Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

A Passive Image Forgery Detection Technique

Dr. Dayanand G. Savakar[1] and Mr. Raju Hiremath[2,*]

[1] Professor, Dept. of Computer Science, Rani Channamma University, Belagavi;
dgsavakar@gmail.com

[2] Research Scholar, Dept. of Computer Science, Rani Channamma University, Belagavi;
* rajuhiremath@rcub.ac.in

Abstract

The digital image is the main source of communication in the current scenario. The digital images are miscommunicated by using various image manipulation softwares. The digital images are altered in such a way that it is difficult to understand the originality of the contents. The proposed system addresses a passive approach to image forgery detection. In this system first, the input image is partitioned into blocks. Then various features are extracted from each block like energy, entropy, contrast, homogeneity, mean, standard deviation and variance then store it to the knowledge base. Next each block features are compared with knowledge base. The proposed system identifies original and forged images accurately. The result of experiment is much better than the existing techniques.

Keywords: Passive approach, forgery, contrast, homogeneity, energy, entropy, mean, standard deviation, variance.

1. Introduction

The image is the main stream in the digital communication medium. The various types of images are shared and communicated in day-day life. Now a day because of smart tools and technology it is difficult to recognize the genuine and fake images. The various techniques are proposed to identify the originality of an image [1-14]. The various attacks are utilized to forge the image such as copy-move splicing resampling etc.,

The image forgery is nothing but manipulation or tampering of an image in such a way that it is difficult to identify. The image tampering identification methods are categorized as active and passive approach. In active methods secret code, public key and private key are used to validate the digital content. In active approach there are two forms Digital Signature and Digital Watermarking. In Digital Signature public and private key is utilized to validate the digital

document or content. In Digital Watermarking the secret code in embedded in to the digital document or image further that secret code is utilized for validation.

In passive approach there are three kinds or methods copy-move, splicing and resampling. In copy-move the portion of a digital image is copied and insert into the source image. This method is utilized to hide the content of the image or to duplicate the content of the image. The various researchers address the copy-move forgery detection [1-5,8-10,14]. In splicing method, the portion of one image is copied and insert into different image. This method is adopted to cover the part of an image or to add new content to an image. The several researchers proposed the splicing forgery detection techniques [6,11]. In resampling method, the rotation or resized or scaling operation is performed in an image. The some of the authors presented the technique based on resampling method [13].

