ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

Image Forgery Detection Using Zernike Moments and Texture Features

Prasanna Bharekar[1], Dr S.K.Shah [2]

P.G. Student, Department of E & TC Engineering, SKN College of Engineering, Pune, Maharashtra, India[1]

HOD PG E&TC, Department of E & TC Engineering, SKN College of Engineering, Pune, Maharashtra, India[2]

ABSTRACT: Now a days with the widely availability of various media photo editing software, certifying authenticity of the image contents has become an major issue. Image hashing is a method by which one can extracts a short sequence from the image which is its contents, and therefore it can be used for image authentication. Image hashing functions are one of the most used methods used for detecting and localizing tampering. Both Zernike Moments and Haralick Texture features are used in extracting the hash sequence. The Zernike moments representing Y component i.e. luminance and CbCr component i.e. chrominance characteristics of the image. The Haralick texture features represent texture information of every block. Although image hashing is robust against most of the common content-preserving image processing operation, the hash is highly sensitive to malicious tampering such as copy and move, slicing etc and, therefore, can be used for image authentication. The hash value of a test image is compared with that of a input reference image. When the hash sequences are more than and less than a certain threshold value, the received image is confirmed as forged. By further analysing the hashes, one can determine the type of image forgery and also location of forged areas.

KEYWORDS: Zernike moments, Haralick Texture Features, Block Base Technique, Image Hash.

I. INTRODUCTION

With the development of technology, digital images play a crucial role in our day to day life. Digital image are used as medium of communication and consists of significant information. For now being, credible digital images may be taken as evidence at court; everyday newspaper and corporate magazines deal with digital images. However, sophisticated digital cameras and photo editing software are present everywhere at once. So, it has become relatively easy to tamper digital images and create forgeries that are difficult to distinguish from authentic images. The reality and privacy of digital images are suffering very badly. In consequence, it is important and necessary to discover the skill to distinguish the original images from the false images. Image hashing can be used for image authentication because it extracts a short sequence from the image that is nothing but the content of the image. In image hashing, image authentication is achieved by comparing the similarity of two individual image hashes that are extracted from the original image and the tampered image. Two images would have a large hash distance between them.

An image hash should have the following properties; it should be reasonably as short as possible, robust to ordinary common image manipulations, and sensitive to tampering. Manipulation .Unique means that two different images should not have same hash values and should be secure enough so that a wrong party cannot find the extracted hash value. Image hashing is considered to be the desired authentication technique for most tampering cases.
At the sender side, the hash is derived for the input image which is encrypted with some method and sent along with the image to the receiver side. Receiver removes the image hash from the received image and generates the hash for the received image in the same way as the sender. Then at the receiver side, both the hashes are compared to find the authenticity of the image and to locate the tampered or malicious regions of the image.
The work in this paper is divided in two stages. 1) Feature Extraction 2) Feature Matching. Feature Extraction is done by using Zernike moments and Haralick features. Zernike moments are robust against most of the common content-preserving image processing operation and Haralick features are highly sensitive to malicious tampering such as copy

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

and move, slicing etc .For Feature matching simply distance metric is used as criteria. Paper is organized as follows. Section II describes related work in image forgery detection Proposed methodology is given in Section III. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

