International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 02, February-2015

A Bayesian Classifier Approach for GLCM Based Image Forgery Detection

S. Dhevana
M.E Student :Dept of E.C.E
A.V.C College of Engineering
Tamilnadu, India.

C. Jayasri
Assitant professor: Dept of E.C.E
A.V.C College of Engineering
Tamilnadu, India.

***Abstract*-Generally the image manipulation techniques employed on the digital images causes the tampering on the image ,in which the noise will also get added to the image. Hence to get the authenticity of an image, we go for the image forgery detection methodologies. In which image forgery detection methods based on the PRNU(photo response non uniformity) has the major disadvantage that forgery cannot be detected in the absence of camera PRNU.In this paper we are going to detect the forgeries in the image with the help of the GLCM(gray level co-occurrence matrix) .The neural network training has to be done before the application of the GLCM features to predict whether the given input image is forged or not.Later,the processing on the image has to be done with the help of the Bayesian classifier to detect the forged part of the image.**

Keywords-GLCM(Gray Level Co-occurrence Matrix), PRNU(Photo Response Non Uniformity),Bayesian classifier, Neural Network.

I. INTRODUCTION

The image processing techniques done on the images are wide in varieties which will cause the different effect on the images likewise some of the techniques such as copy-move (or) splicing, signature, watermarking or any other object which get added to the original by various means. The image forgery means the manipulation of the digital images to conceal some meaningful or useful information, this may be done for also illegal message transaction .hence it is important to find the effective tool for the detection of the image forgery ,among that ,Bayesian classifier is one such tool for the prediction of the forgery in the digital image here the processing is done on the whole image instead of individual pixels. This process can be classified into three major classification blocks. The initial step is the preprocessing which is done by the neural network training. The second one is application of the glcm features .Finally the classification of the forged object is done by the Bayesian classifier.

In the previous works the classification is done with the Bayesian MRF approach for PRNU based image forgery detection. As such type of the process needs an another factor of finding camera PRNU,which is varying for different cameras. This forgery detection method can be done in different forms according to the type of the forgery present in an image.The forgery detection which occurred in an image can be detected in three levels. Which are, format analysis of the image, error level analysis present in the image and the inconsistency in the image quality. The process involving neural network training will train the input image according to our needs. Here the training is done for the image format. The given input image is trained with the standard format of the image. This training process will take the least amount of time compared to the other methodologies.

The entire process in this paper can be defined with the help of the flow chart given below. In this the input image is preprocessed with the help of the neural network training tool. This preprocessed image is further converted into GLCM.Then we will get the normalized matrix of this image. From this normalized matrix we can compute the certain features of the image. Then the Bayesian classification has to be done this will classify the forged object from the original image, which is based on the method of maximum likelihood.

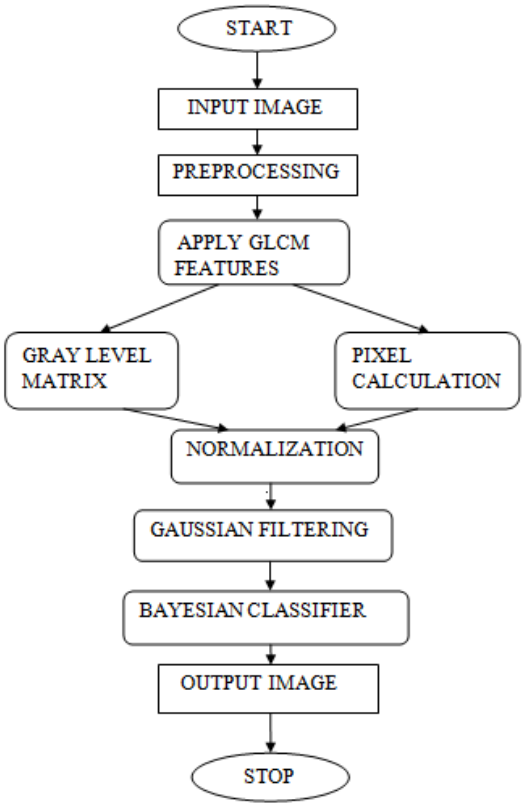

Fig 1. Flowchart

II. PREPROCESSING

For each and every process preprocessing is the necessary one, here the preprocessing is done with the help of the artificial neural network. The definition for the artificial neural network given by one of the inventor of neural computer is given by,"A computing system made up of the simple externally inters related processing elements, which practice information by their dynamic state response to their peripheral inputs". The artificial neural network consists of the three layers which are input layer, hidden layer, output layer. In this each layer consists of the interconnected nodes, in this each node will perform certain activation function. The input image patterns are available to the network by means of the input layer. This input layer communicates with the more number of hidden layers present in the network where the actual processing is done ,then these hidden layers unite to form the output layer ,this output layer gives the output of the preprocessing system