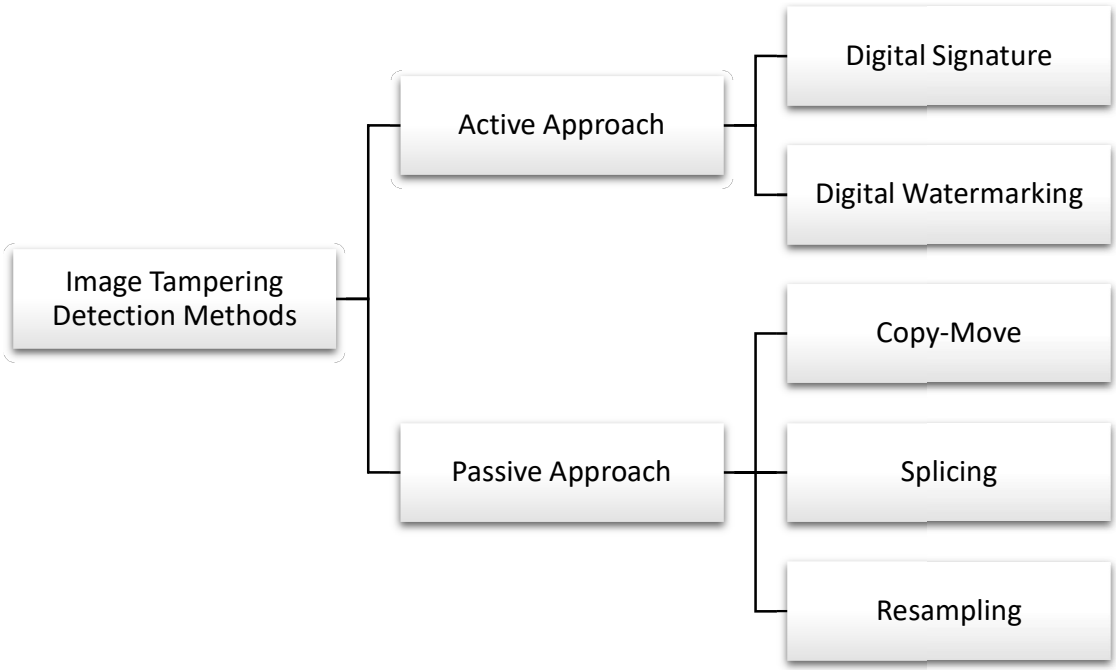

Fig. 1. Image Forgery Detection Methods

The rest of the paper is arranged as follows. Section 2 and 3 gives the related work and proposed methodology. Section 4 gives result and discussion and section 5 gives conclusions.

2. Related Work

The many research work conducted on passive image tampering identification [1-14]. In this paper the passive approach image forgery detection technique is addressed. The passive image forgery detection approach is classified as copy-move, splicing and resampling techniques.

2.1 Copy-move image forgery

The copy-move forgery detection technique is frequently used technique. The various researcher proposed techniques to identify the copy-move forgery in an image [1-5,8-10,14]. The various research work has been carried out to detect copy-move forgery detection using different techniques such as Convolution Neural Network [1,7], Discrete Cosine Transformation [1], Entropy [9], etc., The author Yanfen Gan et. al [14]presented the fusion technique for identification of duplicate forgery with the help Radial Harmonic Fourier Moments and SIFT. In this technique SIFT is used for extracting the features, then the unwanted features are removed using the adaptive Euclidian distance, nearest neighbor and Random sample consensus. Next the input image is segmented into texture patches using Simple Linear Iterative Clustering technique. Finally, the geometric operations are performed. The proposed system achieved good performance as compared with other techniques.

The author [5] proposed the block-based copy-move tamper identification technique using DCT, cellular automata and patch match. In this technique Discrete Cosine Transformation and cellular automata is utilized for fetching the features from an image. Then the features are matched using patch matching technique. The proposed system produced good result in terms of accuracy. The improved copy-move image tampering identification method is proposed by B. Rakesh Babu and Dr. S. Narayana Reddy [1] based on deep learning approach. In this technique the features are fetched with the help of CNN and the extracted features are matched utilizing Deep learning technique. The proposed system detects and localized forged part in an image with good accuracy.

2.2. Splicing forgery detection

The splicing forgery is nothing but the portion of one image is copied and insert into different image. The researcher proposed the splicing forgery detection techniques [6,11] using different techniques. The author Nam Thanh Pham et. al [11] presented hybrid image retrieval technique for detecting the image splicing forgery. In this method the first phase is image retrieval, in which the image is segmented into background part and spliced part. Then the SIFT and Zernike moment features are extracted. Finally, the regions are matched using various manipulation operations. The proposed method efficiently retrieved the spliced part of an image. The author [6] proposed an enhanced image tamper identification technique employing MWC-Net (Multi-task Wavelet Corrected Network). In this technique the MWC-Net is utilized to wavelet up-pooling and wavelet pooling for compression and reconstruction of features of splicing forged images. Then the MWC-Net employs multi-task approach for enhancing the ability of the learning. The experiment result shows good result for identification and localization of the splicing forgery is good related to the other techniques.

2.3 Resampling forgery detection

The image forgery detection of type resampling is nothing but the rotation, resizing and scaling operation is performed on the image. The A. Flenner et. al [13] proposed the resampling counterfeit identification technique sourcing A-Contrario analysis and deep learning. In this technique there are three phases are there. In -first phase from the image blocks resampling features are evaluated. In the second phase the heat map is generated using deep learning classifier which specifies the resampled image block. In the last phase a-contrario hypothetical testing technique. The proposed system competently identifies and locates the resampling forgery in an image.

3. Proposed method

The proposed technique addresses a passive forgery detection method. In this technique first input the original or forged image as Img. Then the block-based technique is adopted. The block size is assigned as 5. Next the binary image of the original or forged image is created and opened for writing the data into the file. The Img is divided to R, G, B channel blocks. Then the contrast, homogeneity, energy, entropy, mean, standard deviation and variance features are extracted from each block. Next save the features to the knowledge base.

