International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 2248-2259

Forgery Detection by Using Zernike Moments and Nearest Neighbour

Kavita Rathi Panwar
Department of Computer Science & Engineering, D. C. R University of Science & Technology, Murthal

Parvinder Singh
Department of Computer Science & Engineering, D. C. R University of Science & Technology, Murthal

Abstract

With the increasing use of internet, risk for the information is also increasing. High quality software's are available to make manipulations in the images. These fabrications are so minute that it is not possible to detect them with naked human eyes. It may affect the social, political, economic and personal aspects of society. Wrong prediction of images may also result in jeopardise of judicial system. Therefore, there is a great need to evolve an image authentication system that is capable of detecting forgery in images with high precision rate. Orthogonal image moments are the most popular and most efficient methods to describe an image as they can represent an image with minimum information. They are robust against noise and rotation and can be made invariant to scaling and translation as well. Zernike moments are the most popular orthogonal moment as they are invariant to arbitrary rotation. This paper presents an improved Zernike moment block based technique integrated with generalized nearest neighbour to detect image forgeries. Generalized nearest neighbour is used for feature matching as g2NN is capable of detecting multiple forgeries. Performance of proposed block based Zernike moment method is shown for various attacks like translation, Rotation, scaling and combination of rotation and scaling attacks. Comparison of the proposed technique with the existing techniques is also presented.

Keywords: *orthogonal moments, rotation invariant, g2NN, dataset, forgery detection*

Introduction

Copy move Image forgery detection techniques are of two types. One is key-point based techniques and the second is block-based techniques. In case of key point based techniques: key-points (high entropy area) are extracted from the image with the help of feature extractor. [1][2]Instead of working on the whole image now the matching will be carried out on the key-points only. However in case of block- based techniques the image is first divided into overlapping or non-overlapping blocks depending upon the extractor used then feature are extracted for the whole image by calculating feature vectors for all the blocks. A number of feature extractors and feature matching algorithms are available as shown in the workflow diagram. [3][4] Filtering is used to remove the outliers to improve the detection results. Post processing techniques are used to display forged regions after improving the results like if simple translation is used to copy and move the object then geometrical distance is best and simplest post processing method to be used to detect the correct region. [5][6]However if intermediate attacks are performed like rotation then geometric distance will not work. RANSAC can be used in that case as it works good in case of rotation detection. [7][8]

ISSN: 2233-7857 IJFGCN

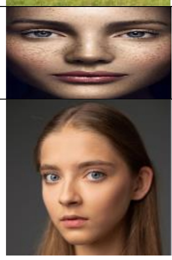
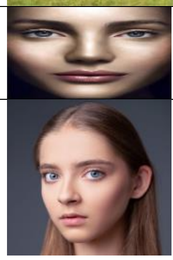
S.no	Type Of Forgery	Forgery	Original	Forged Image
1 2	Passive	Copy Move Forgery		
3 4				
5 6		Image Splicing		
7 8		Retouching		
9 10		Lightning		

Figure **Error! No text of specified style in document.**: An example of passive forgery types

There are numerous examples of copy-move forgery images for example authors have presented an image were a tree is copied from one image to another [9]. In case of CMF Object can be copied and simply pasted to some other location of the same image or the object may be rotated or scaled and then pasted to the image at a new location. [10]

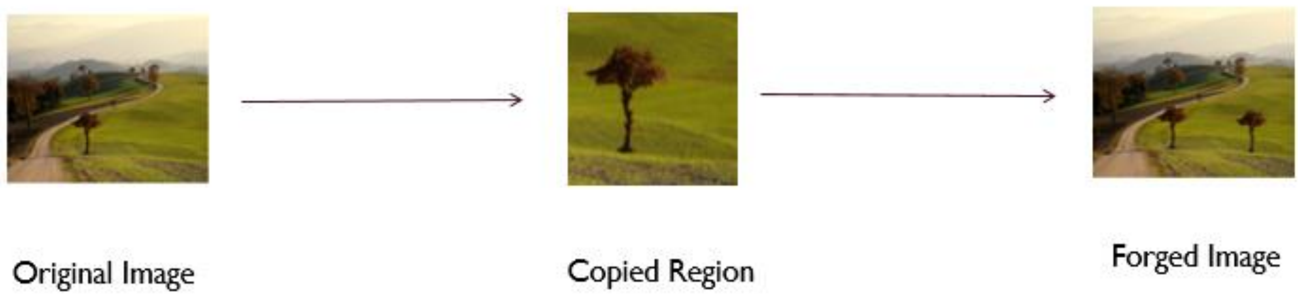


Figure 2 An example of Copy Move Image forgery

Workflow for the block-based techniques is presented mentioning all the techniques available for pre-processing, feature extraction, feature matching, filtering, post-processing etc. block-based techniques work very efficiently for detecting image forgeries in case of simple translation and in the smooth regions of the image. However, they fail to detect forgery if rotation and scaling are performed in the forgery. [11]

