DETECTION TECHNIQUE FOR IMAGE FORGERY FROM GLOBAL AND LOCAL FEATURES USING HASHES

K.Hemalatha,
M.Tech (DECS) Student,
Dept. of ECE
DECS, AITS
Tirupati, India

M.Anitha,
Assistant professor
Dept. of ECE
AITS
Tirupati, India

N.Pushpalatha
Assistant professor
Dept. of ECE
AITS
Tirupati, India

Abstract-A defective method or a robust hashing method is developed for detecting forgery which includes removal, insertion and replacement of objects and abnormal color modifications and locating the forged area, and tells the nature of forgery. This undesirable method is used both globally and locally. The local feature represents position and texture information of salient regions in the image, and its generates secret keys in the image. The global features are based on Zernike moments representing luminance and chrominance characteristics of the image as a whole. The hash test is compared with that of reference image. When the hash distance is different from the entrance values T_1 and T_2 the received image is judged as fake. T_1 andT_2 represent the threshold values. By decomposing the hashes the forgery and location can be determined. The experimental results are presented to producing favorable result effectiveness of the method.

KEYWORDS: image hash, forgery detection, global features, local features, Zernike moments.

I.INTRODUCTION

In digital world image forgery detection technique is an important issue with the extensive use of image editing software. Image hashing technique can be used for image authentication. Unlike the hash functions in cryptograph as it is extremely sensitive to slight changes the image hash should be robust against normal image processing. The good characteristics of the image hash should be reasonably short, robust and sensitive to tampering. It should be unique and not allow any unauthorized party to break key and coin the hash.

Now we propose a method combining advantages of both and local features. Our objective is to provide a reasonably short image hash with good performance. Zernike moments of the luminance components to reflect the images global characteristics are used to decide whether given image is an original or maliciously electrode. Compared with some other methods the proposed method has better overall performance in major specifications especially the ability of distinguishing regional tampering from content-preserving processing.

In section II existing methods are describe. III Zernike moments, salient region detection and texture are briefly introduced. IV the proposed image has hashing scheme and the procedure of image authentication is presented. Section IV gives experimental result and analyzes performance of the method. V concludes the paper.

II.EXISTING METHODS

Various image hashing methods have been proposed one of them among is khelifi et al' [1] proposed a robust and secure hashing scheme based on virtual watermark detection. Monga et al' [2] apply NMF to pseudo randomly selected sub images, andtheyconstruct a secondary image. These methods obtain a low- rank matrix approximation of the secondary image with NMF again. A.swaminathan [3] proposed an image hash method based on rotation invariance of Fourier-mellin transform and present a new framework to study the security issues of existing image hashing schemes. This method has been robust to geometric distortions. Monga [4] two-step frame work and hash become a routine practice in many image hashing methods. Many previous schemes were short but insensitive which local reflectedregional modifications. Tang et al' [5] cultivate a global method using non-negative matrix factorization [NMF]. The first image was converted into fixed sized pixel array. A secondary image was obtained by rearranging pixels and applying NMF to produce a feature bearing co-efficient matrix. In [6] xinag et al' proposed a method using invariance of

ISSN: 2278 – 1323

the image histogram to geometric deformation. Though it was robust it could not distinguish images with similar histograms.in [7] lei et al' calculate DFT of the in variant moments of significant radon transform coefficients and normalize the DFT coefficient to form the image hash for content authentication.

III. BRIEF DESCRIPTION OF USEFUL TOOLS AND CONCEPTS

A).ZERNIKE MOMENTS

Zernike moments are dependent on the translation and scaling moments of object and are used for extracting global features of image. Zernike moments(zm) of order n and repetition m of image I(ρ, θ).

$$Z_{n,\,m}=\frac{n+1}{\pi}\sum_{(n,m)\epsilon \text{unit disk}}\sum I(\rho,\theta)V^{*}_{n,m}(\rho,\theta)$$

Where $V_{n,\,m}(\rho\theta)$ is a Zernike polynomial of order n and represent m.

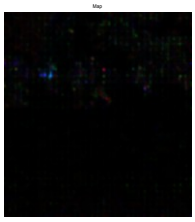
B).SALIENT REGION DETECTION

A salient region in an image is one that visual attention according to information in an image can be viewed as a sum of two parts that of innovation and that of prior knowledge the information of saliency is obtained when the redundant part is removed.

$$A(f) = h_l * L(f)$$

A (f) represent redundant information defined as convolution between L (f) and h_l, L (f) represents general information of the image, h_l represent l×l low-pass kernel.

(a) Original image



(b) saliency map

(c)saliency region

(d)forgery image

Fig1.Salient region detection (a) original image (b) saliency map (c) salient region (d) three rectangles

IV. PROPOSED HASHING SCHEME

In this section the proposed image hashing scheme and the procedure of image authentication using the hash are described.

A. IMAGE HASH CONSTRUCTION

The image hash generation procedure includes the following.

