Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777177

PERFORMANCE ANALYSIS OF ALGORITHMIC APPROACH OF ROTATION INVARIANT FORGERY DETECTION USING LBP VARIANTS

Dr Gurpreet Kaur
Assistant Professor in Computer Science, Asian Group of Colleges, Patiala
Kripakalra85@gmail.com

Abstract:
The principal method used for digital image forgery is Copy-move forgery (CMF). The replicated region may be rotated or flipped to appropriate the scene enhanced for copy-move forgery. In copy–move image forgery, a section from certain image position is replicated and fixed to a different position of the similar image. Typically, post-processing is applied in order to conceal the forgery. The existing forgery detection methods, which generally follow a common procedure especially for copy- move forgery detection are: (1) pre-processing in which forged images are converted to gray space or color space (2) feature extraction in which where features are extracted from different image regions (e.g., overlapped blocks), (3) feature matching, which obtains matched features to determine the original, suspected forgery regions, and (4) post-processing, which discards inconsistently matched pixels or outliers from matched region and only uses the left pixels to obtain the final forgery detected output. As feature extraction majorly affects the accuracy of detection, such methods are generally categorized into three main types named as block-based methods, segmentation-based methods and key point-based methods. In block-based detection methods, the input image is divided into overlapping regular image blocks, and then a descriptor of each block is calculated by various transforms. To extract features that are not affected by normal distortions (e.g., JPEG compression and noise addition) or geometric-distortions (e.g., rotation and scaling), transforms such as the, Principle Component Analysis (PCA) , (PCET) Moment and YCbCr color, Discrete Wavelet Transform (DWT) , Histogram of Orientation Gradient (HOG) ,Discrete Cosine Transform (DCT), Zernike Moment , Krawtchouk Moment , Fourier–Mellin Transform, Signal Value Decomposition (SVD), Polar Cosine Transform (PCT) , and 1-D reflection/rotation-invariant descriptors are applied to blocks to calculate block features [2].
Keywords:- — Block Based Forgery Detection, Mean, Variance, DCT

1. INTRODUCTION

The images in digital format could be manipulated via forgery that conveys false information without any trait of evidence. A number of available software is dedicated to aid in the conventional approach of forgery, i.e. copy-move-rotate (CMR). The forging is defined as "The production of fraudulent copy or imitation of a document, signature, banknote or a work of art". In the domain of digital images, the forgery is the state of art classified in two models additive approach and subtractive approach based on the content of the original image. The additive approach copies a segment of random image (or same image) and mixes it with the original image to enhance original information. The subtractive approach clips a part of information from the original image. Here, the classification of forgery is for purposes strictly in relation to theoretical studies of the problem and many researchers have addressed the manipulation of the original image information in their work irrespective of classification.

In an example of subtractive forgery, the original picture of Joseph Stalin and Nikolai Yezhov was forged and Nikolai Yezhov was erased from the picture (Figure 1.1) newspaper published the altered image from three images that showed a white house in the background of the two presidents Bill Clinton and Saddam Hussain (Figure 1.2). This image involved copy and move approach as the images for forgery were secured from different images. In an example of involvement of rotation of a forged image, an additive forging of four missiles instead of three missile launching image was in the newspapers a few decades ago . Here, the fourth missile (outlined by a black line) is the maneuvering missile (in white outline) to forge the image (Figure 1.3) This forgery involved the manipulation of the image without any geometric changes. For this particular image, the requirement of rotation does not seem valuable; yet the artists with little computational knowledge introduced rotation in an image that makes it difficult for a naked eye to identify the source of forging. Figure 1.4 depicts the factor of rotation to enhance the precision in forgery. The jet was tilted that convinced the false originality of the image

Figure 1.1: Subtractive forging of Joseph and Nikolai Yezhov (a) Original image (left) (b) Forged image (Right)

INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

1 2 3

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agensies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

Figure 1.2: The altered image of two political legends (1) Original image of Saddam Hussain (2) The white house (3) Original image of Bill Clinton

Figure 1.3: Copy–move forgery image of Iranian missiles

The white outlined missile is the original image that was manipulated to create a fake missile (black outline).