ISSN: 2233-7857 IJFGCN

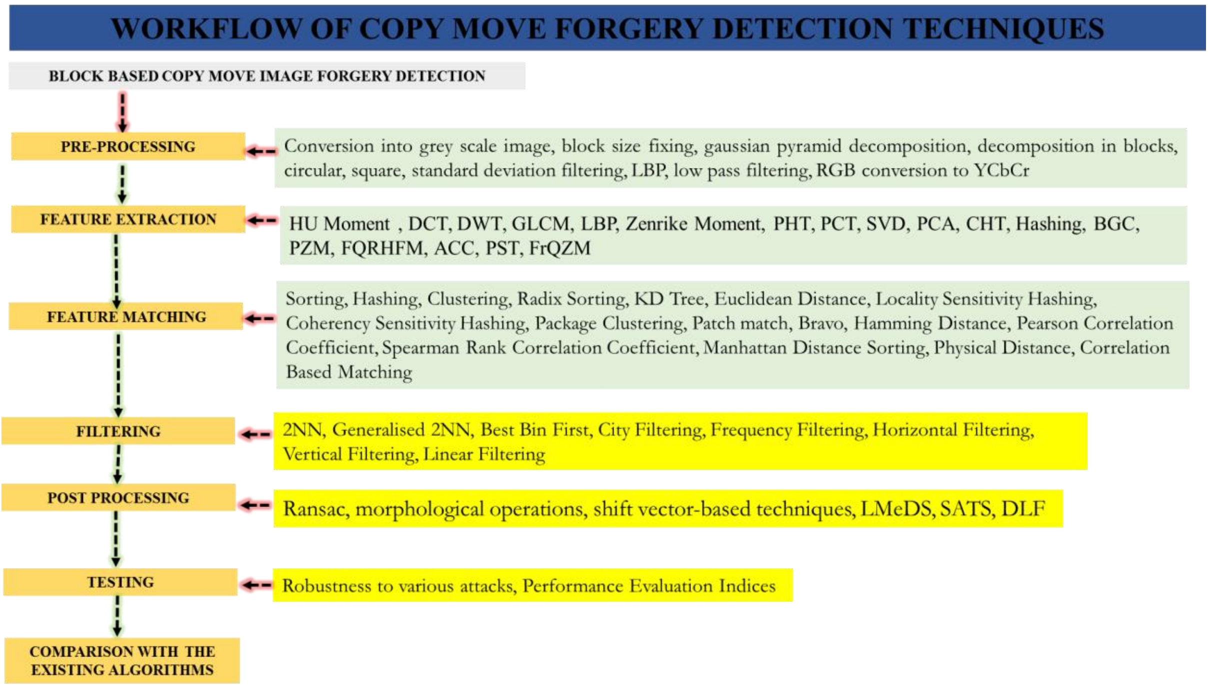


Figure 3 Workflow diagram for Block Based techniques

LITERATURE REVIEW

S.no	Paper	Method	Performance Parameter	Merits/ demerits
1.	[11][32][21]	Zernike Moments	F1: Precision: 65.625 Recall: 76.36	Zernike moments are rotation invariant
2.	[12][22][28][38]	Zernike moments & SIFT	F1: Precision:96.36 Recall: 98.14	Zernike moments are fast in calculating feature of an image and are robust to various intermediate attacks.
3	[13][29][30]	Zernike , SIFT & SLIC	F1: 0.7377 Precision: 0.7627 Recall: 0.7143	Zernike moments are rotation and translation invariant and can be made as scaling invariant.
4	[14][23][34][50]	DWT , Modified Zernike Moments	F1: 92.61 Precision: 93.07 Recall: 92.15	Among all orthogonal moments, Zernike is considered as the best method for image feature extraction due to its invariant nature towards rotation and scaling.
5	[15][27]	Adaptive fusion, SIFT & Zernike Moments	F1: 0.8491 Precision: 0.7759 Recall: 0.9375	Zernike is rotation invariant but to some extent only. It is not invariant to rotation after a certain angle of rotation.
6	[16][46][47]	Pyramid Model & Zernike	F1: Precision: 94.5	Zernike moments are computationally

ISSN: 2233-7857 IJFGCN

		Moments	Recall: 71.2	complex.
7	[17][26][39][40]	PCA, Zernike Moment, Wavelet Decomposition	F1:94.20 Precision: 95.87 Recall: 92.59	Zernike moments are capable of representing image with less information.
8	[18][31][42]	Wavelet Transform & Zernike Moment	F1: 91.65 Precision: 86.71 Recall: 94.78	Invariant to rotation, scaling and noise adding but to certain extent only.
9	[19][36][33]	Zernike Moment	F1: 78.89 Precision: 83.59 Recall: 76.63	Best feature extractor for block based technique.
10	[20][24][25][27]	Zernike Moment & Wavelet Decomposition	F1: 94.20 Precision: 95.87 Recall: 92.59	Moment based feature extractor are comparatively better than other available extractor in block based techniques and Zernike moments are best among them.

Table Error! No text of specified style in document. **Literature review for Zernike Moments**

PROPOSED ALGORITHM

Orthogonal image moments are the most popular and most efficient methods to describe an image as they can represent an image with minimum information. They are robust against noise and rotation and can be made invariant to scaling and translation as well. Zernike moments are the most popular orthogonal moment as they are invariant to arbitrary rotation. Generalized nearest neighbour is used for feature matching as g2NN is capable of detecting multiple forgeries.

1. PRE-PROCESSING

The pre-processing stage of a CMFD algorithm help in dimensionality reduction, filtering unnecessary information and conversions for making the CMFD process comparatively faster, efficient and accurate.

CONVERSION OF COLOURED IMAGE TO GRAYSCALE IMAGE

In case of coloured images, the processing speed of algorithm is improved by reduction in image dimension by converting the coloured image to grayscale image by application of weighted sum of the RGB bands of coloured image with the weights$w_R = 0.299, w_B = 0.587, w_G = 1-(w_R+w_B)$.

