International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Robust Blind Image Forensic-Detection Method Based On Fuzzy Technique

V.Thirunavukkarasu, J.Satheesh Kumar

Abstract: ***Blind forensic-investigation in a digital image is a new research direction in image security. It aims to discover the altered image content without any embedded security scheme. Block and key point based methods are the two dispensation options in blind image forensic investigation. Both the techniques exhibit the best performance to reveal the tampered image. The success of these methods is limited due to computational complexity and detection accuracy against various image distortions and geometric transformation operations. This article introduces different blind image tampering methods and introduces a robust image forensic investigation method to determine the copy-move tampered image by means of fuzzy logic approach. Empirical outcomes facilitate that the projected scheme effectively classifies copy-move type of forensic images as well as blurred tampered image. Overall detection accuracy of this method is high over the existing methods.***

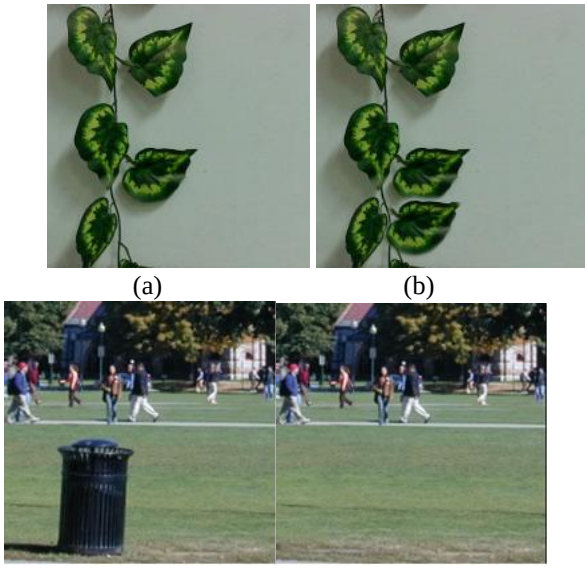
Index Terms: ***Blurring, computational complexity, detection accuracy, fuzzy logic, forensic-Investigation, image security.***

I. INTRODUCTION

Inserting or obliterating some imperative characteristics of an image without any ocular indication becomes easy with the availability of powerful image expurgation tools and techniques [1]. There exist different tampering techniques to phoney the substance of an image. Copy-move, compositing and retouching are recurrently used methods [2] [3].

A. copy-move

This is a familiar category of image phoney where, one needs to duplicate or hide the region in an image by bootlegging unambiguous segment of an image and gluing in dissimilar part of the same image. Textured regions are suitable part for copy-move forgery since, it has same colour, dynamic range and noise variation properties. Figure 1 exemplify copy-move tampering [4]



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

Fig 1: (a & c) original Images (b & d) Tampered Images

B. Image splicing

Image splicing or photomontage is another important and frequently used image manipulation technique in which multiple images are fused together to form a spliced image. Figure 2 illustrate this kind of manoeuvring [5].

C. Image retouching

To improve the appearance of an image certain features are increased or decreased by means of retouching tools. It will not change the image content [6]. Figure 3 is an example for image retouching.

The tampering is acceptable if it is performed to improve the image quality, remove the noise and enhance the contrast or highlight some important regions in an image.

(a) (b)

Manuscript published on 30 September 2019
* Correspondence Author
Dr.V.Thirunavukkarasu*, School of CSA, REVA University, Bangalore, India
Dr.J.Satheesh Kumar, Department of Computer Applications, Bharathiar University, Coimbatore, India.

(c)

Fig 2: (a) & (b) Authentic images (c) spliced image

(a) (b)

Fig 3: (a) Authentic image (b) Re-touched image

When it is performed to deceive a court or public then forensic investigation is necessary to guarantee the reliability of an image. Various state of art tamper edifying techniques is dwindled into two types such as active and blind (passive) techniques. The application of tamper discovery includes Insurance claims, industrial photography, medical imaging, e-commerce, journalistic photography and so on. Different tampering methods are shown in figure 4 [7].

Remnants of this paper are organized as follows. Section II introduces different blind tamper detection methods, Section III presents related works in image forensic-investigation, the proposed fuzzy-logic based scheme is introduced in section IV, Pragmatic upshots are examined in section V and section VI concludes the paper.

II. BLIND IMAGE TAMPERING METHODS

The active methods merely rely on authentication code which is inserted at the time of image capturing or recording. Instead of authentication code the user defined algorithms are used in blind methods.