The original image in Figure 1.4 consists of two prime subjects. The jet from this image was copied and pasted in the same image that creates the false impression on viewers about the number of jets buzzing around. The fake image of the jet went through further modification and rotation was introduced in it. In the final image, the involvement of rotation reflected more originality than image (b).

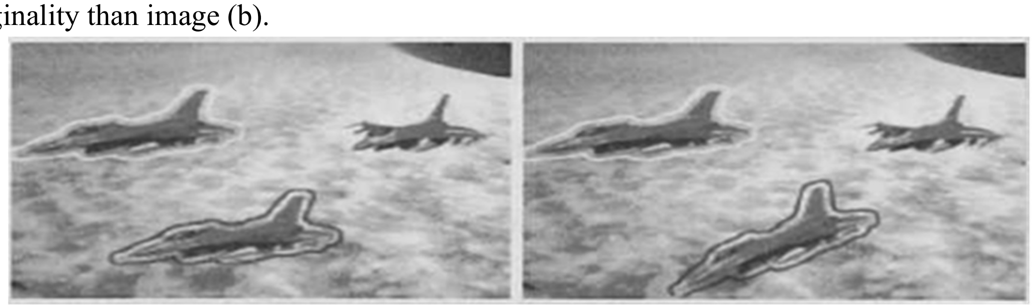

Figure 1.4: Demonstration of forgery with copy and rotational approach (a) the original image (b) Image in white outline copied and pasted in same image (black outline) (c) Image tilting enhance false originality of the image

1.2 Copy-move forgery detection techniques

The problem of copy-move forgery detection problem has attracted a large number of researchers and in the literature there a number of published papers on this problem. This section categorizes the existing copy-move forgery detection algorithms according to the extracted features that are used for classifying the image as authentic or forged.[5]

Most of the copy-move forgery detection algorithms divide a given image into small fixed size overlapping blocks to extract the image features, which are saved in feature vectors. These vectors are then sorted lexicographically and compared to find the similarity between two successive vectors and detect the corresponding copied regions. A threshold is also used to decide the similarity of vectors.

1.2.1 Texture and Intensity based Algorithms

Texture is an important feature for image classification and recognition. Image intensity has been widely used for feature extraction. The main advantage of exploiting texture and intensity is to extract the relevant and discriminatory information for classification.

The early work in this category was done by Langille and Gong [15]. They proposed a method that is based on similar intensity patterns for similar blocks. They used a kdtree to reduce the computational complexity.

1.2.2 SVD based algorithms

Singular value decomposition (SVD) is a matrix factorization technique that is used to extract algebraic and geometric features from an image. SVD features have been widely used to detect copy-move forgery due to their stability, and scaling and rotation invariance. SVD [14] was applied to extract the algebraic and geometric features from small overlapping image blocks to produce a features matrix based on SVD. This matrix was then reduced by reduced-rank approximation before checking the similarity of vectors. The dataset used for evaluation was only 100 images, which indicates that the method evaluation is very poor.

1.2.3 PCA-based algorithms

Principle Component Analysis (PCA) is also a candidate to extract image features and has been used to detect copy-move forgery. In this procedure, a feature vector is extracted by the eigen-analysis of the covariance matrix of block vectors. For this purpose, a duplication map is defined to produce a zero image of the same size as the original and all pixels in a duplicated region are assigned a unique grayscale value. With the reduced dimension of the PCA representation Nt and total number of image pixels N, the algorithm has complexity of O(NtNlogN). Mahdian and Saic[65] tried to improve Popescu's algorithm by combining PCA and kd-tree.

1.2.4 DCT-based algorithms

Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are popular techniques to transform an image into the frequency domain before extracting its features. DCT was proposed as a new approach for copy-move forgery detection in 2003 and was developed with DWT as a pair of effective transformations in image processing, especially in the detection of forged images. Several researchers used DCT coefficients to extract the texture of an image. They sort DCT coefficients lexicographically to reduce the cost of computation and the complexity of comparisons, and then apply a block matching technique for copy-move forgery detection.

1.2.5 Algorithms based on invariant key-points

Non-block-based techniques such as Scale Invariant Feature Transform (SIFT), and SURF [15], were used by different researchers to extract distinctive local level features in the image. Although these techniques have reduced computation complexity, they have poor accuracy when scaling and rotation transformations are applied as post-processing operations on a copied region.

