International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.4 (2016), pp. 37-48
http://dx.doi.org/10.14257/ijmue.2016.11.4.05

Forgery Detection Using Noise Estimation and HOG Feature Extraction

Mandeep Kaur[1] and Savita Walia[2]

[1]*Information Technology, University Institute of Engineering and Technology*
Panjab University, Chandigarh
[2]*Information Technology, University Institute of Engineering and Technology*
Panjab University, Chandigarh
[1]*mandeep@pu.ac.in,* [2]*savita_walia@rediffmail.com*

Abstract

Forgery detection techniques are required to verify the authenticity of the digital images. The additional noise is the most general way to hide the traces of the tampering done to the image. Original images which do not undergo any alterations are supposed to have a consistency in noise variation. If the image is forged, the noise no longer remains consistent throughout the image. In this paper, a method is proposed to detect the forgery based upon noise estimation and hog feature extraction. The image is first converted to YIQ colorspace, and then the block segmentation is performed on Y component of the YIQ image. Noise is estimated using PCA and hog features are extracted from each block of the image. An unsupervised clustering method is used to cluster the blocks of the image. The experimental results show that the proposed technique detects forged images more effectively as compared to previous method based only on noise estimation.

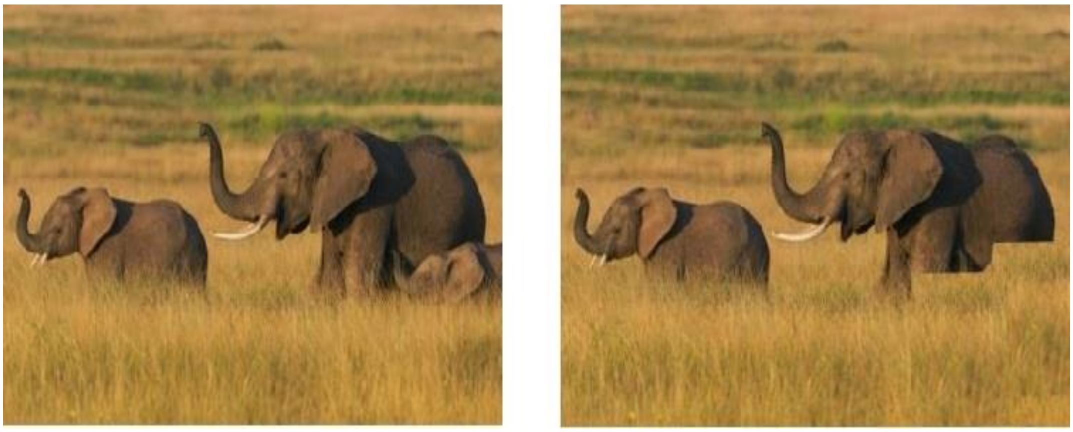
Keywords*: Image forgery detection, noise estimation, authenticity, hog, ntsc, image forensics, blind verification*

1. Introduction

In this era of technology, digital images have become the most widely used communication media. It's not that the images are used as a purpose of communication media but they are also being used in various fields like military services, law, scientific purposes, industrial use, educational use, forensics *etc.* The originality and integrity of these images are very sensitive parameters while dealing with images. Image forensics deal with the issues concerned with forgeries done to the images. The digital image forensic science aims to inspect the digital media with an intention of identifying, conserve, convalesce, analyzing and presenting facts and figures about the information obtained from the digital images. Due to the advancement in the computer technology, various methods of creating forgery or altering the images have been developed by forgery creators so as to use the images for their personal benefits. The digital forensics needs forgery detection techniques in order to maintain the integrity of the images and to check their authenticity.

There exist various ways in which images can be altered. Some of the most common types of forgeries are copy-move, splicing, altering the brightness/contrast of the images, geometrical transformations *etc.* An example of forgery is shown in Figure 1 which is taken from CASIA Database.