$Y = \sum w_C \times C, \;\; C \in \{R,G,B\}$

2. FEATURE EXTRACTION

Zernike moments are the most commonly used moments among all orthogonal moments. The reason for their popularity is that they are rotation invariant and can be made scaling and translation invariant. Zernike moments have shown considerable improvements in the results when used in pattern recognition and image retrievals.

First time Zernike moments were used in images by Teague [48] as a set of polynomials with circle$x^2 + y^2 = 1$.

$$V_{nm}(\mathrm{X,Y}) = V_{nm}(\rho,\theta) = R_{nm}(\rho)\exp(jm\theta)$$

$$R_{nm}(\rho) = \sum_{s=0}^{\frac{n-|m|}{2}} (-1)^s \cdot \frac{(n-s)!}{s!\,(\frac{n+|m|}{2}-s)!\,(\frac{n-|m|}{2}-s)!}\rho^{n-2s}$$

Note $R_{n,-m}(\rho) = R_{nm}(\rho)$.

ISSN: 2233-7857 IJFGCN

International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 2248-2259

$$\iint_{x^2+y^2\leq 1} V^*{}_{nm}(x,y).V_{pq}(x,y)dxdy = \frac{\pi}{n+1}\delta_{np}\delta_{mq}$$

Where $\delta_{\alpha\beta}$ = 1 for α = β and $\delta_{\alpha\beta}$ = 0.

The Zernike moment for image fraction $f(x,y)$ is

$$Z_{nm} = \frac{n+1}{\pi}\iint_{x^2+y^2\leq 1} f(x,y)V^*{}_{nm}(\rho,\theta)dxdy$$

After replacing integrals by summations

$$Z_{nm} = \frac{n+1}{\pi}\sum_{x}\sum_{y} f(x,y)V^*{}_{nm}(\rho,\theta), \quad x^2+y^2\leq 1$$

If all moments Z_{nm} of $f(x,y)$ are known to n_{max}order then discrete function may be rewrite as $\hat{f}(x,y)$with same moments as $f(x,y)$, for n_{max}. By orthogonality of Zernike

$$\hat{f}(x,y) = \sum_{n=0}^{n_{max}}\sum_{m} Z_{nm}V_{nm}(\rho,\theta)$$

With m having same constraints as in eq. (1) and as n_{max} approaches infinity $\hat{f}(x,y)$ will approach$f(x,y)$.

To fasten the computation process instead of using direct method recursive equations are introduced for computing polynomials. Recursive equations to calculate radial polynomials are

$$R_{nn}(r) = r^n \; for \; n = m,$$

$$R_{n(n-2)}(r) = nR_{nn}(r) - (n-1)R_{(n-2)(n-2)}(r) \quad for \; n-m = 2,$$

$$R_{n(m-4)} = H_1R_{nm}(r) + (H_2 + \frac{H_3}{r^2})\, R_{n(m-2)}$$

Otherwise, where the coefficients $H_1, H_2 \; and \; H_3$ are given by

$$H_3 = \frac{-4(m-2)(m-3)}{(n+m-2)(n-m+4)}$$

$$H_2 = \frac{H_3(n+m)(n-m+2)}{4(m-1)} + (m-2)$$

$$H_1 = \frac{m(m-1)}{2} - mH_2 + \frac{H_3(n+m+2)(n-m)}{8}$$

3. FEATURE MATCHING

Euclidean distance d $\in (d_1, \dots\dots, d_k)$ between point p and q in Euclidean space is

$d = \| q - p \| = \sqrt{\sum_1^n (p_i - q_i)^2}$

The **nearest neighbour** test is used for filtering through matching procedure of different candidate matches with respect to the threshold value. Generalised Nearest Neighbourhood g2NN has capacity to match multiple copies making it invariant to multiple CMF[49].

$\frac{d_i}{d_i+1} > T$

Threshold T $\in$ (0,1) taken as 0.6 in[34], 0.5 in[38], the authors considered 0.5 as threshold value.

4. POST-PROCESSING

Morphological operations are carried out to provide real picture of forged components. After doing the post-processing, the forged region is displayed.