1.2.6 Algorithms based on invariant key-points

Non-block-based techniques such as Scale Invariant Feature Transform (SIFT), and SURF [11], were used by different researchers to extract distinctive local level features in the image. Although these techniques have reduced computation complexity, they have poor accuracy when scaling and rotation transformations are applied as post-processing operations on a copied region.

2. Background of the Problem statement

There are few issues in the realm of forgery detection. Numerous recognition systems bring tampering pieces of information from better places, for example, color filter array, source light direction, sensor noise JPEG blocking, camera reaction, and so on. Therefore, large portion of them are not suitable for detecting duplication regions. The intention is to have the copied region from the same picture, which may have identical qualities with the original picture. Additionally, the above procedures simply check the genuineness of a picture; they do not have the capacity of naming the altered regions. Another issue is the multi-layered computational nature of the detection method. Since there is no clue about the size, area and state of the duplicated regions, there are practically a boundless number of methodologies to determining the picture into self-confident areas and the computational nature will make the detection farfetched. The post processing like blurring and JPEG compression will be the final problem, which may hide the altering imitations. The main problem with existed copy move methods that they fail when copy moved patch is rotated and placed in the image. For this issue rotation invariant methods of feature extraction need to be explored. Therefore, DCT, DWT, LBP (Rosin et al. 2016) etc. feature extraction algorithms will be decided to work on in our research work. There are many variants of LBP found which shows effective results in texture analysis i.e. Median LBP, RLBP, and DRLBP (Rosin et al. 2016) etc.

3. Objectives

Copy-Move forgery or Region-duplication forgery is one of most common tampering techniques. In copy-move forgery, some parts of the image are copied and then pasted in the same image (with possible transformations) for duplicating or concealing objects from images. The key idea of copy-move forgery detection is to divide the image into small blocks, extract the invariant features, and find similar block pairs. In the last decade, various copy-move forgery detection (CMFD) algorithms have been proposed, which can be classified into two main categories: block-based methods and keypoint-based methods (or visual feature-based methods) but CMFD methods fail when the copy region is moved after rotation. Local binary patterns are texture feature extraction technique which is used to classify the images according to content in it. Traditional LBP can be amended to make it rotation invariant hence can be applied in copy-move-rotation forgery detection. So following objectives has been set to reach our aim of copy-move-rotation forgery detection.

- To study and implement various LBP variant approaches i.e. OC-LBP, CS- LBP, RLBP, DRLBP, MLBP etc.
- To implement Gabor and Sobel edge enhancement and edge detection methods to get the binary edge image and to use them in matching process in order to reduce computation time
- To extract the texture features using DCT features for copy-move forgery and rotation-invariant LBP variants for rotation-copy-move forgery by dividing the images into blocks and to concatenate them for feature classificationTo evaluate the performance of the algorithm in terms of sensitivity, specificity and accuracy parameters.

Research methodology

The general process of copy-move forgery detection used in earlier approaches consists of the following steps.

Step 1 Divide the input image into overlapping blocks. Step 2 Produce feature vectors from blocks.

Step 3 Sort the feature vectors lexicographically. Step 4 Find duplicate vectors.

Step 5 Perform block matching. Step 6 Detect the forgery.

From a given image, feature vectors are extracted directly based on statistical analysis of pixels, singular value decomposition, intensity of pixels, radon transformation, local binary patterns, etc. Many methods are robust against the post-processing operations, such as blurring, filtering, JPEG compression, Gaussian noise and geometric transformation (rotation and scaling). Copy-move forgery detection algorithms are classified according to their strengths and weaknesses in the next subsections.