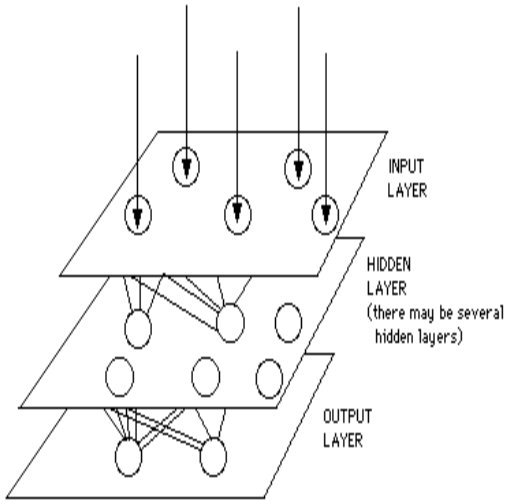

Fig 2. Neural network model

The neural network model will be as shown in the fig.

The pictorial representation of this tool will be as shown below

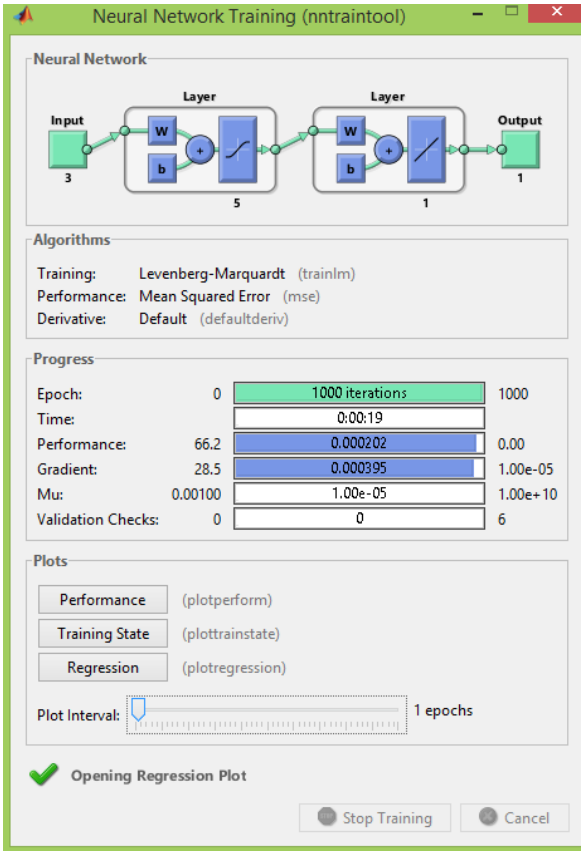

Fig 3. Neural Network Training Tool

After the completion of this training a graph will be automatically generated in it reveals that how far the training is done over the target.

III. GLCM(Gray Level Co occurrence Matrix)

This is generally defined as the matrix, the features which are calculated by using GLCM are mean square error, peak signal to noise ratio, entrophy, structural content ,overall entrophy.GLCM matrix can be calculated with certain steps which are as follows;

i. Create the framework matrix
ii. Compute the spatial relationship between the adjacent pixel,
iii. Count the occurrences and fill the framework matrix.
iv. Add the matrix to its transpose to make it symmetrical.
v. Normalize the matrix.

From this normalized matrix, thus obtained we can calculate the certain characteristics features of an image this features will determine the quality of the image.

After getting the normalized matrix the filtering has to be done with the help of the Gaussian function to reduce or to eliminate the undesired high frequency components.

IV. BAYESIAN CLASSIFICATION

This Bayesian classifier is the simple probabilistic approach based on applying the bayes theorem. It has the advantage over the Bayesian MRF by recognizing the false rate in high value.

This bayes classifier assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature. This classification is done on gray scale image obtained.

The major advantage of the Bayesian classifier over the other methods are, it requires only the small amount of training data to estimate the parameters necessary for classification. This approach can be trained efficiently in the supervised learning setting.

V. EXPERIMENTAL RESULTS

The software used here is the MATLAB with GUI tool. After running the code in this tool the figure 4 shows the snapshot of the main GUI .the first push button is for loading the input image. The message box will appear to select the input image from the database. After loading the image will be loaded as shown in the figure 5 which has to be trained with the help of the neural network training as shown in the figure 3.in this training it reveals that how far the pixels of the input image matches with the standard format of that image.