ISSN: 2233-7857 IJFGCN

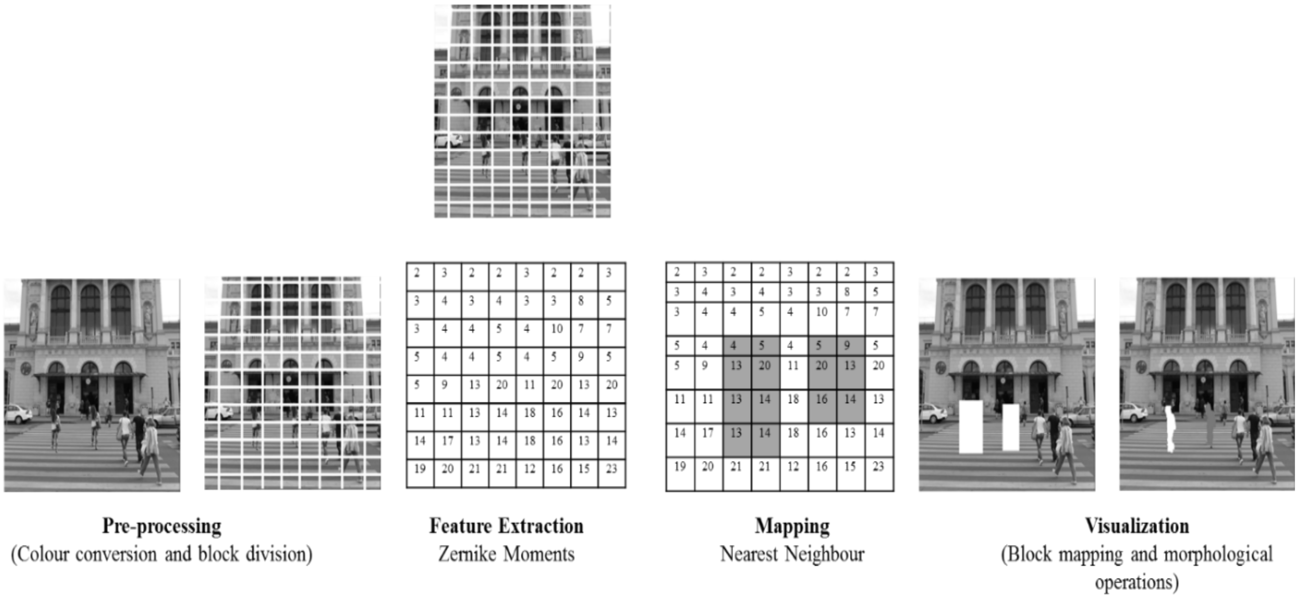


Figure 4 Working of proposed Block Based Techniques

DATASET

No standard dataset is available in the literature that covers all types of images and all types of attacks so researchers have used two datasets named CoMoFoD and Copy move dataset for this work. CoMoFoD database for a copy-move forgery detection has two parts. One is for small image size and the other is for large image size. [35][37][41]This paper has used small category as it is available free of cost and is having binary and coloured mask available for all the images. This dataset cover several post processing and pre-processing attacks like rotation, scaling, translations, blurring, noise adding, contrast enhancement, colour change etc.[43]

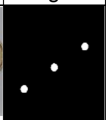
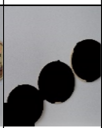
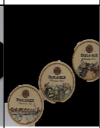
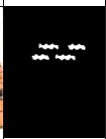
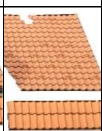
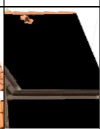
S. No	Image	Ground Truth Images	Result	Smooth Region	Textured egion	JPEG Compression[20]	Image Blurring σ(0.009)	Noise Adding (3x3)	Brightness Change[(0.01,0.95)]	ColorReduction[32]	Contrast Adjustment[(0.01,0.95)]
1.											
2.											

Figure 5 An example of images available from the Dataset with different attacks available

Second dataset used is Copy-Move Forgery Dataset:the dataset is divided into three subsets D0, D1 and D2 depending upon intermediate and post processing operations. D0 contains simple translation images with no compression. D2 and D3 contain images with rotation and scaling respectively. Image size is 1000x700 or 700x1000 pixels. Simple images are considered in this dataset rather than taking complex scenes.[44][45]

RESULTS

Performance of proposed block based Zernike moment method is shown for various attacks like translation, Rotation, scaling and combination of rotation and scaling attacks.

ISSN: 2233-7857 IJFGCN

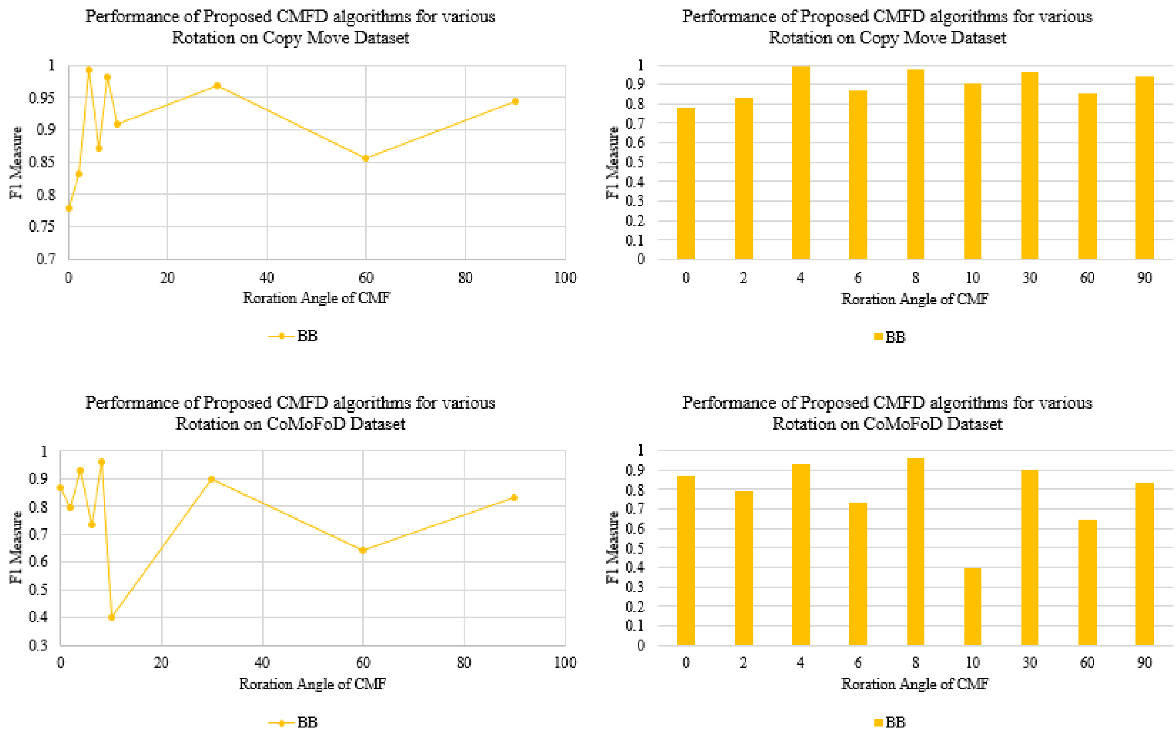


Figure 6 Performance of the proposed Zernike moments method against Rotation Angles

Performance of the proposed Zernike moments based method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against rotation attack at various angles (0, 2, 4, 6,8,10,30,60,90 degrees).