3.1 Feature Extraction

The different types of texture and statistical features are extracted such as contrast, homogeneity, energy, entropy, mean, standard deviation and variance. The various notations are used for evaluation of the texture features are as follows.

$p(i,j)$	-	*Element (i,j) in GLCM (Gray Level Co-occurrence Matrix)*	
N	-	*Number of gray levels in the quantized image*	
$p_x(i)$	-	$\sum_{j=1}^{N} p(i,j).$	Equal for symmetric GLCM
$p_y(j)$	-	$\sum_{i=1}^{N} p(i,j).$	
$q(i,j)$	-	$\sum_k \frac{p(i,k)p(j,k)}{p_x(i)p_y(k)}$	
μ_x	-	$\sum_{i=1}^{N} i.p_x(i)$	μ, Equal for symmetric GLCM
μ_y	-	$\sum_{j=1}^{N} j.p_y(j)$	
σ_x^2	-	$\sum_{i=1}^{N}(i-\mu_x)^2.p_x(i)$	σ^2, Equal for symmetric GLCM
σ_y^2	-	$\sum_{j=1}^{N}(j-\mu_y)^2.p_y(j)$	

The equations utilized to calculate the textual features of an image is showed in Table 1.

Table 1

The different textual features and their equations

Function Name	Equation	Reference No
Energy	$\sum_{i=1}^{N}\sum_{j=1}^{N} p(i,j)^2$	15
Contrast	$\sum_{i=1}^{N}\sum_{j=1}^{N} (i-j)^2 p(i,j)$	15
Homogeneity	$\sum_{i=1}^{N}\sum_{j=1}^{N} \frac{p(i,j)}{1+(i-j)^2}$	15
Entropy	$\sum_{i=1}^{N}\sum_{j=1}^{N} p(i,j)logp(i,j)$	15

The statistical features are extracted from each block as described as follows.

Mean: The average values of the pixels of each block [16].

$$i_m = \frac{1}{K} * \sum_{k=1}^{K} i(k) \qquad (1)$$

Standard Deviation: The Deviation from the mean of pixel values of each block [16].

$$i_{sd} = \sqrt{\frac{\sum_{k=1}^{K}(i(K)-i_m)^2}{(K-1)}} \qquad (2)$$

Variance: The Square of the Standard Deviation [16].

$$i_v = \frac{\sum_{k=1}^{K}(i(K)-i_m)^2}{(K-1)} \qquad (3)$$

The extracted features are stored into binary file. After feature extraction each block features are matched with all blocks. If matched blocks are greater than 10 then the image is identified as forged. Otherwise, the image is original.

3.1 Algorithm: A Passive image forgery detection technique

Input: Input image

Output: Display Original or Forged Image

Start

Step1: Read image as Img

Step2: Assign Block size Bsize=5

Step3: Create the binary file as Img_bfile.asv

Step4: Divide the Img into R, G, B Channel blocks rbk, gbk, bbk

Step5: Extract contrast, homogeneity, energy, entropy, mean, standard deviation and variance features from each block rbk, gbk, bbk

Step6: Save the features to knowledge base as ffile

Step7: Compare the features of each block to the knowledge base

Step8: If matched_block > 10 then

Display “Forged Image”

Else

Display “Original Image”