4. Proposed Work

Nowadays, digital images are used widely in numerous areas in our lifecycle for
`instance forensics sciences, news reports, online marketing and medical diagnosis. Furthermore, these could be used as evidence in courts, and in the media to transform the sense of images with the purpose of affecting the readers' points of observations. Therefore, the region of digital image forensics to state the originality of digital image has come to be a

significant area of investigation to regain belief in digital image . At the present time, it is simple to generate image forgeries by commanding present digital image processing software packages. Image Forgery is of two types: copy- move forgery and splicing forgery. In copy-move forgery, portions of one image are copied and then pasted into the image itself, whereas in splicing forgery; portions of one or more images are copied and then pasted into a different image.The principal method used for digital image forgery is Copy-move forgery (CMF). The existing forgery detection methods, which generally follow a common procedure especially for copy-move forgery detection are: (1) pre-processing in which forged images are converted to gray space or color space (2) feature extraction in which where features are extracted from different image regions (e.g., overlapped blocks), (3) feature matching, which obtains matched features to determine the original, suspected forgery regions, and (4) post-processing, which discards inconsistently matched pixel and obtain the final forgery detected output. As feature extraction majorly affects the accuracy of detection, such methods are generally categorized into three main types named as block-based methods, segmentation-based methods and key point-based methods. In block-based detection methods, the input image is divided into overlapping regular image blocks, and then a descriptor of each block is calculated.So,In the existing algorithms, the feature vector matching contains two main steps. Firstly, lexicographically sorting is applied to all feature vectors. The next step is to compare the feature vectors based on the sorted results. In fact, the above mentioned two steps may generate a large number of false positives that will affect the detection results and their time complexity is unsatisfactory. In the proposed method, the idea of package clustering algorithm is used to replace the lexicographically sorting to improve the detection precision and reduce the times of feature vector comparing for any two blocks. For any two blocks, their pixel values are similar and the means of them are basically identical if the two blocks are duplicated. Then, the two blocks belong to a same cluster and their feature vectors should be put into a same package. In the same manner, all blocks and their feature vectors can be put into different packages according to the means of pixel values of blocks by adopting the idea of package clustering algorithm. We can match the feature vectors of any two blocks that belong to a same package to determine whether the two blocks are similar and then the duplicated regions can be located. In the package clustering algorithm, the matching times of each block in a package is proportion to the offset of the packages and the detection precision is inverse with the offset of the packages.

So the main weakness of the block-based methods is that the computational complexity of the dense field CMFD method is relatively high because all pixels must be examined. In some recently proposed CMFD methods, the robustness problem has been solved to some extent but the computational complexity of CMFD methods, which consists mainly of the cost of calculating features and matching them has not proven yet. Almost all existing CMFD methods use exhaustive searching of the features to obtain matched features. Exhaustive searching can obtain exactly matched

features that can easily generate the final detected regions in post-processing. However, the computational complexity of exhaustive searching is directly related to the number of features. Whether block-based, keypoint-based or segmentation- based, almost all CMFD methods aim to reduce the number of features to decrease the computational time. Also CMFD methods fails when there is rotation of copy-move region which is major challenge among the researchers. In order to reduce computation time and to increase detection accuracy of forgery for CMFD, Soble- edge and DCT based algorithm is proposed. At first edge detection is carried out to get the high entropy pixels in the image so that matching process is carried out only for high entropy pixel blocks. Then feature extraction is carried out by converting image into overlapped blocks and mean and DCT features are extracted. Then mean values are put into a matrix and corresponding blocks are noted. Then mean value matrix is sorted in order to match the blocks with similar mean values. In matching process, variance of DCT features is used for similarity measure and forgery detection. Experimental results show that proposed method has high accuracy of forgery detection which comes in range of 97 to 99% along with least computation time. As this algorithm is highly efficient for CMFD only but for not copy-move-rotation forgery detection (CMRFD), a rotation invariant feature extraction is proposed using Zernike moments and local binary patterns. In this method, first image is divided into overlapped blocks in which Zernike moments are calculated first by rotating block pixels into different directions. Then rotated block with minimum value of Zernike moments is evaluated for which LBP features are extracted. Similar procedure is followed for all blocks. For matching process, mean values of block pixels is used after sorting them in an array. For similar mean value blocks, matching process is carried out by taking the variance difference of LBP features. Blocks with similar variance values are marked as forged pixels in the image. For decreasing the time complexity, edge detector is used which gives edge binary image for high gradient pixels in the image. First matching is carried out for edge pixel blocks only. Then in post processing, morphological operations are used and again matching procedure is followed to get the forged pixels in the image. Results are validated using a standard CoMoFoD dataset which contains images for both CMFD as well as CMRFD .Experiment results are carried out on a standard dataset in which detection accuracy (DA) and false positive rate (FPR) are used for performance evaluation. Results show high value of detection accuracy and lowest false positive rates.

