International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Humming Bird (01st March 2014)

RESEARCH ARTICLE OPEN ACCESS

Adaptive Gabor Wavelet and Zernike Moment Based Hashing for Image Authentication

Akshara Anand.S.D S.Gayathri
1Akshara Anand.S. D. Author is currently pursuing M.Tech (Information Technology) in Vins Christian College of Engineering, e-mail:aksharasd5@gmail.com.
2S Gayathri . Assistant professor of Information Technology in Vins Christian college of Engineering

Abstract:
The great advancement in image processing demands a guarantee for assuring integrity of images. For detecting image forgery which includes removal, insertion, and replacement of objects, abnormal color modification and for locating the forged area an robust hashing method is developed. Gabor wavelet transform is an efficient method for local feature extraction especially texture features. In medical applications efficient texture extraction can easily distinguish normal tissue from abnormal tissue and is possible only through Gabor wavelet transform approach. Global feature extraction means extracting global features from global perspective. Global features are based on Zernike moments represents luminance and chrominance characteristics of image. Local features are extracted from local regions but contain much more information. To extract certain features from the image data to generate image hash a secret key is used. The type of image forgery and location of forged areas can be determined by decomposing the hashes.Implementation results confirm that our proposed system has higher hashing efficiency when compared with the previous methods.

Keywords— Gabor wavelets transform, Global features, Local features, Image hash, Zernike moments

1. INTRODUCTION

More and more digital images are being created and used every day due to the popularity of digital technology. However they are susceptible to modification and forgery. When the digital image contains important, their credibility must be ensured. So it is necessary to have reliable image authentication system Robustness and securities are two important design criteria for image hash functions. By robustness, we mean that when the same key is used, perceptually similar images should produce similar hashes. Here, the similarity of hashes is measured in terms of some distance metric, such as the Euclidean or Hamming distance. A.Swaminathan [1] proposed an image hash method is based on rotation invariance of Fourier-Mellon transform features. Their method is good to filtering operations, geometric distortions, and various content-preserving manipulations. Using image hashing for multimedia searching operations is computationally highly efficient where the hash has much smaller size with respect to original data[2]. The method proposed in [2] robust against geometric transformation and normal image processing operations, and can detect content changes in relatively large areas.

The increasing availability of multimedia data has led to the growth of tools to manipulate digital multimedia information. To ensure trustworthiness, multimedia authentication techniques have emerged to verify content integrity and prevent forgery [3], [4]. Monga[5] develop a two-step framework that includes feature extraction (intermediate hash) and coding of the intermediate result to form the final hash.

. In [10] , the authors proposed to extract content-based features from the DWT approximation sub band to generate two complementary watermarks: edge-based watermark to detect the manipulations and content –based watermark to localize tampered regions. In watermarking scheme for image authentication local feature is usually computed and embedded locally, just like the algorithms in [11] in order to locate the tampered areas, However, restricted by the embedded capacity and invisibility of the watermarked image, the watermark generated by local feature should be low bitrates. Thus the feature will not have the first property listed above and the algorithm is susceptible to attack.

In section II global and local feature extractors are briefly described. The section III presents proposed hashing scheme. The section IV presents performance studies.

The section V presents conclusion.

II. REVIEW OF FEATURE EXTRACTORS

A. ZERNIKE MOMENTS

Zernike moments are selected as feature extractor due to its robustness to image noise, geometrical invariants and orthogonal property. Zernike moments are used efficiently as shape descriptors of image objects that cannot be defined by a single outline. The equation of Zernike moment is represented in (1) Zernike moments can represent the properties of an image with no redundancy or overlap of information between the moments. Zernike moments are dependent on the translation and scaling moments of the object. Zernike moments are used for extracting global features of image such as chrominance and luminance characteristics.

Zernike moments (ZM) of order n and repetition m of a digital image I(p,θ)

$$Zn,m = \frac{n+1}{\pi} \sum_{(\rho,\theta)\in unitdisk} \sum I(p,\theta)\, V^{*}_{n.m(\rho,\theta)} \qquad (1)$$

Where $V_{n,m\,(\rho,\theta)}$ is a Zernike polynomial of order n. Magnitudes of the Zernike moments are rounded and used to form a global vector, Z´=$[Z_Y\ Zc]$.