II. RELATED WORK

There are various forgery detecting techniques have been invented so far. Monga [1] developed a process that includes first feature extraction (image hash) and second is coding of the hash result to form the final resultant hash. Image hashing methods are either global or local depending on requirement. Global features not sensitive to tampering in small areas in the image at the same time hashes are short, while local features can detect possible regional modifications but usually produce longer hashes as compared to global feature. In [2], Xiang *et al.* used a method which is using image histogram invariance to geometric deformations. It is strong to geometric attacks such as scaling, but images with similar histograms and different contents distinguishing are not possible here. Tang *et al.* [3] propose a forgery detection method using nonnegative matrix factorization (NMF). The given input image is first converted into a fixed-sized array of pixel. A next image is created by pixels rearranging and applying Non Negative matrix Factorization (NMF) to produce a final feature matrix, which is then quantized. The generated hash string is encrypted to generate the final image hash. Swaminathan *et al.* [4] proposed hashing technique based on rotation invariance using Fourier-Mellin transform. Proposed method is robust to various content-preserving manipulations such as jpeg compression geometric distortions such as filtering operations, scaling. Lei.et al. [5] proposed a method in which the DFT(Discrete Fourier Transform) of random transform coefficients find first and then quantization of the DFT coefficients to form image hash for image content authentication take place . The proposed algorithm can withstand almost all the important image processing manipulations, including blur, JPEG compression, addition of noise, geometric distortion, and enhancement .This method is useful for image authentication in terms performance detection of image and to reduce hash size. Khelifi *et al.* [6] propose virtual watermark detection based secure image hashing method which is a robust and secure. It is robust against normal image preserving operations such as jpeg compression and geometric transformation such as scaling, and it can also detect malicious content tampering in relatively large areas. Chun-Shein Lu et al. [7] proposed a method in which the mesh generation algorithm is executed which extracts robust and required salient points first. After that, a mesh normalization process is used to transfer the decomposed meshes to normalized meshes of fixed sizes. In [8], Yan Zhao et al. proposed that both the global and local features are considered. Zernike moments are taken as the global features and the local features include the position and texture information of the salient regions. These two features are combined to obtain the hash value. In [8], Gayathri Soman and Jyothish K. John et al. proposed that considered both the global and local features .Zernike moments are taken as the global features . These two features are combined to obtain the final hash value.

III. PROPOSED METHODOLOGY

Proposed system uses amplitude feature of Zernike Moments and 13 Texture features for image hashing. Following Fig .1 shows the General procedure for copy move Forgery detection.

Pre-processing

The input image is rescaled to a fixed-size 256*256 . Large value of dimensions leads to max computation complexity, while small value leads to loss of image details. We select fixed size of 256. Then the input image is converted from its RGB representation into YCbCr representation. The Y component represents the luminance of the image and the Cb–Cr represents the chrominance component.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

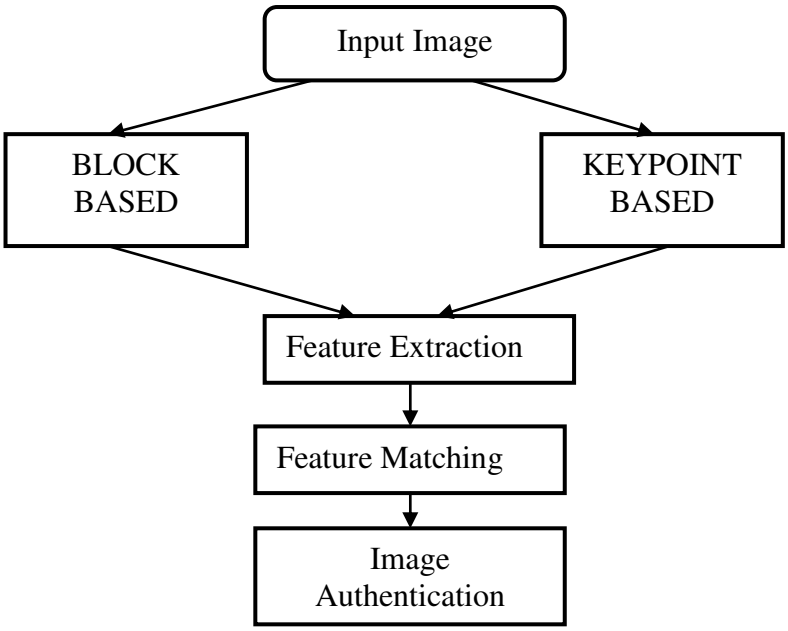

Fig. 1 General pipeline of copy-move detection methods

Zernike Moment Feature Extraction

The Zernike features are obtained Using the Zernike moments of the luminance(Y) and the chrominance component(CbCr) of the image. Here the order of the Zernike moment, n = 5. As a result we get row vector with 11 × 2 = 22 elements.