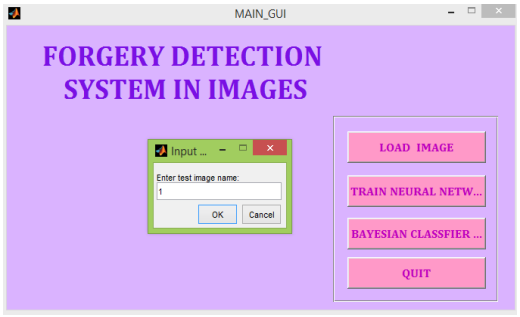

Fig 4. The Main GUI Image

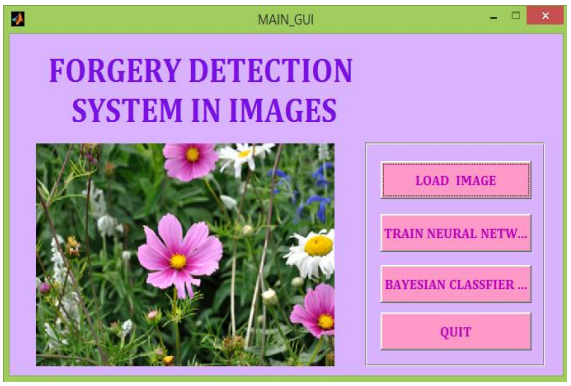

Fig 5. The Input Image

Up to this stage we detected that the given image is forged one or not. The next stage is to define the forged part of the image this can be implemented with the help of the Bayesian classifier based on the GLCM. While click on the classifier button the image is converted into the grayscale, which will be as shown in the figure 6.then the forged part of the image will be obtained with the various zooming parameters. These zooming parameters can be made according to our needs. This parameter will be as shown in the figure 7 and figure 8.

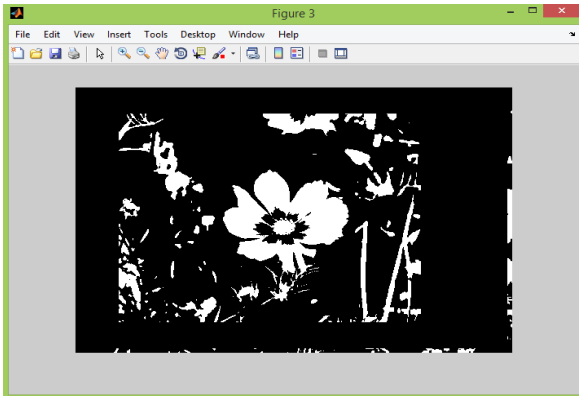

Fig 6. The Gray Scale Image

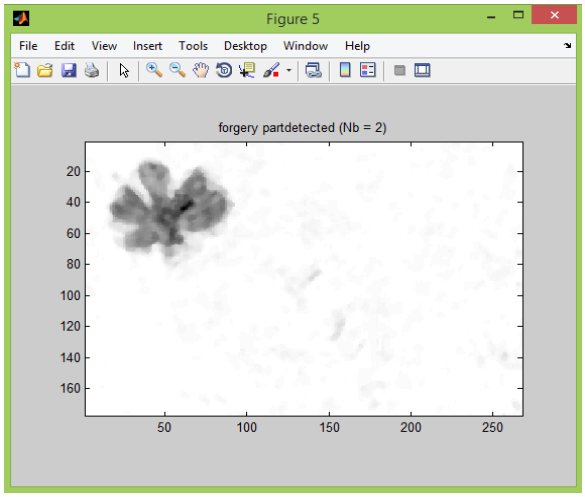

Fig 7. The Detected Forged Part

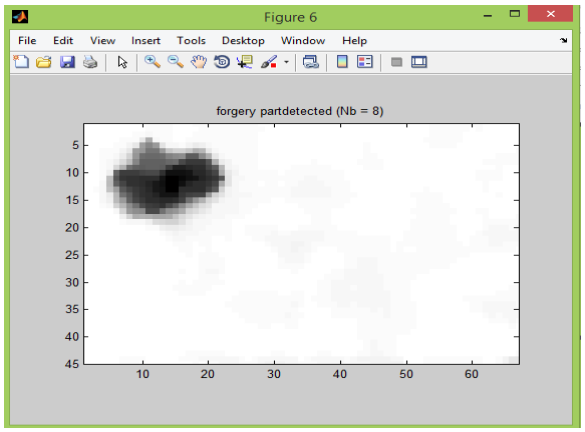

Fig 8. The Forged Part (Zoomed)