1) PRE-PROCESSING

Its object is an improvement of the image data that subdue undesired distortions or enhances of some image features. Here the image is first rescaled to a fixed size and converted from RGB to the YC_bC_r representation. YC_bC_r, $Y^1C_bC_r$ is a family of color spaces which also can be written as YC_bC_r or $Y^1C_bC_r$. Y indicates the luma component and $C_b$and C_r are representing the blue difference red difference Chroma component. The most obvious and common way to change the size of an image is to resize or scale an image.

2) GLOBALFEATURE EXTRACTION

Global feature are extracted from global perspective. This consider image as whole and then extracts features such as luminance and chrominance. Zernike moments are used for generating global feature which is then scrambled with key. Zernike moments are used efficiently as shape descriptions of image objects. Magnitude of thee Zernike moments are rounded and used to from a global vector Z= [Z_yZ_c].

ISSN: 2278 – 1323

Generator. The encrypted global vector Z is obtained by scrambling with key K_1.

3) LOCAL FEATURE EXTRACTION

This is the most important for solving the computational task related to a certain kind of Saliency region are shown in fig1 texture means the regular repetition of an elements or pattern or a surfaces.

4) HASH CONSTRUCTION

The global and local vectors are concatenated to form an intermediate hash sequence. The hash production is 560 bits long.

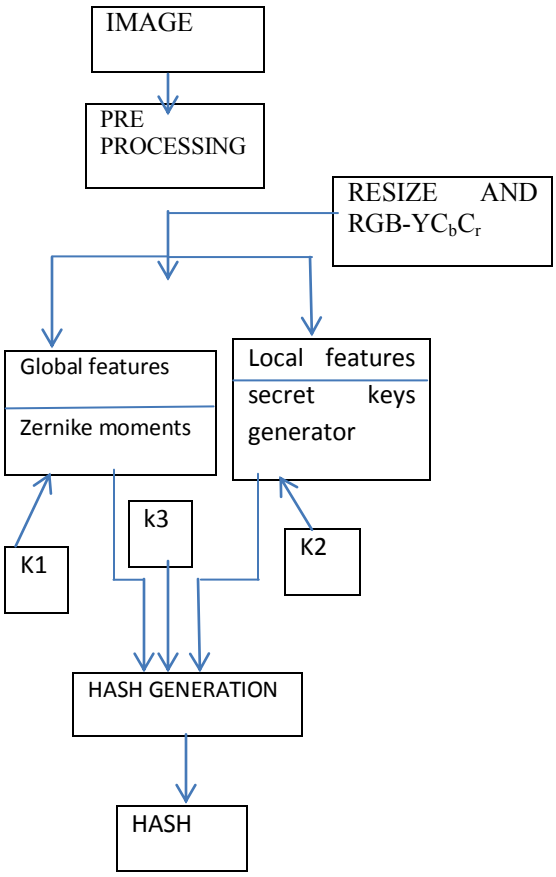


Fig 2 block diagram of proposed image hashing method

applications and feature representation piece of information. Position and texture features are mainly considered as local features. For feature extraction a secret key K_2 is used to generate encrypted local vectors.

B. FORGERYCLASSIFICATIONAND LOCATION

After coming to a conclusion that a test message 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, replacement of objects and universal color changes fig 3 show forgery localization. DecodeHoandH_1 into components representing global and local feature R and the numbers of salient regions in the reference and test images N_0 and N_1

1) If $N_0>N_1=R$ some objects have been removed from the entrance received test image. It informs the positions of the missing objects are located by comparing the saliency regions.
2) If $N_{1>}N_0=R$ the test image contains some additional objects whose positions are locate by comparing the saliency indices
3) .If $N_0=N_1=R$ check the luminance and chrominance components in the Zernike moments.
4) If $N_0>R$ and $N_1>R$ informs the salient regions are not matched.

ISSN: 2278 – 1323

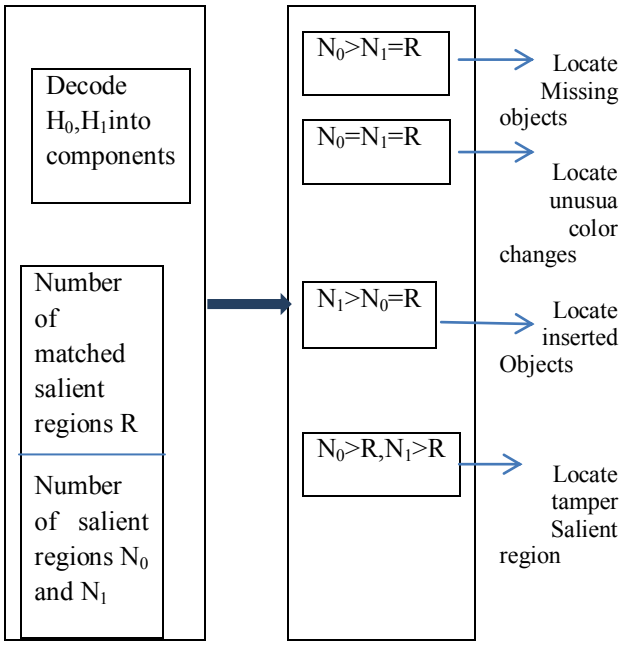


Fig 3: forgery classification and localization

C) *FORGERY DETECTION CAPABILITY*

The proposed method can differentiate similar forged and different images. A comparison between the proposed method and previousmethod is given is table1. The hash of [2],[1] is robust against slight croppingbut not to rotation even if the angle is small because it is based on pseudo-randomly selected sub images. The hash will also be changed by the after revolution. The method of [10] and [7] are not designed to localize forgery. Performance of the proposed method is basically due to the combination of global and local features.