End if

Stop

3.2 Methodology

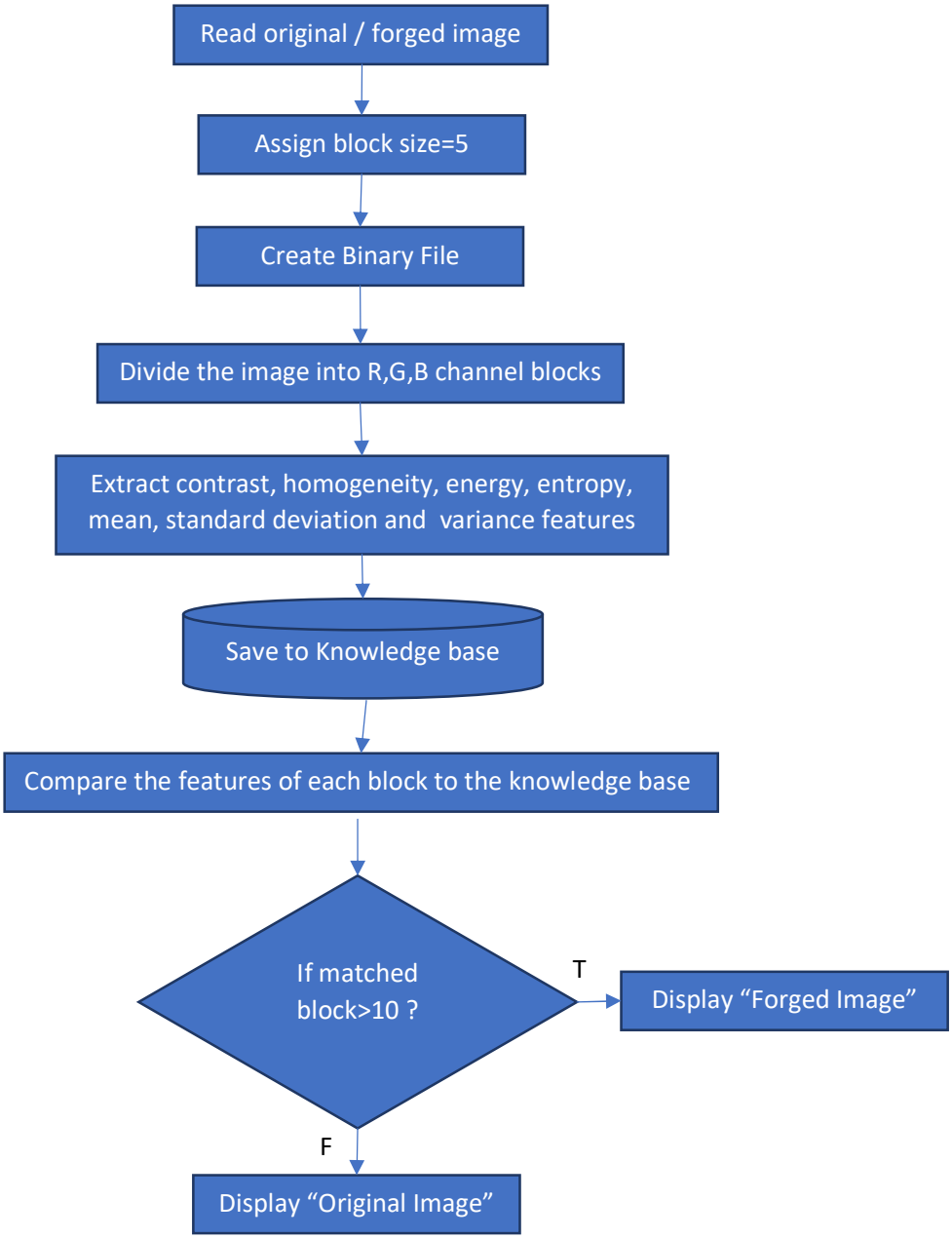

Fig. 2. The proposed methodology

4. Result and Discussions

The testing the proposed system our own dataset will be utilized. In this dataset total 100 images are there, in those original 50 images and forged 50 images.

Performance evaluation

The performance of the proposed system is analyzed by calculating the accuracy of the result obtained. The accuracy is evaluated by sum of correctly recognized original images and the sum of correctly recognized forged images which is divided by sum of correctly recognized original and forged images added with sum of wrongly recognized original and forged images. The accuracy (Ac)of the proposed system is evaluated using the Eq (4). The confusion matrix used for performance measure is shown in Table 2.

$$\text{Ac}=\frac{TP+TN}{TP+FN+FP+TN} X\ 100 \qquad (4)$$

Where,
TP=The sum of correctly recognized original images.
TN= The sum of correctly recognized forged images.
FP=The sum of wrongly recognized original images.
FN= The sum of wrongly recognized forged images.

Table 2
Confusion matrix

Predicted Value	**Actual value**	
	Positive	Negative
Positive	True Positive	False Positive
Negative	False Negative	True Negative

TP= True Positive, TN= True Negative, FP= False Positive

Table 3
Comparison of our method with other methods.