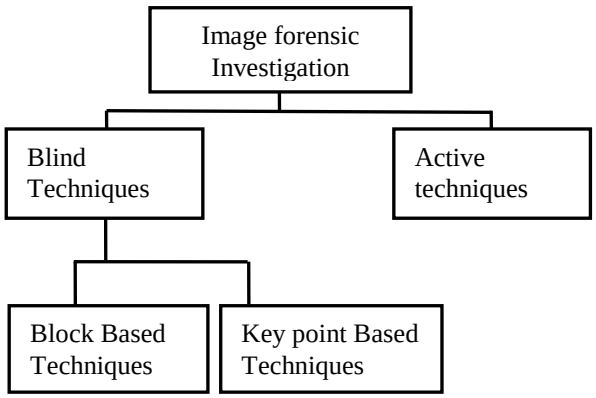


Fig 4: Image Forensic Investigation Methods

A. Block based techniques

In this technique, suspected M X N image is alienated in to overlapped blocks of dimension b X b to reduce the complexity of tamper detection.

The feature vector intended to every block is computed using frequency transformation, image intensity or moments. The similar feature vectors are matched using lexicographical sorting or approximate nearest neighbour method. To remove the false matches with adjacent blocks Euclidean distance measure is employed [8].

B. Key point based techniques

A point through well distinct location and high entropy is called key point. It preserves related features of an image region and perceived even after various statistical renovations or illumination distortion [9].

In block based technique the computational cost will be increased when each block is matched by making series of comparison with other blocks. The detection accuracy will fall when tampered region is rotated or scaled. To overcome the above issues key point based methods are introduced [10].

III. RELATED WORKS

Girija et al. employed a fuzzy fusion method to perceive forensic region in an image by means of ICA and CCA. This method is successfully identified the tampered images but fails to discover different types of tampering and tampered image with geometrical and post processing operations[11].

Barni et al. introduced fuzzy based framework to deal with ambiguity in error-prone tools and fuse the information endow with different tools in to single output. This framework resolves the problem of depending on more than one tool to discover different types of image manipulations. This technique is used to deal with uncertainty in copy-paste manipulation and does not concentrate on other types of manipulations such as photo montage or retouching [12].

Mohammad et al. proposed a block and fuzzy based technique to discover manipulated images. This method employed six different tools such as DWT, PCA, DWT-DCT, DCT, DFT and DWT-DCT-SVD to ascertain manipulated image regions and the result is passed to Fuzzy based classifier to compact with improbability in detection of manipulated image under different image renovations like blurring, intensity variation and noise. This method achieves 94.12% of accuracy in 81 X 81 copied regions but fails to discover the manipulated region under different geometric transformations [13].

IV. PROPOSED DETECTION TECHNIQUE

Workflow of projected technique is shown in figure 5. The input images are gathered from three existing data sets such as KODAK image data set[14], CoMoFoD image data base [15] and Muhammad et al. dataset[16]. The existing three techniques such as frequency transformation, dimension reduction (DR) and Zernike moment based methods were successfully implemented using MATLAB-2015 and the results were passed to fuzzy fusion framework for decision making [17]-[19]. Table 1 illustrate the different features and feature matching techniques used in the existing techniques.

Table 1: Different methods and its feature representation

Method	Image representation	Feature Dimension
Frequency transformation method	DCT	64
DR method	PCA	32
Zernike moment based method	Zernike moments	12

A. Fuzzy Fusion assessment formation

The detection accuracy and reliability are the two measures which are used to decide certain type of tampering.

The proposed method make use of four fuzzy sets to determine the severity of tampering such as very strong, strong, weak, very weak . Based on the behaviour of three tools in presence of certain tampering, proposed methodology will identify whether tampering belongs to above four categories. Different rules are formed by means of fuzzy fusion assessment.

RULE 1: Detection accuracy is lofty AND consistency is lofty then tampering is very strong

RULE 2: Detection accuracy is lofty AND consistency is stumpy then tampering is strong

RULE 3: Detection accuracy is stumpy AND consistency is lofty then tampering is weak.

RULE 4: Detection accuracy is stumpy AND consistency is stumpy then tampering is very weak.