TABLE I
ZERNIKE MOMENTS OF DIFFERENT ORDERS

Order *n*	Zernike moments	Number of moments
1	$Z_{1,1}$	1
2	$Z_{2,0}$, $Z_{2,2}$	2
3	$Z_{3,1}$, $Z_{3,3}$	2
4	$Z_{4,0}$, $Z_{4,2}$, $Z_{4,4}$	3
5	$Z_{5,1}$, $Z_{5,3}$, $Z_{5,5}$	3

Haralick Feature Extraction

The image is then divided into blocks of size (32 × 32), and the local features (Haralick Features)are extracted from each of blocks. The mean of the 10 Haralick features out of is 14 Haralick features extracted from each block.

Final Hash Construction

The Final hash (V)is then constructed by concatenating both Zernike moments and Haralick feature vectors.Fig.2 shows the block diagram for hash construction.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

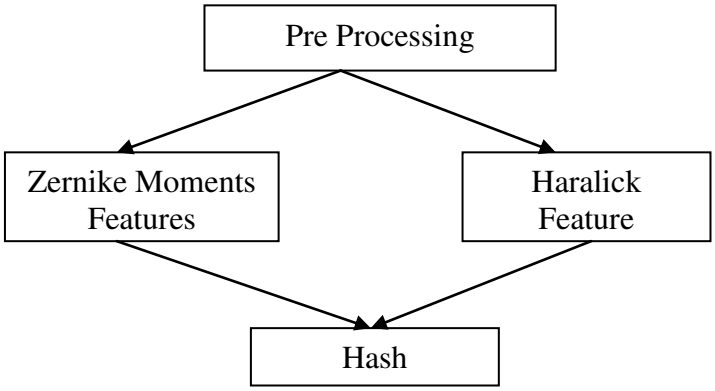

Fig. 2 Block Diagram of Hash Construction

Image Authentication

Next step is Image Authentication, In this the hash of a original image H0 is available with us and this is also called as reference hash. The hash of the received image is calculated at the receiver end using the same method to obtain the received hash H1, called test hash. Then these two hashes are compared and and analysed to find whether the image is Forged or original.

Distance Measurement

We use a Euclidean distance metric to calculate the distance between the reference hash and test hash to find whether the image has been tampered. The Euclidean distance metric between the reference and test image hash is given by

$$D=|V1-V0|.$$

If D is greater than a particular threshold, we can say that the image has been tampered.

Forgery Localization And Detection

The Haralick feature of the reference (Original) and the test (Forged) image is been compared. Fig 3.shows the block diagram of Forgery detection and Localization If the Haralick feature of any of the block of the reference image is more compared to same position block in the test image, then we can say that something object has been deleted. If the Haralick feature of any of the block of the reference(Original) image is less compared to same position block in the test (Received)image, then we can say that something object has been inserted.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