B. GABOR WAVELET TRANSFORM

Gabor wavelet transform is one of the most effective feature extraction techniques for textures. Feature extraction is a special form of reduction. Transforming the input data into the set of features is called feature extraction. Feature extraction involves simplifying the amount of resources required to describe a large set of data accurately. The multi-resolution and multi-orientation properties of the Gabor wavelet transform makes it a popular method for feature extraction.

III. PROPOSED HASHING SCHEME

In this section, we describe the proposed image hashing scheme and the procedure of image authentication using the hash. The hash is formed from Zernike moments to represent global properties of the image, and the GWT to represent local properties of image especially texture features.

A. IMAGE HASH CONSTRUCTION

The image hash generation procedure includes the following
steps.

1) *Preprocessing:*

The aim of pre-processing is an improvement of the image data that suppresses undesired distortions or enhances some image features relevant for further processing and analysis task. In this paper, it will be presented that the image is first rescaled to a fixed size with bilinear interpolation, and converted from RGB to the YCbCr representation. YCbCr, Y′CbCr, or Y Pb/CbPr/Cr, also written as YC$_B$C$_R$ or Y′C$_B$C$_R$, is a family of color spaces . Y′ is the luma component and C$_B$ and C$_R$ are the blue-difference and red-difference Chroma components. Y′ (with prime) is distinguished from Y, it sents luminance means that light intensity is ded based on gamma corrected RGB primaries. Fig 1 color image and its Y,CB and CR components.

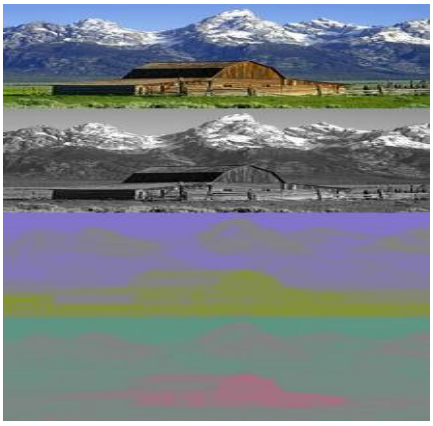


Fig 1. A color image and its Y,CB and CR components.

Image pre-processing can significantly increase the reliability of an optical inspection. The most obvious and common way to change the size of an image is to resize or scale an image. Scaling is a non-trivial process that involves a trade-off between efficiency, smoothness and sharpness. Fig 2a and 2b shows original and resized image respectively.

2) Global Feature Extraction:

Global features are extracted from global perspective. These content are usually on macro level. Consider image as whole and then extract features such as luminance and chrominance. Luminance is a photometric measure of the luminous intensity per unit area of light travelling in a given direction. Chrominance (Chroma or C for short) is the signal used in video systems to convey the color information of the picture. Zernike moments are used for generating global features which is then scrambled with key. Zernike moments are the mappings of an image onto a set of complex Zernike polynomials. Fig 3 shows proposed image hashing method. Zernike moments are selected as feature extractor due to its robustness to image noise, geometrical invariants and orthogonal property. Zernike moments are often used efficiently as shape descriptors of image objects. Magnitudes of the Zernike moments are rounded and used to form a global vector, $Z'=[Z_Y\ Zc]$. Magnitude represents size of objects especially mathematical object, a property by which the object can be compared as larger or smaller than other objects of the same kind of object. A secret key K1 is generated from pseudo-random generator .The encrypted global vector Z is obtained by scrambling with key K1