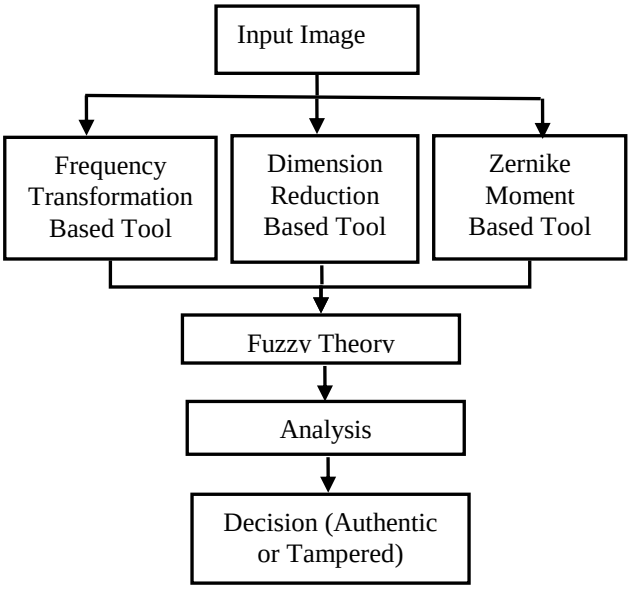


Fig 5: Workflow of proposed forensic investigation Method

B. Fuzzy Inference Process

The fuzzy interface process with respect to above four rules is revealed in figure 6. Discovered outcome is supplied as an input to the fuzzy interface and all four rules are assessed in parallel by means of fuzzy interpretation. The outcome of the rules are pooled (Defuzzified) and belongs to any of the four types such as very strong, strong, weak and very weak. The input values are crisp and restricted to a meticulous range. Four rules are assessed in analogous using fuzzy interpretation and the outcome of the rules are pooled and condensed. Finally, the results are converted in to non-fuzzy numbers.

V. EMPIRICAL RESULTS AND DICUSSION

Recital of the proposed technique is estimated with existing three states of art methods by means of the metrics sensitivity and specificity.

A. Sensitivity

Sensitivity signifies the magnitude of tampered images that are precisely classified as tampered. It is computed with the formula,

$$\text{Sensitivity} = \frac{TP}{TP + FN} \quad (1)$$

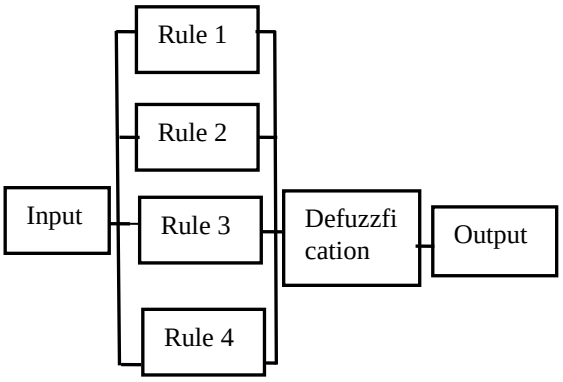


Fig 6: Fuzzy Interface process

Where TP signifies true positive and FN designate false negatives.

B. Specificity:

It signifies the magnitude of genuine images that are precisely exposed as genuine. It is premeditated with the formula,

$$\text{Specificity} = \frac{TN}{TN + FP} \quad (2)$$

Where TN signifies true negative and FP indicates false positive [20]. Performance evaluation of projected technique with the existing techniques (FT, DR and Zernike Method) is plotted in figure 7.

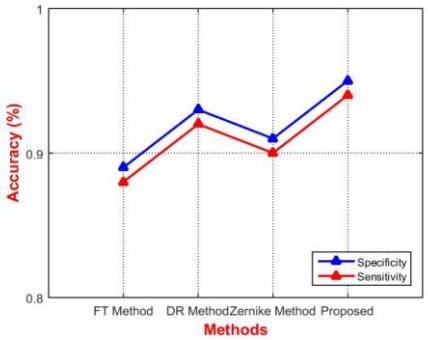


Fig 7: Assessment of proposed technique with existing Techniques

VI. CONCLUSION

A robust fuzzy based image forensic investigation method is presented in this article. This method automatically predicts simple, multiple copy-move tampered image and also the tampered image with blurring. Recital of the proposed technique is compared with frequency transformation based, dimension reduction based and Zernike moment based methods. Performance evaluation curve shows that PCA based method outperform other two methods but dimension of this method is high over the Zernike moment based method. The proposed fuzzy based image forensic investigation method exhibit 94% sensitivity and 95% specificity and outperforms all three methods.

ACKNOWLEDGMENT

The authors would like to thank Vision Group of Science and Technology (VGST), Government of Karnataka, India for their financial support under the RGS/F grant (Grant No: KSTePS/VGST-RGS/F/GRD No.695/20L7).

