Image Forensic Analysis And Recognition In Copy-Move Using Bag Of Features And Svm

R.Bharat Kumar[1] Ch.V.V.S.Srinivas[2] Abdul Rahaman Shaik[3]

[1]Assistant professor, [2]Associate professor , [3]Associate professor
[1,2,3]*ECE Department, Vishnu Institute of Technology, Bhimavaram, India*

Abstract

Digital image forgery is a developing issue as the picture could be effectively controlled. Various image processing tools can be forged from digital image forgery. Forging process consists of recompression technique which will erase the traces of existed un-compressed images. The recompressed images are obtained in this proposed system by the process of detection of traces. So the proposed forgery image detection approach will produce periodicity analysis with the double compression effect in spatial domain. Experimental results exhibit that the proposed procedure is performed well on the discovery of fraud limitation.

Keywords — *Digital image forensics; passive forgery detection, discrete cosine transform (DCT), Speeded up Robust Features (SURF), spatial and colour rich model (SCRM)* .

I.INTRODUCTION

With the development of society, digital image plays important part in daily life. Digital image serves as medium of communication and involves a great deal of significant information. For instance, a credible digital photo may be taken as evidence at court; everyday newspaper and magazines have a close connection with digital images; of course, it depends on digital images that doctors diagnose the patients. However, sophisticated digital cameras and photo-editing software packages are becoming ubiquitous. The reality and integrity of digital images are suffering badly threats. In consequence, it is vital and urgent to discover the skill to distinguish the truth from the false images. Naturally, digital image forensics technology is a newEASE OF USE

implanted into computerized pictures ahead of time or not. Active evidence is mainly about watermark, but it has many disadvantages: What is embedded with watermark makes the quality of the picture a decline. At present, many of the digital cameras have not been imbedded the function of watermark. Watermark is easy to attack and destroy. When we obtain the evidence, we need a third institute to be involved in, of course, the third institute needs accepting by the recognition of the two sides and the court. Therefore, the passive-blind evidence that detects the changed regions only by depending on the content itself will become a research topic of digital image forensics technology. Some rely on detecting the traces resulted from image forgery operations such as re-sampling, colour filter array interpolation, camera sensor noise pattern, and double JPEG compression.

We first present the whole framework for forgery localization, and then introduce two improved forensic approaches used in the framework, respectively. Finally, we propose the fusion method for integrating the detection results of both approaches. The proposed forgery localization framework is *illustrated. This framework consists of the following two steps.*

Step #1: Producing the possibility map for each forensic approach. In this step, we use two different forensic approaches, i.e., a statistical feature based approach and a copy- move detection based approach, to analyze the given image. The main reason for choosing the former approach is that some advanced steganalysis features can detect various image operations based on our previous work, and we expect that such features can achieve good performance in detecting image splicing/erasing operations, which are commonly used in image tampering.

However, the statistical feature based approaches cannot perform well in detecting another popular used operation, copy-move. Thus, the copy-move detector is included as a complement. Please note that the methods based on sensor pattern noise and near duplicate analysis are not considered in the proposed framework due to their limitations. In this work, we carefully improve the two selected approaches. What is more, unlike the existing methods, we produce a tampering possibility map for each approach, which is very helpful for the subsequent fusion step.

Step #2: Fusing the possibility maps to locate the tampering regions. In this step, we try to obtain the *final localization result via combining the possibility maps* obtained in the first step. Recently, some fusion methods have been proposed for forgery localization. Unlike the exiting methods, in the proposed framework, we carefully analyse the distributions of the values within the tampering possibility maps for pristine and fake pixels, and design a decision curve to differentiate between pristine and fake pixels.

Furthermore, some copy-move or copy-paste detecting methods have been developed. Another common form of digital image forgery is called splicing forgery. It is a copy-and- paste operation of image regions from one image onto another. Inspired by the works mentioned above, we propose an integrated technique for forgery image detection which combines discrete cosine transform (DCT) coefficients analysis by double JPEG compression and Speeded up Robust Features (SURF). This paper focuses on JPEG format and aims to detect two forgery images based on copy-move and splicing forgery. In the proposed technique, the main contribution is to locate the copy- move regions and find out non- original regions. Experimental results demonstrate the proposed technique has good performance to identify image authenticity.

