fluctuation [10]. New region descriptor is robust to common photometric and geometric transformations but the applications such as textured image classification and image retrieval is currently underway.

A simple method for the visual saliency detection is independent of features, categories, or other forms of prior knowledge of the objects. By analyzing the log-spectrum of an input image, extracts the spectral residual of an image in spectral domain, and propose a fast method to construct the corresponding saliency map in spatial domain. Tests this model on both natural pictures and artificial images such as psychological patterns.[11]

III. Proposed System

The proposed method consists of the detection of the image forgeries such as splicing attack and copy move attack. In copy-move attack, a part of the image is copied and pasted somewhere else in the image with the intend to cover an important image feature. Simple joining of fragments of two or more different images leads to the splicing attack. The figure shows the architecture of the proposed method.

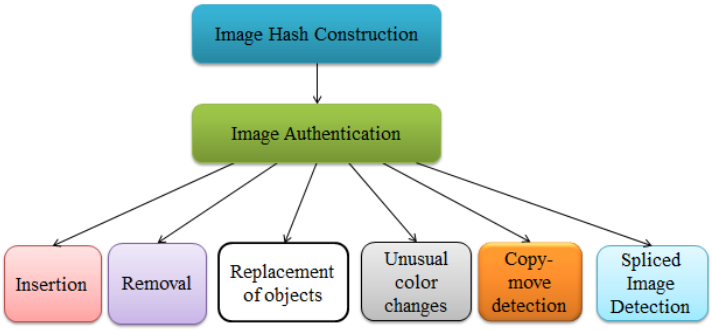


Figure 1. The proposed architecture

The proposed method starts with the hash construction of both the trusted image and the tested image. Then the two hashes are compared to find the authenticity of the tested image in the authentication phase. After the authentic identification we are moving into the detection of forgery attacks. The peculiarity we are focusing is any type of forgery can be identified by our system.

Image forgery methods including removal, insertion, replacement of objects and unusual color changes attacks are described in paper[1]. The remaining possible attacks namely spliced forgery and copy move forgery are dealing herewith. The architecture is as shown in figure 4.1.

Spliced attacks can be identified with the help of CRF Estimation. For that, the system will computes the geometry invariants from the pixels within each region. Then it is possible to estimate Camera Response Function from these geometry invariants. The consistency of CRF's can be checked using cross- fitting techniques. If the data from a certain region fits well to the CRF from another region, this image is likely to be authentic. Otherwise, if it is fits poorly, then the image is very likely to be spliced.

Matching among the hashed image and the test image is used for the task of determining Copy-move attack. The copied part has basically the same appearance of the original one, thus keypoints extracted in the forged region will be quite similar to the original ones. Therefore, matching between the hashed image and the test image helps to detect the copy-move attack. After this, reconstructing the original image by the help of precalculated shares.

IV. Solution Methodology

In this section we present the global and local feature extraction for the construction of image hash for the authentication process. The authentication process decomposes the hash and performs the salient region matching inorder to classify the possible forgeries like insertion, removal, replacement of objects,unusual color changes, spliced image forgery and copy-move forgery.

A. HASH Function

In the proposed algorithm, the hash is produced by concatenating global and local vectors. The global vector is based on Zernike moments representing the luminance and chrominance characteristics of the image as a whole. The local features include position and texture information of salient regions in the image.
The Zernike moments can be calculated using the algorithm :

a) Select the values for order 'n' and the repetition 'm' for the Zernike Moment.
b) Calculate the Zernike Polynomial of order 'n' and repetition 'm'.
c) Multiply the digital image with the Zernike Polynomial.
d) Take the summation over the entire image.

Magnitude of the Zernike moments are rounded and used to form a global vector $Z` = [Z_Y Z_C]$. The position and texture features together makes the local vector. Position features can be obtained by calculating the Salient regions.
Salient Region Detection can be obtained by the algorithm :

a) Calculate the log spectrum of the image.
b) Find the redundant information exists in the image.
c) Obtain the spectral residual by subtracting redundant information from the log spectrum of the image.
d) Calculate the saliency map by inversely Fourier transforming the spectral residual.

The texture features includes Coarseness, Contrast, Correlation and Inverse difference moment.
The algorithm used to find the Coarseness around a pixel is :

a) Select a pixel at (x,y).
b) Averaging the 2^k x 2^k neighborhood pixels of the above selected pixel . where k=1,2,…5
c) Find the average values of non overlapping neighborhoods on opposite sides of the selected pixel in horizontal and vertical directions.
d) Calculate the difference between the pairs of average values.
e) Find the size that leads to the highest difference value.
f) Take average on the highest difference value over a region in order to obtain Coarseness.

The algorithm for obtaining the Contrast is :

a) Calculate the variance of the gray values of the image.
b) Calculate the fourth order moment of the gray values of the image.
c) Multiply the calculated variance and the fourth-order moment within the region.