REFERENCES

1. Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on Information Forensics and Security, Vol. 7(6), 2012, pp:1-26.
2. Osamah M, Al-Qershi , Bee Ee Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art", Forensic Science International, Elsevier publication (2013), pp:284–295.
3. V.Thirunavukkarasu, J.Satheesh Kumar , "Evolution of Blind Methods for Image Tamper Detection-A Review", International Journal of Applied Engineering Research (IJAER) ,vol. 9(21), 2014, pp:5069-5076.
4. V.Thirunavukkarasu, J.Satheesh Kumar, "A Novel Method to Detect Copy-Move Tampering in Digital Images", Indian Journal of Science and Technology (IND-JST), Vol. 9(8), 2016
5. Satheesh Kumar J, Thirunavukkarsu V, "Image splicing detection based on camera characteristics and lighting inconsistencies", ICIoTC, Vol.1 (1), 2015, pp: 10–14
6. Gang Cao, Yao Zhao, Rongrong Ni, Xuelong Li, "Contrast Enhancement-Based Forensics in Digital Images", IEEE Transactions on Information Forensics and Security, VOL. 9(3), pp:515-525, 2014
7. Thirunavukkarasu V, Satheeshkumar J, "Passive Image Tamper Detection Technique Based on Moment Invariants", IJCTA, Vol.9 (10), 2016, pp: 4705-4714
8. Thirunavukkarasu V, Satheesh Kumar J, Gyoo Soo Chae, Kishorkumar J, "Non-intrusive Forensic Detection Method Using DSWT with Reduced Feature Set for Copy-Move Image Tampering" ,WPC, SPRINGER, 1-19.
9. Thirunavukkarasu V, Satheeshkumar J, "Passive Image Tamper Detection Based on Fast Retina Key point Descriptor", IEEE Xplore Digital library,2016, pp.279-285.
10. V.Thirunavukkarasu, J.Satheeshkumar, " Key Point Based Approaches for Copy-Move Image Tamper Detection-A Review**", IJRAT, Vol 6(6), Jul 2018. PP:1290-1295**
11. Girija Chetty and Monica Singh, "Nonintrusive Image Tamper Detection Based on Fuzzy Fusion", International Journal of Computer Science and Network Security, VOL.10(9), 86-90, September 2010
12. M. Barni , A.Costanzo, "A fuzzy approach to deal with uncertainty in image forensics", Signal Processing: Image Communication, vol.27(1), 998-1010,2012.
13. Mohammad Farukh Hashmi and Avinash G. Keskar, "Block and Fuzzy Techniques Based Forensic Tool for Detection Classification of Image Forgery", Journal of Electrical Engineering Technology, 2015.
14. Kodak Lossless True Color Image Suite: http://r0k.us/graphics/kodak/
15. Muhammad G, Hussain M, Khawaji K, Bebis G, "Blind copy move image forgery detection using dyadic un-decimated wavelet transform", Digital signal processing, pp:1-6, 2011
16. Tralic D, Zupancic I, Grgic S, Grgic M, "CoMoFoD - New Database for Copy-Move Forgery Detection", in Proc. 55th International Symposium ELMAR-2013, pp. 49-54.
17. Fridrich A, Jessica B, David Soukal, A. Jan Lukas, "Detection of copy-move forgery in digital images", In Proceedings of Digital Forensic Research Workshop, 2003.
18. A. Popescu, H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.
19. Ryu, Seung-Jin, Min-Jeong Lee, Heung-Kyu Lee, "Detection of copy-rotate-move forgery using zernike moments", Information Hiding, Vol. 638(7), pp:51-65, Springer, 2010.
20. Thirunavukkarsu V, Satheesh Kumar J, "Intrusive and non-intrusive techniques for detecting fake images", IJBI, Vol.3 (1), 2014, pp: 374–379.

AUTHORS PROFILE

Dr. V.Thirunavukkarasu, received his doctoral degree in computer science from Bharathiar University, Tamil Nadu, India. Currently he is working as an Assistant Professor, School of Computer science and Applications, REVA University, Bengaluru, India. His area of interest includes image forensic investigation, computational intelligence and machine learning algorithms. (E-mail: arasu_mca3@yahoo.com)

Dr. J. Satheesh Kumar is with the Department of Computer Applications, School of Computer Science and Engineering, Bharathiar University, Coimbatore, Tamil Nadu, India. He is having 18 plus years of research and teaching experience. His area of specialization includes soft computing, networks, Image processing and medical imaging. (E-mail: jsathee@rediffmail.com)