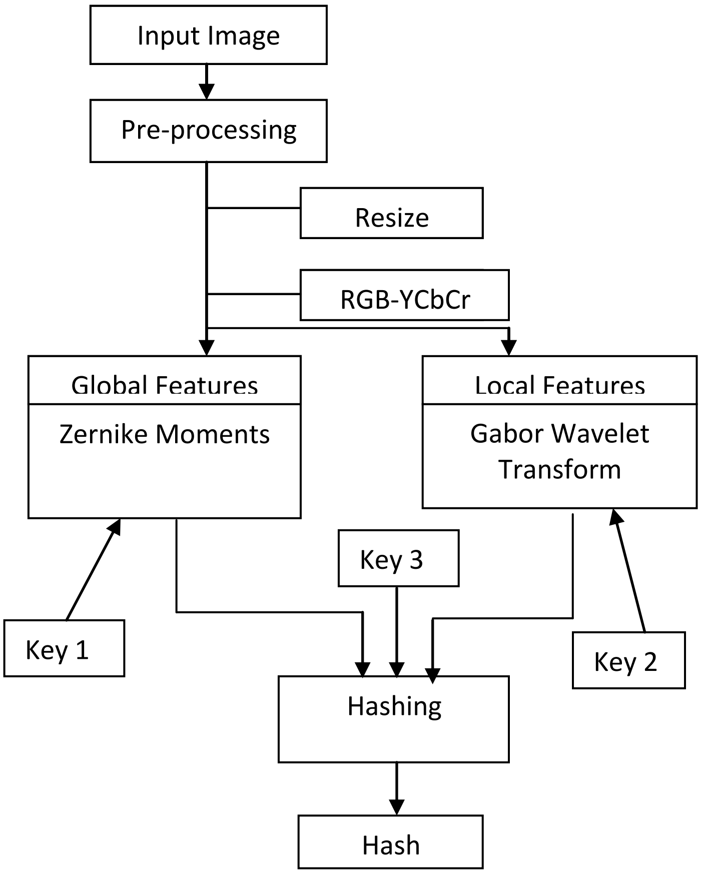


Fig 3. Block diagram of the proposed image hashing method

3) Local Feature Extraction:

Feature represents piece of information which is most important for solving the computational task related to a certain kind of applications. Features can refer to the result of a general neighborhood operation (feature extractor or feature detector) applied to the image. Position and texture features are mainly considered as local features. Saliency map and saliency region are shown in fig 6. For local feature extraction salient regions of images are first considered and then apply Gabor Wavelet Transform method for feature extraction especially texture feature extraction. Texture means the regular repetition of an element or pattern on a surface.Texture analysis plays an increasingly important role in computer vision.

The Gabor wavelets are usually called Gabor filters in the scope of applications. The Gabor wavelets could not only be used for feature extraction for face images, but also for other images such as landscape images, textures etc. Fig 4 shows texture representation. The position/size and texture of all salient regions together form a local feature vector S’=[PT]. A secret key K2 is used to generate encrypted local vector S .

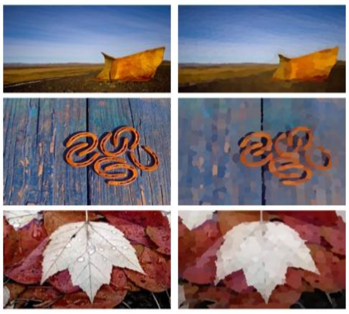


Fig 5a. Original image

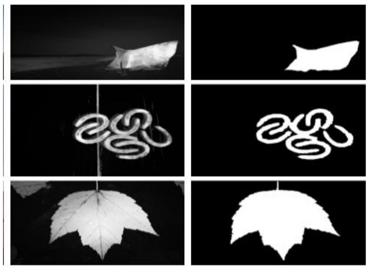
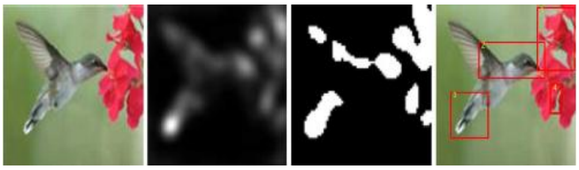


Fig 5b : Saliency region of image



(a) (b) (c) (d)

Fig 6 . Salient region detection (a) Original Image

(b) Saliency map (c) Salient region

(c) Four rectangles

4) Hash Construction:

The global and local vectors are concatenated to form an intermediate hash which is then pseudo-randomly scrambled based on secret key K3 to produce final hash sequence. The hash produced is 560 bits long.