Fig.4 examples of original, tampered, and saliency map images.

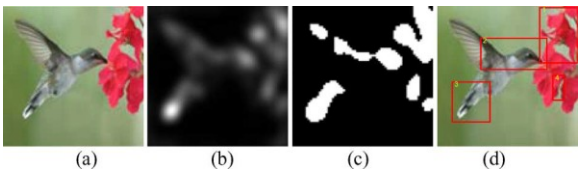


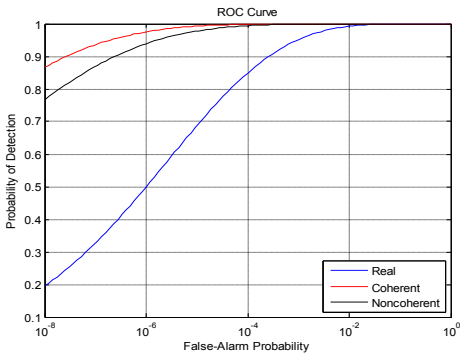
Fig. 5 salient region detection a) original image b) saliency map c) salient region d) four rectangle

D) COMPUTATION COMPLEXITY

The table-1 shows the comparison between the different proposed and previous existing methods, we consider average time consumed in calculating image hashes on a desktop computer with dual core.

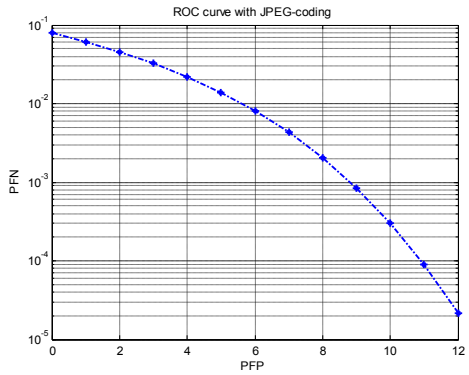
TABLE-1comparsion of hash performance

	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



(a)

ISSN: 2278 – 1323



(b)

fig. 6 a and b graphs represent noise addition and JPEG coding

V. CONCLUSION

In thin paper an image hashing method is developed using both global and local features. 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 received image is judged as fake. Hashes produced with the proposed method are robust against operations including common image processing operations including brightness, adjustment scaling, small angle rotation, and JPEG coding and noise and contamination. The proposed in is used due to its acceptable accuracy and computation complexity. Differentiate similar, forged and different images are using the hashes.

REFERANCES

[1] 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

[2]V. Monga and M.K. Mihcak, "Robust and secure image hashing via non-negative mark factorizations,"IEEE Trans. Inf. Forensics security, vol. 2, no. 3, pp. 376-390, Sep.2007

[3] A.Swaminathan, Y. Mao, and m. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics security, vol, 1, no. 2, pp. 215-230,Jan. 2006.

[4] V. Monga, A.Banerjee, and. L. Evans, "a clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics security, vol. 1, no. 1, pp. 68-79, Mar. 2006

[5] 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.

[6] 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.

[7] Y. Lei, Y. Wang, and J. Huang, "Robust image hash in radon transform domain for authentication," Signal process. : Image commun.Vol 26, no. 6, pp. 280-288, 2011

[8] A. 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.

[9] F. Ahmed, M. Y. Siyal, and V. U. Abbas, "A secure and robust hash based scheme for image authentication," Signal process. Vol 90, no.5, pp. 1456-1470, 2010.

[10] Ms.K.Hemalatha received the B.tech degree in E.C.E from sri sai insititute of technology and science(ssits)rayachoty,india in2012. She is pursuing her M.tech Degree at Annamacharya Institute of Technology and Sciences (AITS) Tirupati. Her area of interest includes image processing, Communications systems.

[11] **MS.M.Anitha** completed her M.TECH at A.I.T.S., Rajampet in 2011. Presentlyshe is working as Assistant Professor of ECE, Annamacharya Institute of Technology and Science, tirupati.
She has guided B.TECH projects. Her Research are includes embedded systems.

[12] **Ms.N.Pushpalatha** completed her B.Tech at JNTU, Hyderabad in 2004 and M.Tech at A.I.T.S., Rajampet in 2007. Presently she is working as Assistant Professor of ECE, Annamacharya Institute of Technology and Sciences, Tirupati.
She has guided many B.Tech projects. Her Research area includes Data Communications and Ad-hoc Wireless Sensor Networks.

ISSN: 2278 – 1323