5. Performance Evaluation

The number of pixels detected after presented forgery detection method and the ground truth image provides the effectiveness of the presented method based on sensitivity of forged pixels and specificity of rest of the image which considers as background portion. Hence Detection Accuracy (DA) which defines sensitivity parameter and False Positive Rate (FPR), which defines background portion which comes as forged region can effectively represent the accuracy of forgery detection by proposed method. The formula for both DA and FPR is given as under .Detection Accuracy (DA) is the percentage of (actually) copy–move-rotated pixels in an image, which are accurately detected by a particular region duplication detection method to be copy–move-rotated. Higher efficiency implies higher detection accuracy.

$$DA = \frac{\#Correctly\ \det ected\ copy - move - rotation\ pixels}{\#\ actually\ copy - moved - rotaion\ pixels} \times 100\% \quad (1)$$

Or in terms of true positive, false positive, false negative parameters, these parameterscan be defined as follows:

False Positive Rate (FPR) is described as the total number of actual image pixels,incorrectly detected to be forged, and formulated as:

$$FPR = \frac{\#incorrectly\ \det ected\ copy - move - rotationpixels}{\#\ actually\ copy - moved - rotation\ pixels} \times 100\% \quad (3)$$

Similarly FPR can be defined as

Where true positive is correctly detected pixels as forged, False-positive as incorrectly detected forged pixels and false negative as incorrectly detected non-forged pixels; Forgery detection results for tested images are shown below in figure 1.4