Correlation can be found by :
$(\Sigma_i \Sigma_j (ij)\, p(i,j) - \mu_x \mu_y) / (\sigma_x \sigma_y)$

Inverse Difference Moment is obtained from :
$\Sigma_i\Sigma_j (1/(1+[i-j]^2))P(i,j)$

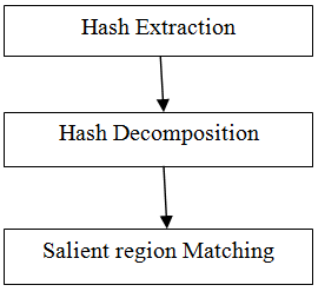
Then, K largest salient regions are detected from the luminance image. Here, K is set as 6 as a reasonable trade-off. The texture features of each salient region including coarseness and contrast , Correlation and Inverse Difference Moment are computed and rounded to give a 6-element vector t(k) (k=1,….,6). The position and texture vectors of all salient regions together form a local feature vector S`= [PT]. The global and salient local vectors are concatenated to form an intermediate hash, namely H`= [ZS]

B. Image Authentication

The next process is the image authentication. The steps needed for the authentication process are listed below :

a) The hash of a received image to be tested (H1) is extracted.
b) Decompose the reference hash(H0) into Global and Local features.
c) Check if the salient regions found in the test image P1 match those in the trusted image P0.
d) Hash distance Calculation.

The block diagram of image authentication is shown below :



C. Forgery Classification

Forgery classification includes classifying the possible forgeries as removal, insertion and replacement of objects, and unusual color changes. For that, Decode H0(hash of the test image) and H1(hash of the reference image) into components representing global and local features, and find the number of matched salient regions R and the numbers of salient regions in the reference N0 and test images N1,then check some conditions:

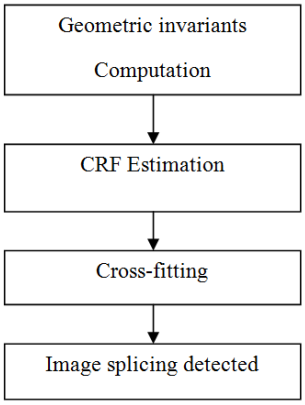
a) If N0>N1 = R some objects have been removed from the received test image.
b) If N1>N0 = R the test image contains some additional objects.
c) If N0 = N1 = R check the luminance and chrominance components and calculate
   i. $\delta Z_C = ||Z_{C1} - Z_{C0}||$, $\delta Z_Y = ||Z_{Y1} - Z_{Y0}||$
   ii. If δZ_C is greater than δZ_Y by a threshold τc , the test image contains substantial color changes.
d) If N1 =N0 = R and (δZ_C - δZ_Y) is less than τc, the test image contains replaced objects because in this case luminance changes are dominant.
e) If N0 > R and N1> R , some of the salient regions are not matched.

D. Spliced Image Detection

In the proposed method, suspicious splicing areas are identified by computing the geometry invariants from the pixels within each region, and then estimate the camera response function (CRF) from these geometry invariants.
The algorithm for the spliced image detection is :

a) Compute the Geometry Invariants.
b) Divide the image into three regions.
c) Extract the points which satisfies the locally planar condition.
d) Compute their gamma transform.
e) Estimate CRF.
f) Fed the CRF values into the SVM to classify authentic and spliced.

The block diagram is shown below :

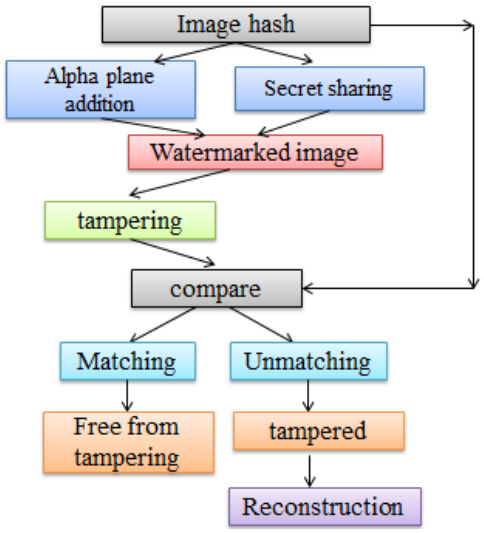


E. Copy-move Forgery Detection

Algorithm for copy-move detection :

a) Compute the image hash and attach it to the alpha plane.
b) Extract the shares from the hashed image and embed it to the alpha plane for producing the watermarked image .
c) Perform copy-move forgery on the watermarked image.
d) Compare the stego image with the precomputed hash and find the tampering.
e) Reconstruct the original image using the precalculated shares.

The block diagram is shown below :



V. Conclusion And Future Work

We have presented in the paper an improved hashing method which can effectively detect copy-move forgery and image splicing. Here, Camera Response Function is used to detect splicing forgery in images. This detection is based on geometry invariants that relate directly to the CRF. If an image consists of regions from more than one camera is determined by cross-fitting. We propose a method which uses the image hashing for the detection of copy-move forgery in images. Shares are extracted for reconstructing the original image. For future work, we he are going to explore other kinds of image forgeries and extend our scheme to detect the Copy-move forgery in videos with minimal time.

Acknowledgment

The authors wish to thank the Management and Principal and Head of the Department(CSE) of Ilahia College of Engineering and Technology for their support and help in completing this work.

References

[1] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, "Robust Hashing for Image Authentication Using Zernike Moments and Local Features" ieee transactions on information forensics and security, vol. 8, no. 1, 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] 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.

[5] A. 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.

[6] 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.

[7] W. Lu, A. L. Varna, and M. Wu, "Forensic hash for multimedia information," in Proc. SPIE,Media Forensics and Security II, San Jose, CA, Jan. 2010, 7541.

[8] W. Lu and M.Wu, "Multimedia forensic hash based on visual words," in Proc. IEEE Conf. on Image Processing, Hong Kong, 2010, pp. 989–992.

[9] 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.

[10] 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.

[11] X. Hou and L. Zhang, "Saliency detection: A spectral residual approach," in Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition, Minneapolis, MN, 2007, pp. 1–8.