II. LITERATURE SURVEY

ith the help of powerful image editing software, we can easily modify digital images without leaving any perceptible artifacts. Maliciously tampered images would lead to some potentially serious consequences in our daily life. Therefore, image forensics has attracted considerable attention during the past decade. For most measurable techniques, it is accepted that some characteristic picture measurements presented by the age pipeline will be unavoidably mutilated after some altering activities, and scientists examine such insights in order to recognize the phonies. For the most part, there are two principle issues in picture legal sciences, one is forgery recognition, and the other one is forgery localization.

Forgery detection aims to discriminate whether a given image is pristine or fake. For instance, by exploiting some camera-related signals such as sensor pattern noise (SPN) and colour filter array (CFA) properties, it is possible to reveal tampered images via camera source identification. By analysing the JPEG compression artefacts, one can expose JPEG decompressed images and detect JPEG recompressed images. Based on the distinctive artifacts left by a certain operation, it can identify contrast enhancement reveal image resampling detect median filtering and so on. In practice, a key influential factor for forgery detection performance is the variety and uncertainty of tampering operations. Since most existing forensic methods assume that only one specific tampering operation is under investigation, they should not be used for a real forensic scenario independently. Usually, it requires to analyzing the image with several forensic detectors and combining the detection results using some fusion schemes.

Some recent works applied fuzzy theory and Dempster- Shafer theory to fuse the detection results, but these methods only considered JPEG compression artifacts, and might not be suitable for more general cases. An alternative solution is to seek for universal features that can identify as many tampering operations as possible. In our previous work, we adopted some universal features in steganalysis to detect various image operations and identify their types. In a set of mixed moment features was proposed for the same topic. In order to evaluate the forensic performance in a practical situation, in 2013 IEEE

Information Forensics and Security Technical Committee (IFS-TC) established the First IFS-TC Image Forensics Challenge, whose first phase was forgery detection. In the challenge, advanced statistical features such as spatial rich model (SRM) were adopted by the winners. By simply merging the detection results of a statistical feature based detector and a copy move detector, Cozzolino et al. obtained the best score, 0.9421, in the first phase of the challenge, meaning that the forensics community has achieved good performance for *forgery detection.*

III. RELATED WORK

In practical forensic applications, we are more interested in figuring out the tampered regions compared to forgery detection. Therefore, forgery localization becomes an important issue in image forensics. Since forgery localization requires pixel-level analysis rather than image-level analysis, it faces more challenges compared to forgery detection. Recently, some forgery localization works have been proposed based on JPEG features inconsistency of photo response non-uniformity (PRNU) local descriptors and so on. Besides, some techniques for augmenting the localization performance have also been studied.

However, since these works covered different topics in forgery localization, they were evaluated on different databases under diverse experimental settings, and their performance for practical applications has not been fully investigated. So far, a complicated and more practical scenario for testing the performance of forgery localization methods was set up in the second phase of the IFS-TC Image Forensics Challenge. The winner generated the localization

maps based on the fusion of results from three forensic approaches and obtained the F1-score of 0.4072. After carefully adjusting the forensic approaches and the fusion scheme used, Gaborini et al. proposed a new method and achieved the best F1-score of 0.4533 at present. Although the improvement is significant, such a result is still far from satisfactory for practical forensic scenarios.

In this paper, we propose an improved framework to deal with the problem of image forgery localization. The proposed framework first analyses the input image using a statistical feature based detector and a copy-move forgery detector, respectively. The results of the two approaches are then converted into tampering possibility maps. By analysing the properties of tampering possibility maps, we employ a simple yet very effective strategy to obtain the localization result.

Compared with the existing methods the main contribution of this paper is to propose a fusion scheme based on tampering possibility maps. The main efforts in our work are as follows. Firstly, after analysing the most popular tampering operations (splicing/erasing and copy-move) in real cases, we choose two forensic approaches and improve them for forgery localization. Although fewer forensic approaches are utilized compared to existing methods, we still significantly boost the overall performance. Secondly, unlike the existing methods that use binary maps, we convert the results of the adopted approaches into maps with continuous values ranging from 0 to 1, which indicate the tampering possibilities of the corresponding pixels. In this way, we can preserve more useful intermediate information of each approach and predict whether a pixel is pristine or fake more reliably. Compared to the binary maps, the tampering possibility maps are able to reduce the false positives and false negatives significantly based on our experiments. Finally and more importantly, the fusion method for integrating tampering possibility maps is newly designed.