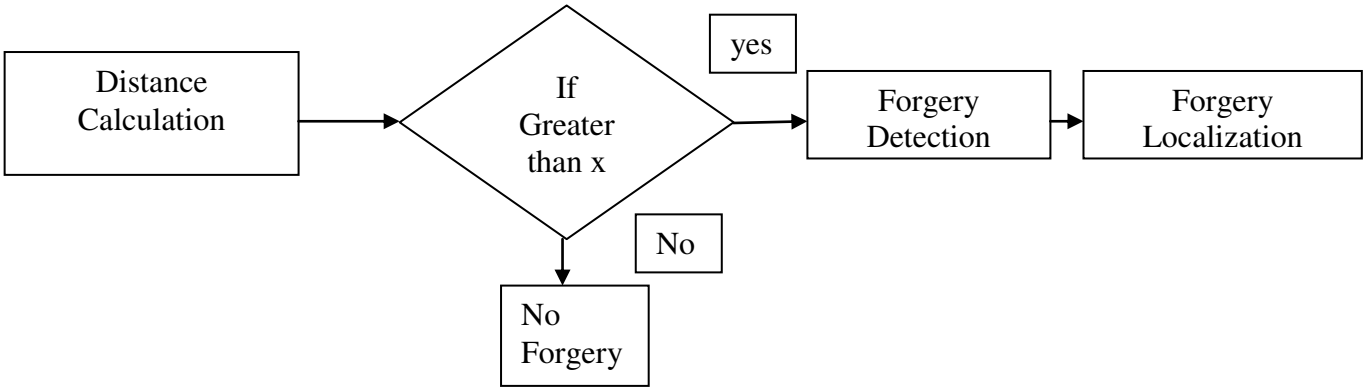

Fig. 3 Block Diagram of Forgery Detection and Localization

IV. EXPERIMENTAL RESULTS

We have tested most of the possible images downloaded from the dataset CoMoFoD. All of the forged images are detected and are correctly localized. The success rate of tampering detection is almost 95 %. The proposed technique is tested on MATLAB R2018a. Robustness of the image hash is checked against various common content-preserving modifications such as blur, brightness, JPEG compression, noise addition, rotation, scaling, brightness and contrast adjustment and slight cropping. Fig 4shows the Forgery detection and tampering localization results of two hashing methods (method based on Haralick and Zernike moments).

Fig4.(a)

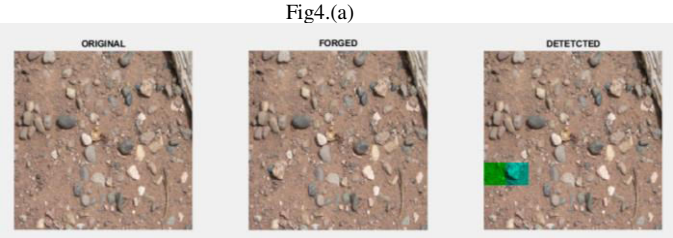

Fig4.(b)

Fig4.(c)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

A comparison between the various image hashing method is given in Table II, showing overall performance of the above method, which generates hashes with generally small length, is robust against several Normal processing manipulations and can also detect and locate Small area tampering.

TABLE II
COMPARISON OF HASH PERFORMANCE

	NMF method	Wavelet Based Method	Global and local features	Proposed Method
Feature used	Global	Local	Global And Saliency Related Feature	Both Global And Local
Robust Against Jpeg Coding	Yes	Yes	Yes	yes
Robust Against Small Angle Rotation	No	No	Yes	Yes
Ability To Detect Tampered Area	No	Yes	Yes	yes

V. CONCLUSION

In this paper, a new modified algorithm for image hash generation is developed using Zernike moments and Haralick features. The hash generated is robust to common content-preserving modifications such as JPEG compression, scaling, brightness adjustment, addition of noise, contrast and small angle rotation, and slight cropping, but sensitive to other forgery. The Haralick features extracted from image blocks are highly sensitive to forged areas. The method explained here is used for image authentication. The hash can differentiate original and faked images. It can also detect the forgery type that is whether it is an insertion of object or deletion of object. The method uses block-based forgery detection, and hence can be used for finding tampering in small regions also.

REFERENCES

[1] Monga V, Evans BL "A Perceptual image hashing using clustering based approach to". IEEE Trans Inf Forensic Secure 1(1):69–79,2006.
[2] Xiang S "Image hashing scheme based on histogram robust against geometric deformations". In: Proceedings of the ACM multimedia and security workshop, New York, pp 1221–128, 2007.
[3] Tang Z, Wang S, and Wei W, Su S R "Image hashing for tamper detection using non-negative matrix factorization (NMF) technique. J Convergence Technol 2(1):19– 26, 2008.
[4] Swaminathan A, Mao Y, Wu M "Robust and secure image hash". IEEE Trans Inf Forensic Security 1(2):215–230, 2006.
[5] Lei Y, Wanga Y, Huang J "Robust image hash in Randomn transform domain for Authentication". Signal Process: Image Commun 26(6):280–288, 2011.
[6] Khelfi F, Jiang Jet. al" Image hashing based on virtual watermark detection". TransImage Process 19(4):981–994, 2010.
[7] Tang Z, "Lexiographical framework for image hashing with implementation based on Discrete Coefficient Transform and Non negetive Matrix Transformation". 52(2– 3):325–345, 2011.
[8] Zhao Y, Wang S, Zhang X, Yao H" Image hashing method for image authentication using local features and Zernike moments ". IEEE Trans Inf Forensics Security 8(2), 2015.
[9] Gayathri Soman and Jyothish K. John " Block Based Forgery detection using global and local features", conference on Soft Computing System Advances In Intelligent System and Computing© Springer India 2016.