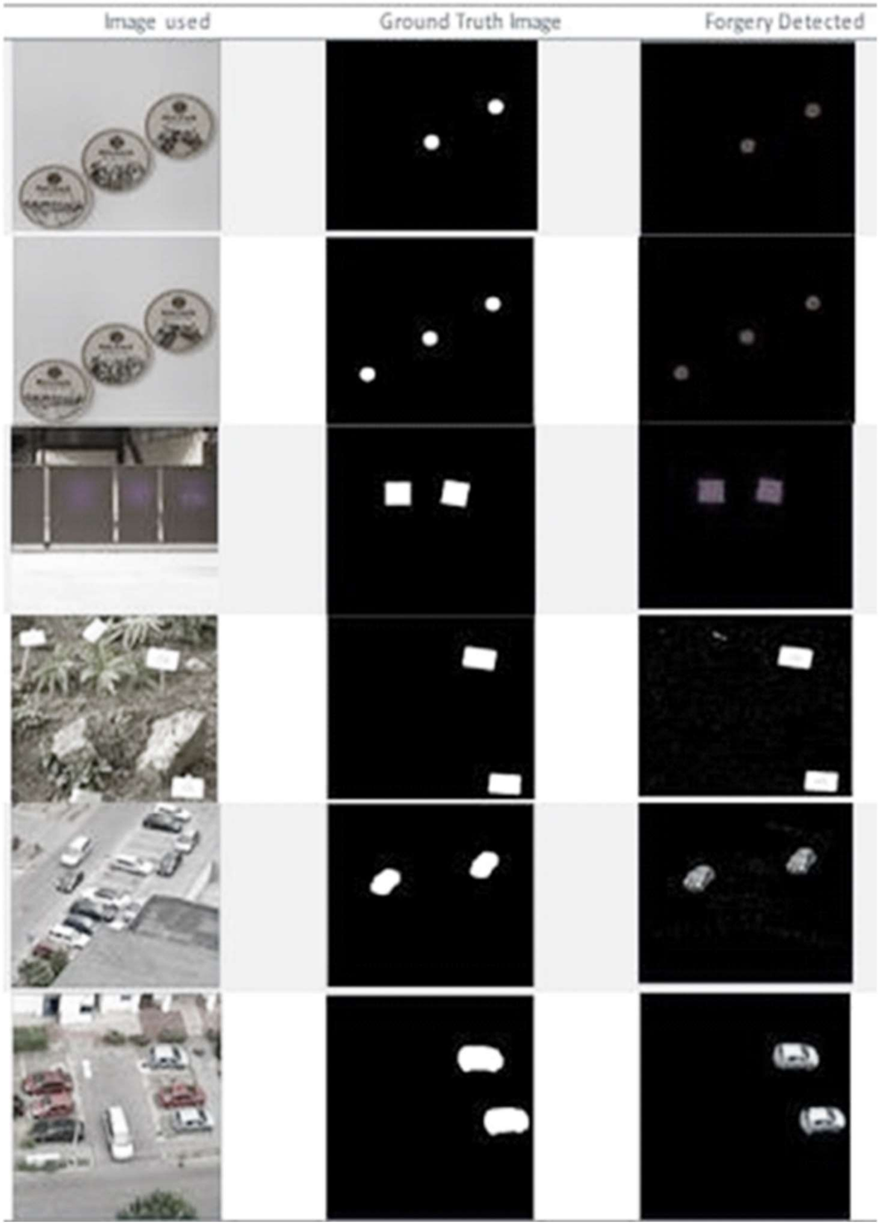

Figure 1.5: Image showing original forged images, binary ouput of forged region detected and forged pixels in original image

Parameters Image name	TP	TN	FP	FN	DA %	FPR
Image1	1996	258964	1184	0	100	0.4551
Image2	2994	258700	450	0	100	0.1736
Image3	7112	253300	1657	75	98.95	0.6499
Image4	7138	251933	2223	850	89.35	0.8746
Image5	6753	254836	538	17	99.74	0.2106
Image6	10383	251563	30	168	98.40773	0.011924

Table 1: Detection accuracy (DA) and False positive rate (FPR) parameters for the tested images

The presented ZLBP and mean-variance based methodology has been implemented in MATLAB. Our test data consists of a set of 512 × 512 color as well as grayscaleimages, taken from the CoMoFoD Database has been used for experimentation and performance evaluation which contains multi types of forged image. Only copy-move-rotated dataset from this database has been used in the experiments. For the sake of experimentation, we have selected test images with copy–move-rotated forgery induced into them. The DA and FPR results of the presented technique are presented in Table 7.1. After optimizing the false matches, the false positive rate is minimized, which is now in the range of 0-2%. All the results presented in Table I are presented for all five test images shown in the figure below.

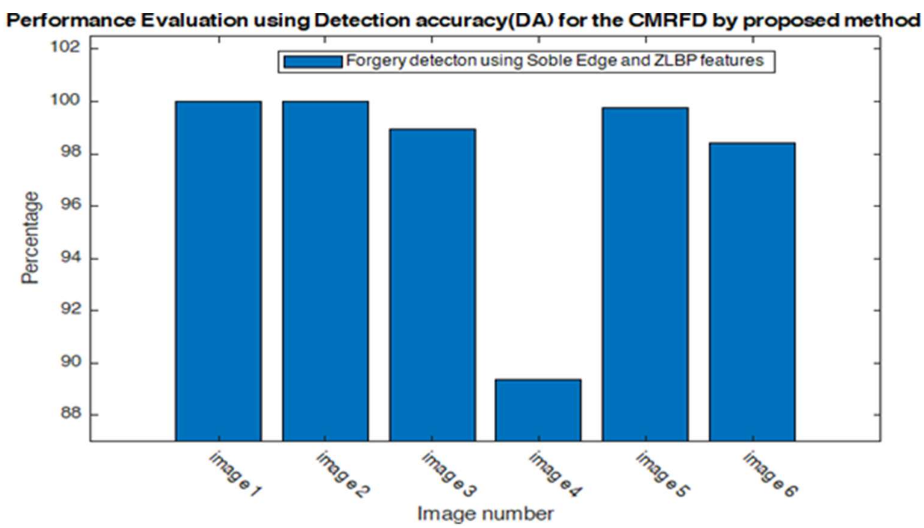

Figure 1.6: Bar graphs for False positive rate (FPR)