IV.EXISTED SYSTEM

Splicing and erasing some objects within an image are the most popular tampering operations in practice. Furthermore, some pre-operations such as scaling and rotation, and some post-operations such as boundary blurring, contrast/colour adjustment, are applied to make the tampered regions more consistent with the whole image. All the operations involved in splicing and erasing would inevitably distort some inherent relationships among the adjacent pixels within a pristine image. Based on our analysis in previous work, some steganalytic features can effectively identify such manipulations. Thus, we try to use such features to locate tampered regions.

Many effective features are available in steganalysis. However, not all of them are suitable for forgery localization. In the previous work, a subset of SRM was used. Since SRM is designed for gray scale images, it is expected that the colour information within an image is not fully exploited. Thus, we decided to use the feature set named spatial and colour rich model (SCRM) in the proposed framework. SCRM is designed with an analogous mechanism as SRM. For a colour image, it respectively extracts SRM features from the R, G, and B channel and adds them together, and then concatenates them with another subset of features that consists of co -occurrence matrices computed on image residuals of the three colour channels.

In addition to feature extraction, another important factor that affects the localization performance is the design of training data. In our method, we implement the feature based approach with a sliding-window strategy. In the training stage, we first analyse the images using 64×64- pixel block with a step of 16-pixel to collect the training samples. The choices of block size and step size are based on the considerations of localization performance and computational cost. Based on our experiments, the detection errors for image block size 128×128, 64×64, and 32×32 are 12%, 15%, and 21%, respectively.

Considering the trade-off between detection accuracy and localization resolution, we set the block size as 64×64. A smaller step size would improve the localization resolution while results in longer processing time. We let the step size be 16 to get a better trade-off between localization resolution and processing time, ensuring that most pixels within an image will be analysed with 16 different 64×64 blocks. For each image, we regard the blocks tampered with 10% to 90% as fake, and extract the features from them as negative samples. After processing all the fake blocks, we randomly choose the same number of pristine blocks, i.e., those without any tampered pixels, and extract the features as positive samples. Based on the negative and positive samples at hand, we train an ensemble classifier with linear discriminant analysis (LDA) base learners for identifying whether an image block is pristine or fake. Please note that the dimensionality of our adopted feature is large (i.e., 18157-D) and the number of blocks is also considerable (a 1024×768 image has more than 2,700 blocks), it will take a very long time for training and testing if other more sophisticated classifiers are used, such as support vector machine (SVM). So we use the ensemble classifiers in this paper, which work much faster than SVM and provide comparable results

V. PROPOSED SYSTEM

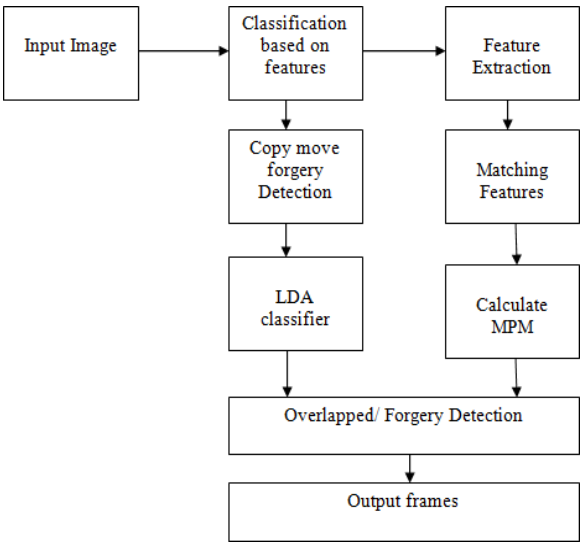

Fig. 1: Proposed system

The above block diagram (1) shows the architecture of proposed system. The first block represents the selection of forged image of interest which will be selected from the user defined folder. Later based on the features, the image is classified by extracting the features, LDA training, LDA based classification. In this, the copy move forgery is considered for detection which includes features extraction, matching of extracted features, and calculation of Mpm. Finally, the performance is evaluated by plotting the obtained ground truth values and parameter values like TP, TN, FP, FN, St, Sp, F1s and Pn are measured. The design implementation is described in this section which includes following algorithms.