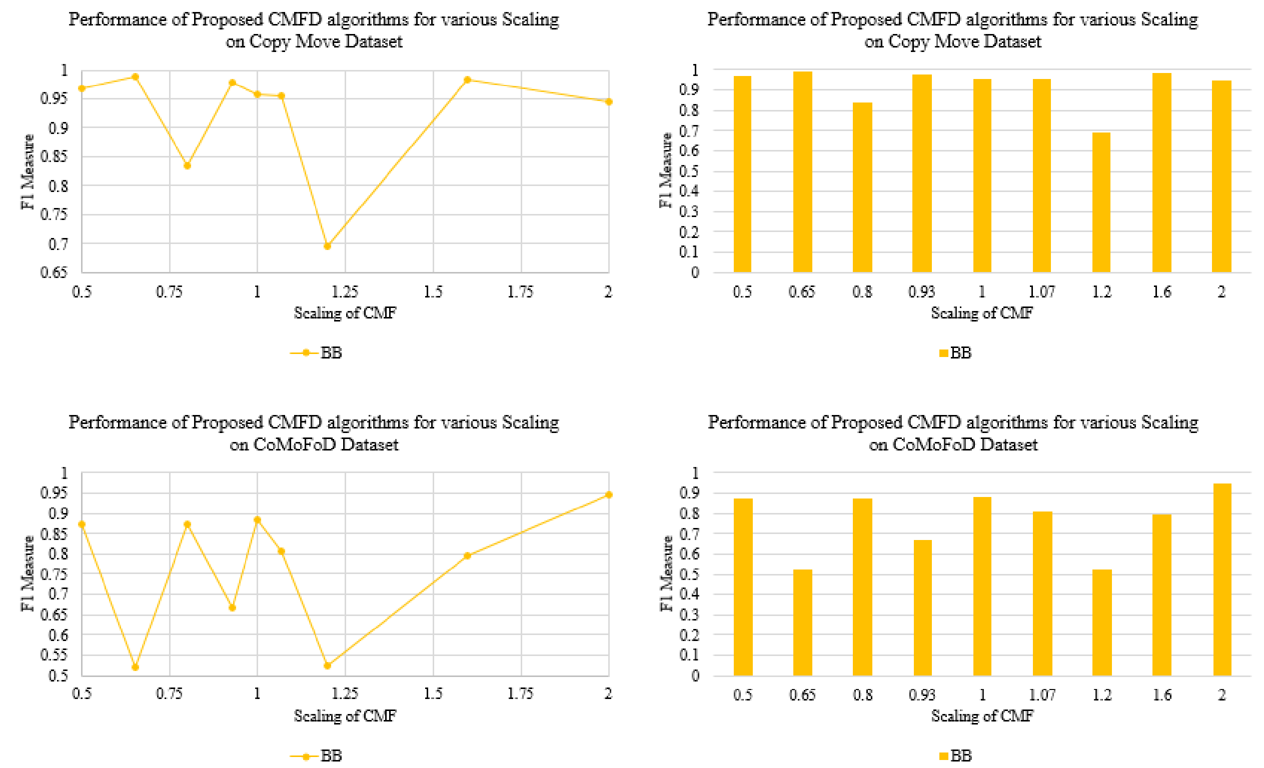


Figure 7 Performance of the proposed Zernike moments method against Scaling levels

ISSN: 2233-7857 IJFGCN

Performance of the proposed Zernike moments based method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against scaling attack at various levels (0.5, 0.65, 0.8, 0.93, 1, 1.07, 1.2, 1.60, 2 levels).

Figure 8 Performance of the proposed Zernike moments method against combinations of attack (Rotation + Scaling)

Performance of the proposed Zernike moments based method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against combinations of attack (Rotation + Scaling) at various levels ([0,0.5], [2,0.65], [4,0.8], [6,0.93], [8,1], [10,1.07], [30,1.2], [60,1.60], [90,2] levels).

COMPARISON WITH STATE OF ART TECHNIQUES

Proposed block based copy move forgery detection technique is compared with existing image forgery detection techniques to show the improvement in results.