Author(s)	**Forgery Type**	**Ac**
B. Rakesh Babu1, Dr. S. Narayana Reddy [1]	Copy-Move	95.02%
Muhammad Naveed Abbas et al [4]	Copy-Move	87.00%
Dayanand G. Savakar and Raju Hiremath [9]	Copy-Move	94.29%
Nam Thanh Pham et.al [11]	Splicing	84.89%
Ritu Agarwal and Mallika Pant [12]	Copy-Move and Splicing	93.33%
Proposed method	Copy-Move	96.00%

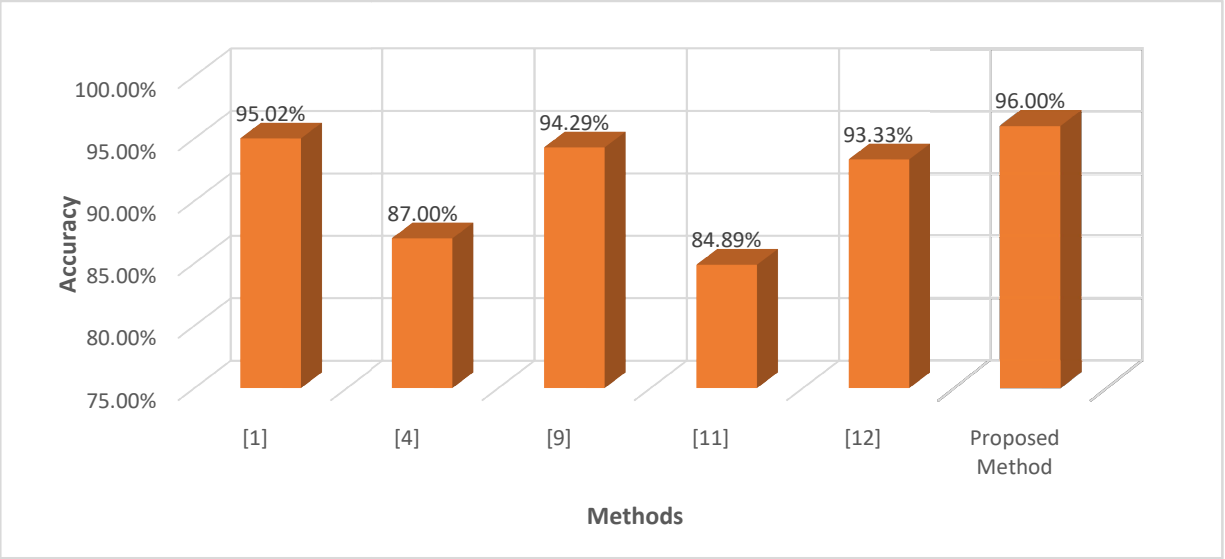

Fig. 3. The comparison of accuracy with other methods

5. Conclusion

The passive image forgery detection technique is frequently used forgery types. In which one of the popular types of forgery copy-move forgery is addressed. In suggested system first the image is partitioned into blocks then, the different texture features like contrast, energy, entropy, homogeneity and statistical features like mean, standard deviation and variance extracted from each block. Then the extracted features are stored into the knowledge base. Next the features of each block are compared with knowledge base. If the more than 10 blocks are matched then it displayed as forged image or else it displayed as original image. The proposed system higher accuracy compared with other methods.

References

[1] B. Rakesh Babu and Dr. S. Narayana Reddy, "Copy – Move Forgery Detection in Digital Images Based on deep Learning", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Volume 10, Issue 2, February 2021, DOI:10.15680/IJIRSET.2021.1002028, pp:856-859.

[2] V.Shiva Narayana Reddy, K. Vaghdevi and Dr. Kamakshaiah Kolli, (2021), "Digital Image Forgery Detection Using Super Pixel Segmentation And Hybrid Feature Point Mapping", European Journal of Molecular & Clinical Medicine, Volume 08, Issue 02, 2021, pp:1485-1500

[3] Sharanjit Kaur and Manpreet Kaur, "Novel Method for Copy-Move Forgery Detection", International Journal of Computer Applications (0975 – 8887) Volume 174 – No. 18, February 2021, pp.10-14

[4] Muhammad Naveed Abbas, Mohammad Samar Ansari, Mamoona Naveed Asghar, Nadia Kanwal, Terry O`Neill and Brian Lee (2021), "Lightweight Deep Learning Model for Detection of Copy-move Image Forgery with Post-processed Attacks", SAMI 2021 • IEEE 19th World Symposium on Applied Machine Intelligence and Informatics, 978-1-7281-8053-3/21/$31.00 ©2021 IEEE, pp.125-130.