A. IMAGE SELECTION

This case of implementation gives the input image selection from the desired folder of user (UF). The user selects the name of the file (nF) and path of the file (pF). These nF and pF will directs to image path (Ipath). The input image (Ini) is chosen from the Ipath and is resized to get the original input image (Inimg).

B. FEATURE BASEDCLASSIFICATION

This contains three different stages like extraction of statistical features (EsF), training through Linear Discriminated analysis (LDA) (TLDA), classification based on LDA (CLDA). These stages are illustrates as below.

C. EXTRACTION OF STATISTICAL FEATURES

Before extracting the statistical features, the ground truth (GT) is considered. For GT, the image size (nr – rows and nc - columns) is taken into consideration, if the size is of 3 i.e.; RGB then converts it to Gray scale i.e., rgb2gray. Then obtained image is resized to get the GT image (GTimg).

For extraction, both the Inimg and GTimg are considered and then RGB color spaces (Cs) are obtained. The image is divided as block size of 3, from this center pixel (Cp) is obtained. The color image converted to Hue, Saturation, and Value (HSV) form. Then the empty features are initialized to get the statistical features (Sf). Later, calculated the features for every bocks and store in labels. Then obtained the vector for each color (Rv, Gv, Bv) and concatenate outcome to get vector (Cv). Finally, calculate the statistical features (Sf) by using Cv.

D. LINEAR DISCRIMINATED ANALYSIS (LDA) TRAINING

In this step of implementation for LDA training, the vectors formed during the Sf extraction i.e. F(:, ii)=(Sf)' (ii)=GTb. These F and L are initialized and its complements are represented with X and Y respectively. Finally, the LDA training is by using X and Y.

E. FEATURE EXTRACTION

This part comes under the forgery detection where to extract the features following algorithm is implemented. The image size is considered. If image size is 3 i.e., colors (RGB) then convert it to gray scale. Then find the matrix form of image size and extract the scale invariant feature transform (SIFT) features. In this case of implementation original image and forged image sift features are stored in S1 and S2 respectively. In this case distance ratio is set to 0.6. Later matching is performed if matching found then collects matching features (Mf) at S3. At last from this it can be observed that compared to existed system, the proposed system gives effective results.