B. FORGERY CLASSIFICATION AND LOCALIZATION:

Having found that a test image is a fake, the next job is to locate the forged region and tell the nature of forgery. Four types of image forgery can be identified: removal, insertion and replacement of objects, and unusual color changes. Fig 8, 9 and 10 shows forgery localization.

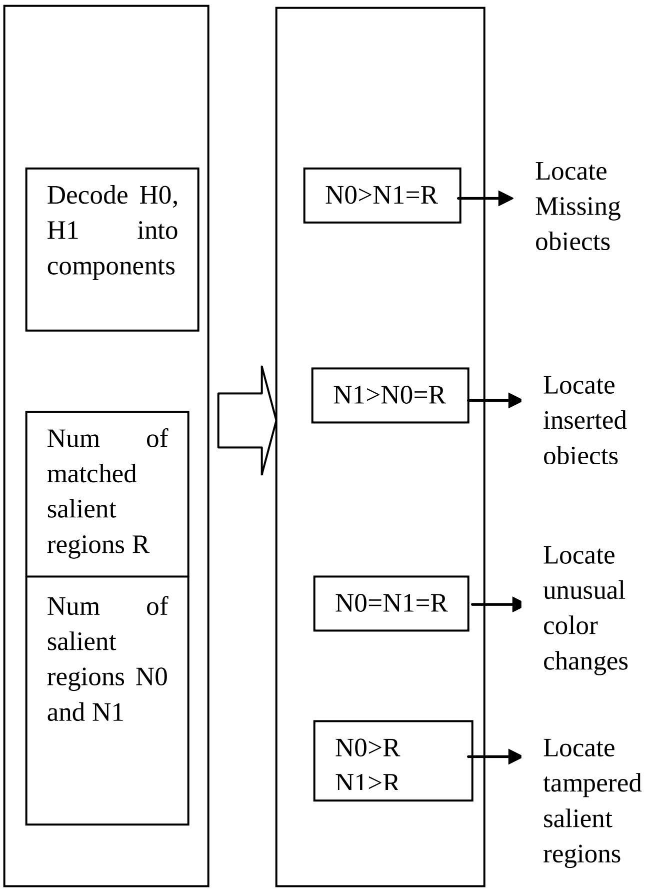

Decode H0, H1 into components
Num of matched salient regions R
Num of salient regions N0 and N1
N0>N1=R
Locate Missing obiects
N1>N0=R
Locate inserted obiects
N0=N1=R
Locate unusual color changes
N0>R N1>R
Locate tampered salient regions

Fig 7 : Forgery classification and localization

Decode H0 and H1into components representing global and local features, and find the number of matched salient regions R and the numbers of salient regions in the reference and test Images, N0 and N1.

1) If N0>N1=R, some objects have been removed from the received test image. Positions of the missing objects are located by comparing the saliency indices.

2) If N1>N0=R , the test image contains some additional objects whose positions are located by comparing the saliency indices.

3) If N0=N1=R , check the luminance and chrominance Components in the Zernike moments .

4) If N0>R and N1>R , some of the salient regions are not matched. Mark the mismatched salient regions in the test image as being tampered.

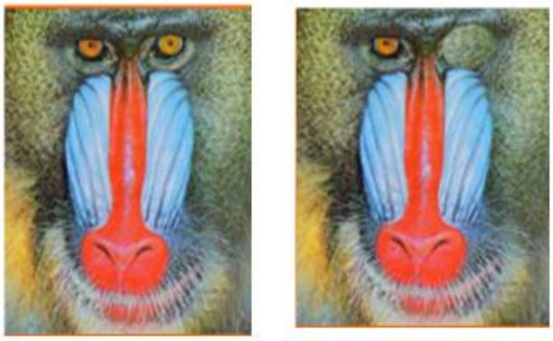


Fig 8: Examples of original and tampered im

IV.EXPERIMENTAL RESULTS

A. FORGERY DETECTION CAPABILITY

The proposed method can differentiate similar (i.e., perceptually the same), forged, and different images. A qualitative comparison between the proposed method and methods is given in Table I, showing good overall performance of the proposed method, which generates hashes with shortest length, is robust against several normal processing manipulations, and can detect and locate small area tampering. The hash of [7] is robust against slight cropping but not to rotation even if the angle is small because it is based on pseudo-randomly selected sub images, which is changed after rotation so that the hash will also be changed. The methods of [10] and [7] are not designed to localize forgery. Cropping that changes the image's geometrical center will cause significant differences in the Zernike moments, and large-angle rotation will affect the saliency-related local features. Performance of the proposed method is basically due to the combination of global and local features.