[5] Gulnawaz Gani, Fasel Qadir (2021), Copy move forgery detection using DCT, PatchMatch and cellular automata", Multimedia Tools and Applications https://doi.org/10.1007/s11042-021-11174-7.

[6] Xiuli Bi,Zhipeng Zhang, Yanbin Liu, Bin Xiao and Weisheng Li, "Multi-Task Wavelet Corrected Network For Image Splicing Forgery Detection And Localization", 2021 IEEE International Conference on Multimedia and Expo (ICME), 2021, pp. 1-6, DOI: 10.1109/ICME51207.2021.9428466

[7] Amit Doegar, Srinidhi Hiriyannaiah, G. M. Siddesh, K. G. Srinivasa and Maitreyee Dutta, "Cloud-Based Fusion of Residual Exploitation-Based Convolutional Neural Network Models for Image Tampering Detection in Bioinformatics", Hindawi BioMed Research International Volume 2021, Article ID 5546572, pp.1-12, https://doi.org/10.1155/2021/5546572.

[8] Yi-Lin Tsai and Jin-Jang Leou, "Image Copy-Move Forgery Detection using Color Features and Hierarchical Feature Point Matching", In Proceedings of the International Conference on Image Processing and Vision Engineering (IMPROVE 2021), DOI: 10.5220/0010492301530159, pp.153-159

[9] Dayanand G. Savakar and Raju Hiremath, "Copy-Move Image Forgery Detection Using Shannon Entropy", © Springer Nature Singapore Pte Ltd. 2020 B. Iyer et al. (eds.), Applied Computer Vision and Image Processing, Advances in Intelligent Systems and Computing 1155, https://doi.org/10.1007/978-981-15-4029-5_8, pp.76-90.

[10] Saif alZahir and Radwa Hammad, "Image forgery detection using image similarity", Multimedia Tools and Applications, 2020, https://doi.org/10.1007/s11042-0 20-09502-4

[11] Nam Thanh Pham, Jong-Weon Lee, Goo-Rak Kwon and Chun-Su Park, "Hybrid Image-Retrieval Method for Image-Splicing Validation", Symmetry 2019, 11, 83, pp.1-15, doi:10.3390/sym11010083

[12] Ritu Agarwal and Mallika Pant, "Image tampering detection using genetic algorithm", MATEC Web of Conferences 277, 02026 (2019), JCMME 2018, https://doi.org/10.1051/matecconf/201927702026

[13] A. Flenner, L. Peterson, J. Bunk, T. M. Mohammed, L. Nataraj and B.S. Manjunath, "Resampling Forgery Detection Using Deep Learning and A-Contrario Analysis", IS&T International Symposium on Electronic Imaging 2018 Media Watermarking, Security, and Forensics 2018, pp. 1-7, https://doi.org/10.2352/ISSN.2470-1173.2018.07.MWSF-212

[14] Yanfen Gana, JimleeChungb, Janson Youngc, Zixin Hub and Jinhong Zhao, "A Duplicated Forgery Detection Fusion Algorithm using SIFT and Radial-Harmonic Fourier Moments", International Journal of Performability Engineering, 2018, pp. 111-120

[15] Patrik Brynolfsson, David Nilsson, Turid Torheim, Thomas Asklund, Camilla Thellenberg Karlsson, Johan Trygg, Tufve Nyholm and Anders Garpebring, "Haralick texture features from apparent diffusion coefficient (ADC) MRI images depend on imaging and pre-processing parameters", Scientific Reports,2017 | 7: 4041 | DOI:10.1038/s41598-017-04151-4, pp.1-11.

[16] Sanyam Shukla, R. N. Yadav, Jivitesh Sharma and Shankul Khare, "Analysis of Statistical Features for Fault Detection in Ball Bearing", 2015, DOI: 10.1109/ICCIC.2015.7435755