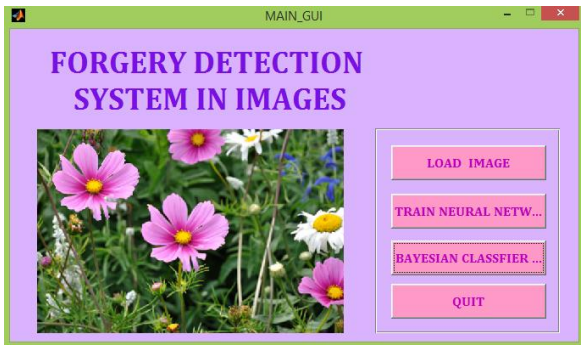

Fig 9. The Original Image

Finally we will get the original image which does not contain any forgery. Simultaneously in the command window we can get the various characteristics which will be as shown in the figure10.

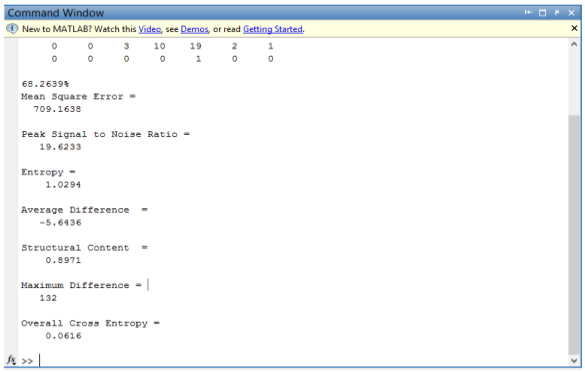

Fig 10. Performance Evaluation

VI. CONCLUSION

In this paper the forgery which occurs in an image has been detected with the help of the GLCM.The GLCM which has to be processed on the image, those images are already trained with the help of the neural network. Here the Bayesian classification is implemented along with the GLCM to find the forged part of an image. In addition to that, certain characteristics features are evaluated in this GLCM based forgery detection.

REFERENCES

1. *Photo Tampering Throughout History* [Online]. Available: http://www.fourandsix.com/photo-tampering-history.
2. G. Zhou and D. Lv, "An overview of digital watermarking in image forensics," in *Proc. Int. Joint Conf. CSO*, Apr. 2011, pp. 332–335.
3. S. Battiato, G. M. Farinella, G. M. Messina, and G. Puglisi, "Robust image alignment for tampering detection," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1105–1117, Aug. 2012.
4. Y. Zhao, S. Wang, X. Zhang, and H. Yao, "Robust hashing for image authentication using Zernike moments and local features," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 55–63, Jan. 2013.
5. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy and move attack detection and Transformation recovery," *IEEE Trans. Inf. Forensics Security*, vol. 6,no. 3, pp. 1099–1110, Mar. 2011.
6. P. Kakar and N. Sudha, "Exposing postprocessed copy-paste forgeries through transform-invariant features," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1018–1028, Jun. 2012..
7. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.
8. M. K. Johnson and H. Farid, "Metric measurements on a plane from a single image," Dept. Comput. Sci., Dartmouth College,Tech. Rep. TR2006-579, 2006.
9. M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3,pp. 450–461, Sep. 2007.
10. Q. Liu, X. Cao, C. Deng, and X. Guo, "Identifying image composites through shadow Matte consistency," *IEEE Trans. Inf. Forensics Security*,vol. 6, no. 3, pp. 1111–1122, Sep. 2011.
11. Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognit.*, vol. 42, no. 11, pp. 2492–2501, 2009.
12. Y.-L. Chen and C.-T. Hsu, "Detecting recompression of JPEG imagesvia periodicity analysis of compression artifacts for tampering detection,"*IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 396–406,Jun. 2011.

13. T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Security*, vol. 7,no. 3, pp. 1003–1017, Jun. 2012.
14. F. Zach, C. Riess, and E. Angelopoulou, "Automated image forgery detection through classification of JPEG ghosts," *Pattern Recognit.*, vol. 7476, pp. 185–194, Jan. 2012.
15. I. Yerushalmy and H. Hel-Or, "Digital image forgery detection based on lens and sensor aberration," *Int. J. Comput. Vis.*, vol. 92, no. 1, pp. 71–91, Nov. 2011.
16. H. Fu and X. Cao, "Forgery authentication in extreme wide-angle lens using distortion cue and fake saliency map," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1301–1314, Aug. 2012.