B. COMPUTATION COMPLEXITY

To compare computation complexity of the different methods, we consider average time consumed in calculating
image hashes on a desktop computer with Dual Core 2.8-GHz CPU and 2 GB RAM, running Mat lab. Performance of the proposed method is basically due to the combination of global and local features. Table I shows comparison of hash
performance. The average time of the proposed method is 2.7 s, and those of [3] and [7] are 2.98 s and 1.43 s respectively.

TABLE 1
COMPARISON OF HASH PERFOMANCE

	NMF method	SVD method	Wavelet based method	Proposed method
Features used	Global	Local	Local	Global and local features
Robust against JPEG coding and additive noise	Yes	Yes	Yes	Yes
Robust against small-angle rotation	No	Yes	No	Yes
Robust against slight cropping	No	Yes	No	Yes
Ability to detect small area forgery	Yes	No	Yes	Yes
Ability to locate forged regions	No	No	Yes	Yes

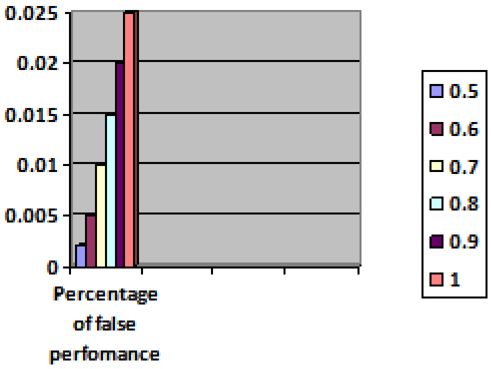


Fig 12 .Tampering localization performance

V. CONCLUSION

In this paper, an image hashing method is developed using both global and local features. The global features are based on Zernike moments representing the luminance and chrominance characteristics of the image as a whole. The local features are extracted using Gabor wavelet transform representing position and texture information of in the image. Hashes produced with the proposed method are robust against common image processing operations including brightness adjustment, scaling, small angle rotation, and JPEG coding and noise contamination. The hash can be used to differentiate similar, forged, and different images. At the same time, it can also identify the type of forgery and locate fake regions containing salient contents. In the image authentication, a hash of a test image is generated and compared with a reference hash. When the hash distance is greater than the threshold but less than the received image is judged as a fake. The method proposed in is used due to its acceptable accuracy and computation complexity.

REFERENCES

[1] 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.

[2] 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.

[3] I. J. Cox, M. L. Miller and J. A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers Inc., San Francisco, 2001.

[4] M. Wu and B. Liu, Multimedia Data Hiding, Springer-Verlag, 2002.

[5] 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.

[6] V. Monga and M. K. Mihcak, Robust and secure image hashing via non-negative matrix factorizations, IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 376- 390, 2007.

[7] 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.

[8] J.Dittmann, “Content-fragile Watermarking forImage Authentication”, Security and Watermarking , 2001.

[9] F. Ahmed, M. Y. Siyal, and V. U. Abbas, “A secure and robust hashbased scheme for image authentication,” Signal Process., vol. 90, no.5, pp. 1456–1470, 2010.

[10] X.Xin and R.Chang, “Image authentication and tamper detection using two complementary watermarks”, Proc.of Int.Conf.on Image Processing,2009,pp.1-11,2005.

[11] R.Radhakrishnan and N.Memon, “On the security of the SARI image authentication system”,Proc.IEEE Int.Conf.on Image Processing,2002,vol.2,pp.901-904.

[12] R. Venkatesan, S. M. Koon, M. H. Jakubowski Moulin, Robust Image Hashing," Proc. of IEEE Int. Conf. on Image Processing, vol. 3, pp. 2000.