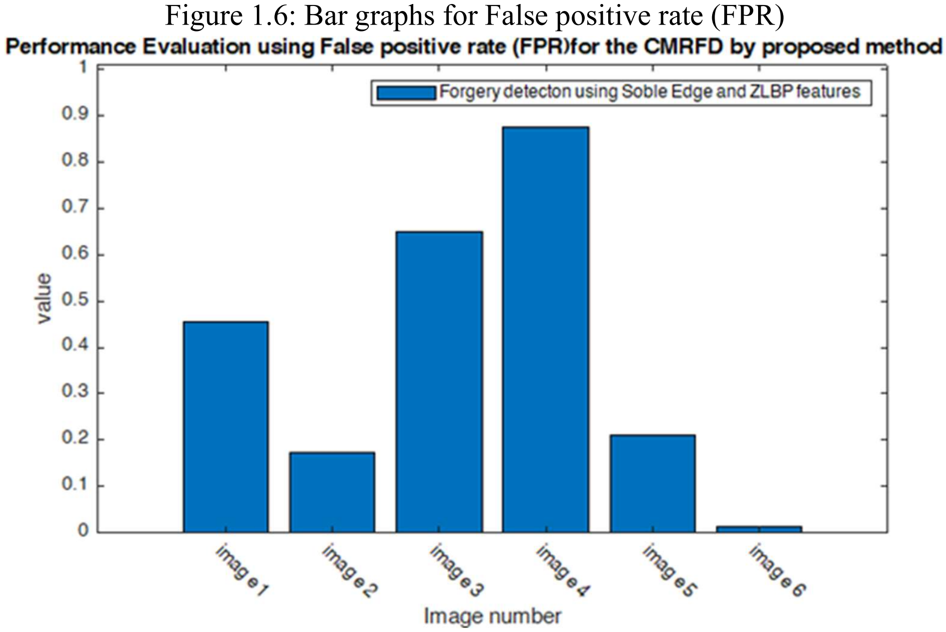

Figure 1.7`: Bar graphs for False positive rate (FPR)

We show the efficiency of the presented method provides accuracy mainly on the principles of operation of LBP with Zernike moment . The performance has been compared visually in terms of DA and FPR, in Figs. 1.5 and 1.6, respectively. From Figs. 1.7, it is evident that the presented algorithm achieves lower false positive rate and higher detection accuracy when copy-move-rotation forgery is induced in images.

6. CONCLUSION

Nowadays, digital images are used widely in numerous areas in our lifecycle for instance forensics sciences, news reports, online marketing, surveillance services and medical diagnosis. Furthermore, these could be used as evidence in courts, and in the media to transform the sense of images with the purpose of affecting the readers' points of observations. Therefore, the region of digital image forensics to state the originality of digital image has come to be a significant area of investigation to regain belief in digital image. The forensic examination for digital images services in providing information to support security, law enforcement, and intelligence agencies. Numerous methods are introduced to examine the digital image's content. The image forgery detection is explored to passive and active methods.

7. References

[1] Al-Qershi, O. M., Khoo, B. E., “Keypoint Based Authentication And Localization Of Copy-Move Forgery In Digital Image”, Multimedia Tools and Applications, Vol. 77, Issue 24, pp. 31807–31833, December 2018.

[2] Al-Qershi, O. M., Khoo, B. E., “Passive detection of copy-move forgery in digital images: State-of-the-art”, Forensic Science International, Vol. 231, Issues 1–3, pp. 284- 295, September 2013.

[3] Alkawaz, M. H., Sulong, G., Saba, T., and Rehman, A., “Detection of copy-move image forgery based on discrete cosine transform”, Neural Computing and Applications, Vol. 30, Issue 1, pp. 183–192, July 2018.

[4] Amerini, I., Ballan, L., Caldelli, R., Del B. A., and Serra, G., “A SIFT-based forensic method for copy-move attack detection and transformation recovery”, IEEE Trans Inf Forensics Secur, Vol. 6, Issue 3, pp. 1099–1110, 2011.

[5] Amerini, I., Ballan, L., Caldelli, R., Del, B. A., Del, T. L., and Serra, G., “Copy-move forgery detection and localization by means of robust clustering with J-linkage”, Signal Process Image Commun, Vol. 28, Issue 6, pp. 659–669, 2013.

[6] Amtullah, S., Koul, D. A., “Passive image forensic method to detect copy move forgery in digital images”, IOSR J ComputEng, Vol. 16, Issue 2, pp. 96–104, 2014.

[7] Ansari, M. D., Ghrera, S. P., and Tyagi, V., “Pixel- Based Image Forgery Detection: A Review”, Journal IETE Journal of Education, Vol. 55, Issue 1, 2014.