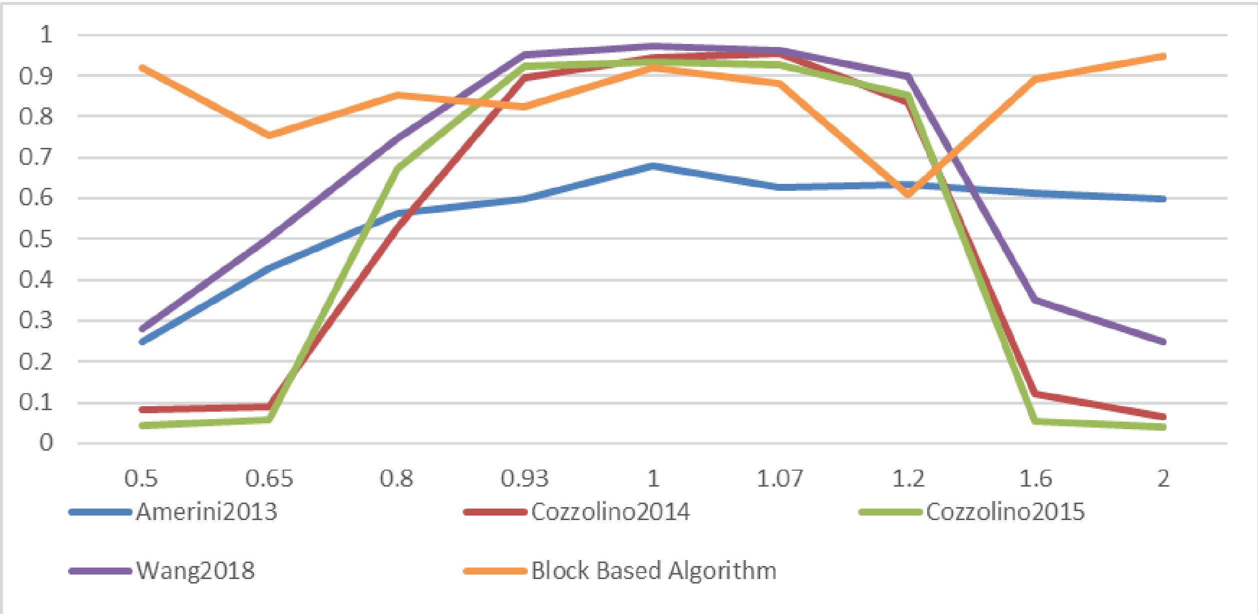


Figure 9 Comparison with other techniques

The proposed block-based CMFD technique outperformed the SIFT with highly fluctuating results for rotation angles compared to another state of the art CMFD. The proposed vital point CMFD technique outperformed the state of art technique proposed by Amerini (2013), Cozzolino (2014), Cozzolino (2015), and Wang (2018), however, has the poor results in comparison to Meena 2020.

ISSN: 2233-7857 IJFGCN

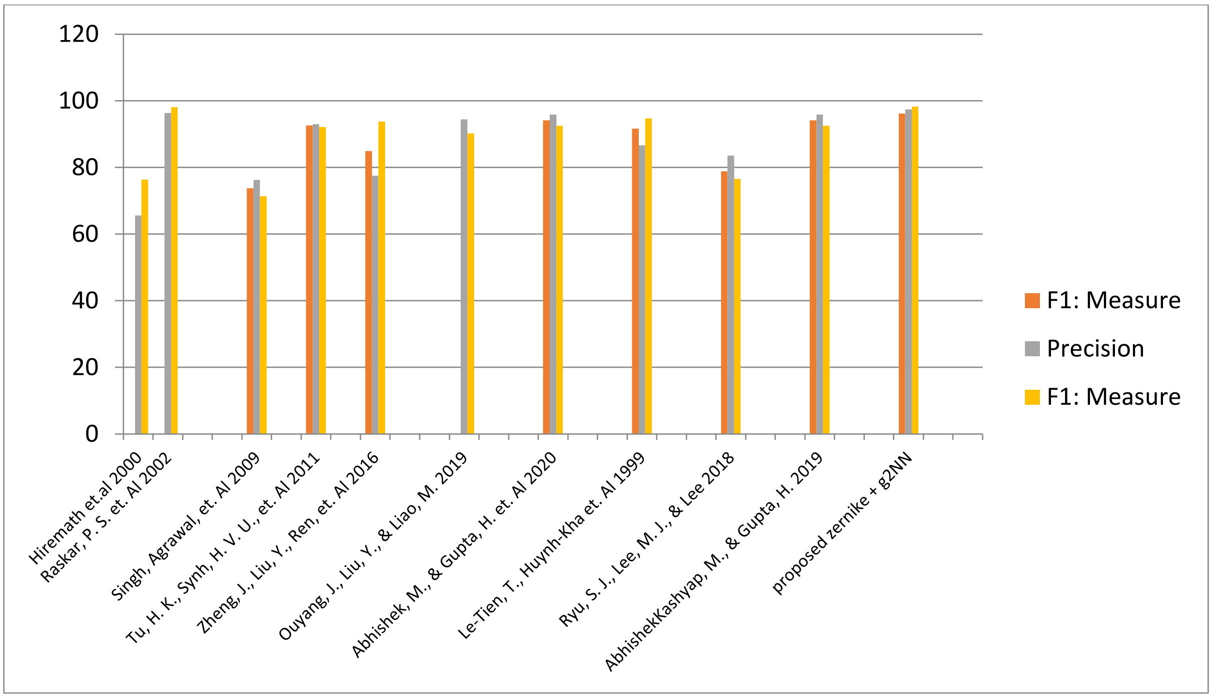


Figure 10: Comparison with state of art techniques

The proposed block-based CMFD technique outperformed as compare to the other techniques proposed by authors during a timeline. All the three majors of performance F1 measure, Precision and recall attained better results than the earlier available techniques.