RESULTS

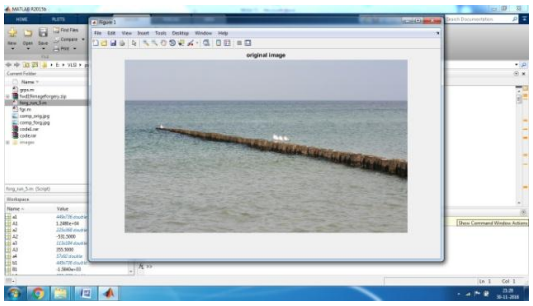

Fig.2: ORIGINAL IMAGE

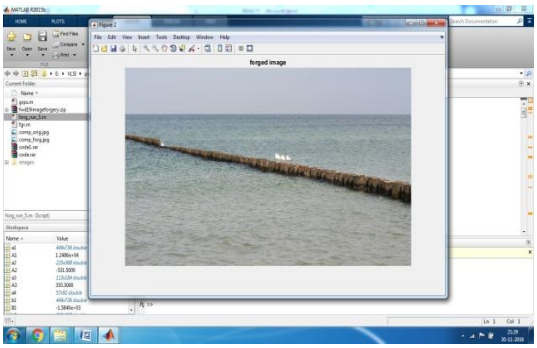

Fig.3: FORGED IMAGE

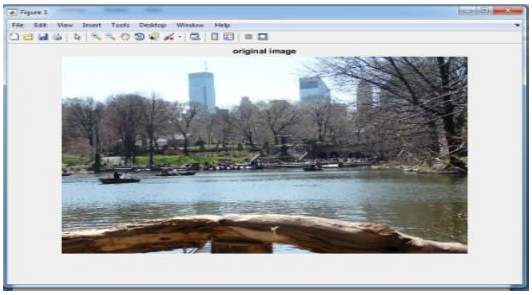

Fig.4: ORIGINAL IMAGE

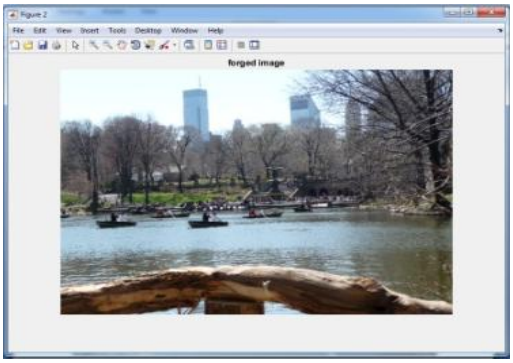

Fig.5: FORGED IMAGE

REFERENCES

[1] Experimental results show that the proposed scheme can achieve much better detection results.

[2] M. M. Yeung, "Digital watermarking," Commun. ACM, vol. 41, p.30, 1998.

[3] J. Fridrich, "Methods for tamper detection in digital images," in Proceedings of Multimedia and Security Workshop at ACM Multimedia '99, pp. 19-23, 1999.

[4] Shinfeng D. Lin and Yu-Hsun Huang, "An Integrated Watermarking Technique With Tamper Detection and Recovery," International Journal of Innovative Computing, Information and Control, Vol. 5, Num. 11, Nov. 2009, SCI.

[5] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 758- 767, 2005.

[6] A.C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Transactions on Signal Processing, 2005.

[7] J. Lukas, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in Proceedings of the SPIE, vol. 6072, pp. 60720Y, 2006.

[8] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004- 515, Dartmouth College, Computer Science, 2004.

[9] H. L. Huang, W. Q. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, pp. 272-276, 2008.

[10] I. Amerini, L. Ballan, R. Caldelli, A.

[11] D. Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 1702- 1705, 2010.

[12] X. Pan and S. Lyu, "Detecting image region duplication using SIFT features," IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp.857-867, 2010.

[13] E. Ardizzone, A. Bruno and G. Mazzola, "Detecting Multiple Copies in Tampered Image," in Proceedings of IEEE 17th International Conference on Image Processing, pp. 2117-2120, 2010.

[14] Z. C. Lin, J. F. He, X. Tang, and

[15] C. K. Tang; "Fast, Automatic and FineGrained Tampered JPEG Image Detection via DCT Coefficient Analysis," Pattern Recognition, Vol. 42, Issue 11, pp. 2492-2501, Nov. 2009.

[16] H. Bay, A. Ess, T. Tuytelaars, and

[17] L. Van Gool, "SURF: Speeded-up robust features," International Journal on Computer Vision and Image Understanding, vol. 110, no. 3, pp. 346-359, 2008.

Author Details

R.Bharat Kumar was born in A.P, India, and Completed M.Tech in VLSI System Design from Swarnandra college of Engineering and Technology, Narsapuram in the year of 2013 and B.Tech from EVM College of Engineering Narsaraoper in the year 2011 in Electronics &Communication engineering. Presently working as an Assistant Professor in Vishnu Institute of Technology, Bhimavaram, A.P, India. His research interests in VLSI Design and low power techniques.

CH V V S Srinivas was born in A.P, India, Completed M.Tech in Communication Systems Engineering from S R K R Engineering College, Bhimavaram in the year of 2010 and B.E from S R K R Engineering College in the year 2006 in Electronics &Communication engineering. He worked as an Assistant professor in TRRCE and presently working as an Asst.Professor in Vishnu Institute of Technology, Bhimavaram ,A.P, India. His research interests in VLSI Design and communication systems.

Abdul Rahaman Shaik was born in A.P, India, and Completed M.Tech in VLSI System Design from NIIT Warangal in the year of 2010 and B.E from Sir C R Reddy Engineering College in the year 2000 in Electronics &Communication engineering. He worked as an Assistant professor in Sir C R Reddy Engineering College and presently working as an Assoc. Professor in Vishnu Institute of Technology, Bhimavaram, A.P, India. His research interests are in VLSI Design and Communication systems.