[8] Ardizzone, E., Bruno, A., Mazzola, G., “Copy-move forgery detection by matching triangles of Keypoints”, IEEE Trans Inf Forensics Secur, Vol. 10, Issue 10, pp. 2084– 2094, 2015.

[9] Ardizzone, E., Bruno, A., and Mazzola, G., “Copy-move forgery detection via texture description”, Proceedings of the 2010 ACM Workshop on Multimedia in Forensics, pp. 59-64, 2010.

[10] Asghar, K., Habib, Z. and Hussain, M., “Copy-move and splicing image forgery detection and localization techniques: a review”, Journal Australian Journal of Forensic Sciences, Vol. 49, Issue 3, pp. 281-307, 2017.

[11] Badal, S., Das, P., and Dalton, T., “Dual system for copy-move forgery detection using block-based lbp-hf and fwht features”, Engineering Letters, Vol. 26, pp. 171-180.

[12] Bi, X., Pun, C. M., “Fast copy-move forgery detection using local bidirectional coherency error refinement” Pattern Recognition, Vol. 81, pp. 161-175, 2018.

[13] Bi, X., Pun, C. M., Yuan, X. C., “Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection”, Information Sciences, Vol. 345, pp. 226–242, 2016.

[14] Bi, X., Pun, C. M., Yuan, X. C., “Multi-scale feature extraction and adaptive matching for copy-move forgery detection” Multimedia Tools and Applications, Vol. 77, Issue 1, pp. 363–385, January 2018.

[15] Bo, X., Junwen, W., Guangjie, L., and Yuewei, D., “Image Copy-Move Forgery Detection Based on SURF”, International Conference on Multimedia Information Networking and Security, pp. 889-892, 2010.

[16] Bravo-Solorio, S., Nandi, A. K., “Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics”, Signal Process, Vol. 91, Issue 8, pp. 1759–1770, 2011.

[17] Brownlee, J., “Metrics To Evaluate Machine Learning Algorithms in Python”, Machine Learning Mastery, 2015.

[18] Cao, Y., Gao, T., Fan, L., and Yang, Q., “A robust detection algorithm for region duplication in digital images”, International Journal of Digital Content Technology and its Applications, Vol. 5, Issue 6, pp. 95–103, 2011.

[19] Cattaneo, G., Roscigno, G., “A Possible Pitfall in the Experimental Analysis of Tampering Detection Algorithms”, 17th International Conference on Network-Based Information Systems, pp. 279-286, 2014.

[20] Chede, S. D., Lakhe, P. R., “Forgery of Copy Move Image Detection Technique by Integrating Block and Feature Based Method”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 1, January 2015.

[21] Chen, C. C. , Wang, H., and Lin, C. S., “An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection”, Multimedia Tools and Applications, Vol. 76, Issue 24, pp. 26503–26522, December 2017.

[22] Choudhary, S. P., Kumar, A., Maheshkar, S., Maheshkar, V., “An integrated method of copy-move and splicing for image forgery detection”, Multimedia Tools and Applications, Vol. 77, Issue 20, pp. 26939–26963, October 2018.

[23] Christlein, V., Riess, C., Jordan, J., Riess, C., and Angelopoulou, E., “An Evaluation of Popular Copy-Move Forgery Detection Approaches”, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, pp. 1841-1854, Dec. 2012.

[24] Cozzolino, D., Poggi, G, and Verdoliva, L., “Copy-move forgery detection based on patch match”, The International Conference on Image Processing (ICIP), pp. 5247– 5251, 2014.

[25] Cozzolino, D., Poggi, G., and Verdoliva, L., “Efficient dense-field copy – move forgery detection” IEEE Transactions on Information Forensics and Security, Vol. 10, Issue 11, pp. 2284–2297, 2015.

Author Details

Dr.Gurpreet Kaur is working as a Assistant Professor in Asian Group of Colleges Patiala ,Punjab,India since 2014.She is Doctorate in Computer Science from Desh Bhagat University , Punjab.She has 14 years of experience in the field of computer science and Information Technology.She has published more than 8 papers in peered review journals,RIP and UGC care Journals...She has been awarded Gold medal in post graduation from Guru Nanak Dev University,Amritsar.