CONCLUSION

Orthogonal image moments are the most popular and most efficient methods to describe an image as they can represent an image with minimum informationand are robust against noise and rotation. The reason to choose Zernike moments is that they are the most popular orthogonal moments and are invariant to arbitrary rotation. This paper presents an improved Zernike moment block based technique integrated with generalized nearest neighbour to detect image forgeries. Standard equations used to calculate Zernike moments involve lots of factorial values so are time consuming. Here author have proposed recursion equations to calculate the polynomials to reduce the computational complexity and also increase the efficiency of the algorithm. Generalized nearest neighbour is used for feature matching as g2NN is capable of detecting multiple forgeries. Performance of the proposed Zernike moments based method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against rotation attack at various angles (0, 2, 4, 6,8,10,30,60,90 degrees) and for scaling attack at various levels (0.5, 0.65, 0.8, 0.93, 1, 1.07, 1.2, 1.60, 2 levels). Performance is also presented against combinations of attack (Rotation + Scaling) at various levels ([0,0.5], [2,0.65], [4,0.8], [6,0.93], [8,1], [10,1.07], [30,1.2], [60,1.60], [90,2] levels). Comparison with existing techniques is also given to show the improvement in results.

REFERENCES

1. Mahmoud, K., &Husien, A. (2016). Copy-move forgery detection using zernike and pseudo zernike moments. Int. Arab J. Inf. Technol., 13(6A), 930-937.
2. Ryu, S. J., Lee, M. J., & Lee, H. K. (2010, June). Detection of copy-rotate-move forgery using Zernike moments. In International workshop on information hiding (pp. 51-65). Springer, Berlin, Heidelberg.
3. Mahmoud, K., &Husien, A. (2016). Copy-move forgery detection using zernike and pseudo zernike moments. Int. Arab J. Inf. Technol., 13(6A), 930-937.
4. Shivakumar, B. L., &Baboo, L. D. S. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology.

ISSN: 2233-7857 IJFGCN

5. Christlein, V., Riess, C., Jordan, J., Riess, C., &Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. IEEE Transactions on information forensics and security, 7(6), 1841-1854.
6. Zhao, Y., Wang, S., Zhang, X., & Yao, H. (2012). Robust hashing for image authentication using Zernike moments and local features. IEEE transactions on information forensics and security, 8(1), 55-63.
7. Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., & Yang, H. (2016). Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidimensional Systems and Signal Processing, 27(4), 989-1005.
8. Zandi, M., Mahmoudi-Aznaveh, A., &Mansouri, A. (2014, December). Adaptive matching for copy-move Forgery detection. In 2014 IEEE international workshop on information forensics and security (WIFS) (pp. 119-124). IEEE.
9. Ouyang, J., Liu, Y., & Liao, M. (2019). Robust copy-move forgery detection method using pyramid model and Zernike moments. Multimedia Tools and Applications, 78(8), 10207-10225.
10. Cozzolino, D., Poggi, G., &Verdoliva, L. (2014, October). Copy-move forgery detection based on patchmatch. In 2014 IEEE international conference on image processing (ICIP) (pp. 5312-5316). IEEE.
11. Hiremath, A, Bhavya, Singh,Biradar.(2018). Digital Image Forgery Detection Using Zernike Moment and Discrete Cosine Transform: A Comparison. International Research Journal of Engineering and Technology(pp.125-132).
12. Raskar, P. S., & Shah, S. K. (2019, September). A Fast Copy-Move Forgery Detection Using Global and Local Features. In 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA) (pp. 1-4). IEEE.
13. Singh, L. U. P., & Agrawal, A. (2017, October). NO-SHAM: an effective tool based on a novel hybrid approach to detect copy-move forgery in images. In 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON) (pp. 399-404). IEEE.
14. Tu, H. K., Synh, H. V. U., San, H. T., & Van Khoa, H. (2017, January). Develop an algorithm for image forensics using feature comparison and sharpness estimation. In 2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom) (pp. 82-87). IEEE.
15. Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., & Yang, H. (2016). Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidimensional Systems and Signal Processing, 27(4), 989-1005.
16. Ouyang, J., Liu, Y., & Liao, M. (2019). Robust copy-move forgery detection method using pyramid model and Zernike moments. Multimedia Tools and Applications, 78(8), 10207-10225.
17. AbhishekKashyap, M., & Gupta, H. (2018). Detection of Copy-Rotate-Move forgery using Wavelet Decomposition and Zernike moments. International Journal of Pure and Applied Mathematics, 119(12), 12955-12967.
18. Le-Tien, T., Huynh-Kha, L. P. C. H., & Tran-Hong, A. (2016, February). Block Based Technique for Detecting Copy-Move Digital Image Forgeries: Wavelet Transform and Zernike Moments. In The Second International Conference on Electrical and Electronic Engineering, Telecommunication Engineering, and Mechatronics (EEETEM2016) (p. 26).
19. Ryu, S. J., Lee, M. J., & Lee, H. K. (2010, June). Detection of copy-rotate-move forgery using Zernike moments. In International workshop on information hiding (pp. 51-65). Springer, Berlin, Heidelberg.
20. AbhishekKashyap, M., & Gupta, H. (2018). Detection of Copy-Rotate-Move forgery using Wavelet Decomposition and Zernike moments. International Journal of Pure and Applied Mathematics, 119(12), 12955-12967.

ISSN: 2233-7857 IJFGCN

21. Mahmoud, K., &Husien, A. (2016). Copy-move forgery detection using zernike and pseudo zernike moments. Int. Arab J. Inf. Technol., 13(6A), 930-937.

22. Chen, B., Qi, X., Sun, X., & Shi, Y. Q. (2017). Quaternion pseudo-Zernike moments combining both of RGB information and depth information for color image splicing detection. Journal of Visual Communication and Image Representation, 49, 283-290.

23. Chen, B., Yu, M., Su, Q., Shim, H. J., & Shi, Y. Q. (2018). Fractional quaternion zernike moments for robust color image copy-move forgery detection. IEEE Access, 6, 56637-56646.

24. Zhao, Y., Wang, S., Zhang, X., & Yao, H. (2012). Robust hashing for image authentication using Zernike moments and local features. IEEE transactions on information forensics and security, 8(1), 55-63.

25. Patel, B., &Degadwala, S. (2020). A Survey Paper on Image forgery detection Using Pseudo Zernike Moment.

26. Wang, S. H., Du, S., Zhang, Y., Phillips, P., Wu, L. N., Chen, X. Q., & Zhang, Y. D. (2017). Alzheimer’s disease detection by pseudo Zernike moment and linear regression classification. CNS & Neurological Disorders-Drug Targets (Formerly Current Drug Targets-CNS & Neurological Disorders), 16(1), 11-15.

27. Zhao, Y., Wang, S., Feng, G., & Tang, Z. (2010). A robust image hashing method based on Zernike moments. Journal of Computational Information Systems, 6(3), 717-725.

28. Mahmood, T., Mehmood, Z., Shah, M., &Saba, T. (2018). A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. Journal of Visual Communication and Image Representation, 53, 202-214.

29. Kandoriya, G. S. M. K. Copy Move Image Forgery Detection using Pseudo Zernike Moment for Better Detection Accuracy.

30. Mahmoud, K., & Al-Rukab, A. H. A. (2016). Moment based copy move forgery detection methods. Int J ComputSciInfSecur (IJCSIS), 14(7).

31. Zhang, Z., Wang, C., & Zhou, X. (2018). A survey on passive image copy-move forgery detection. Journal of Information Processing Systems, 14(1), 6-31.

32. Chen, B., Yu, M., Su, Q., & Li, L. (2019). Fractional quaternion cosine transform and its application in color image copy-move forgery detection. Multimedia Tools and Applications, 78(7), 8057-8073.

33. Elaskily, M. A., Elnemr, H. A., Dessouky, M. M., &Faragallah, O. S. (2019). Two stages object recognition based copy-move forgery detection algorithm. Multimedia Tools and Applications, 78(11), 15353-15373.

34. Hosny, K. M., Hamza, H. M., &Lashin, N. A. (2018). Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators. The Imaging Science Journal, 66(6), 330-345.

35. Su, L., Li, C., Lai, Y., & Yang, J. (2017). A fast forgery detection algorithm based on exponential-Fourier moments for video region duplication. IEEE Transactions on Multimedia, 20(4), 825-840.

36. Thajeel, S. A., &Sulong, G. B. (2013). State of the art of copy-move forgery detection techniques: a review. International Journal of Computer Science Issues (IJCSI), 10(6), 174.

37. Singh, P. K., Jana, B., &Halder, S. (2018). Copy move forgery detection through graph neighborhood degree. Int J ApplEng Res, 13(18), 13421-13427.

38. Solanki, M. G., &Kandoriya, M. K. (2016). Analysis of various copy move image forgery techniques for better detection accuracy.

39. Tom, T., Nandini, D. U., Princemary, S., &Ankayarkanni, B. (2019, October). An Improved Forgery Detection Method for Images. In IOP Conference Series: Materials Science and Engineering (Vol. 590, No. 1, p. 012032). IOP Publishing.

ISSN: 2233-7857 IJFGCN

40. Velmurugan, S., &Subashini, T. S. (2020). Patch-match based detection of copy-move forgeries using rotation invariant features. Materials Today: Proceedings, 33, 4686-4690.

41. Gan, Y., &Zhong, J. (2015). Research on copy-move image forgery detection using features of discrete polar complex exponential transform. International Journal of Bifurcation and Chaos, 25(14), 1540018.

42. Singh, S. P., &Urooj, S. (2019). A New Computational Framework for Fast Computation of a Class of Polar Harmonic Transforms. Journal of Signal Processing Systems, 91(8), 915-922.

43. Preda, R. O., Vizireanu, D. N., &Halunga, S. (2016). Active image forgery detection scheme based on semi-fragile watermarking. Revue Roumaine des Sciences Techniques-SerieElectrotechniqueetEnergetique, Romania, 61(1), 58-62.

44. Puri, D. S., & Dutta, M. (2014). A Comparative Analysis of Offline Signature Verification using Zernike Moment and Minutiae using Artificial Neural Network Approach. International Journal of Computer Applications, 101(14).

45. Ananth, J. P. (2018). Detection of Region-Duplication Forgery in Digital Images using Spectral Hashing based Legendre Moments.

46. CarrazoniEntenza, P. (2019). Copy-move forgery detection in scanned text documents using Zernike and Hu moments (Doctoral dissertation).

47. Velmurugan, S., Subashini, T. S., &Prashanth, M. S. (2020). Dissecting the Literature for studying various Approaches to Copy Move Forgery Detection. IJAST, 29(04), 6416-6438.

48. Zhao, Y., & Wei, W. (2011, June). Extraction of shape feature for image authentication. In 2011 IEEE International Conference on Computer Science and Automation Engineering (Vol. 1, pp. 404-408). IEEE.

49. Mahmood, T., Irtaza, A., Mehmood, Z., & Mahmood, M. T. (2017). Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images. Forensic science international, 279, 8-21.

50. Nandini, C. (2019). Feature based image authentication using symmetric surround saliency mapping in image forensics. International Journal of Computer Applications, 104(13).

ISSN: 2233-7857 IJFGCN