The forgers hide from view the marks of the forgery done to the image. To detect and locate those marks is the aim of the forgery detection methods. The forgery detection methods [1] which have been developed in the past are categorized into two main categories: Active methods and Passive/Blind methods. Active methods [2-3] need prior information about the image. They require embedding of the digital signature/digital watermarks on the authentic image. For detection using active methods the digital watermark/digital signature should be known before in order to compare it with that of the image under consideration.



Original Image Forged Image

Figure 1. Example Showing Forgery in Image (Taken from CASIA Database)

There are images which are not pre-processed with digital watermarks/digital signatures; in that case the active methods cannot be used. So there arises a need for some blind methods which should be capable of detecting forgery without prior information regarding the image. Various blind methods [4-6] exist to fulfill this purpose. Resampling technique is used to detect geometrical transformations, boundary based methods are used for detection of splicing done to the images. There are various forgeries and their corresponding methods to detect those forgeries. But a false proof method needs to be developed which should be capable of detecting forgery based on the intrinsic properties of the image.

The forgers use noise as a healing component to hide out the traces of the forgeries. The image noise is defined as the random deviation of the brightness/contrast and the color information. The image noise is basically produced by the camera sensor while the image is being photographed. It is an unwanted by-product of the image capture that adds forged information in the image. Every image is supposed to have a noise as a by-product of the capturing process. But, the original image has a consistent noise variation all over the image. So the inconsistency in the noise can be used to detect the forgery in the images.

In this paper, we have proposed a method to detect forgery based on noise variance estimation and hog (histogram oriented gradients) on Y component (luminance) of the YIQ colorspace (NTSC image). Hog features are used for detection of copy-move regions or spliced images. The whole paper is organized as follows: Section 2 provides a brief discussion on the previous literature related. The proposed methodology is explained in Section 3. The experimental results are discussed in Section 4. The conclusion is provided in Section 5.

2. Previous Work

Noise detection has been used in previous methods for image source identification and detection of forgery. One of the unique distinguishing attribute of the imaging sensors is the photo response non-uniformity (PRNU). It was utilized as an inherent feature to identify the camera source of the image taken [8]. In [9], authors proposed a method in which the demosaicing features were combined with the PRNU features of the image and then classified using a double-learning process to identify the source camera model. H.

Gou. *et al*. proposed a method in which three sets of attributes were used for detection of forgery. Denoising algorithms were used to estimate the image noise variance. Prediction error of neighborhood was used as another set of features, and the third set of features were obtained from wavelet analysis. These three features were used in combination and classified using a classifier which was built to make a distinction between the original camera image and its tampered version. The classifier used in this method did not provide exact tampered location and it examined only specific models of the digital camera.

In [10-12], the methods used block based techniques to estimate the noise inconsistency to position the tampered regions. In [10], the authors proposed noise inconsistencies detection method which was based on estimation of noise variances of overlapping blocks in which the overall image is tiled into blocks. In this method, white Gaussian noise and non Gaussian uncorrupted image is assumed. Main drawback of this method is that the kurtosis of the original image is assumed to be known which is not true in practice. In [12], Babak Mahdian introduced a method of forgery detection with the help of noise inconsistency. In this method, the authors used the tiled version of the high pass diagonal of the wavelet coefficient with non-overlapping blocks at highest resolution. For estimation of noise variance at block level, a median-based method was used. A homogeneity condition was generated to segment the image into homogeneous areas. The threshold selection was the major drawback of this method. X. Pan [11] gave a forgery detection technique which was based upon the clustering of the blocks on the basis of noise variances. Firstly blocks are classified depending on the initial noise estimation and divided into original and forged blocks. The detected region was further divided into segments and refined noise estimation is done in the next phase to get the improved detection results.

Jiayuan Fan [13] used an effective technique to find correlation between statistical image noise features and Exchangeable Image File Format (EXIF) header features for detecting manipulation. Image manipulations like brightness and contrast enhancements can alter the noise features of the image. The authors observe the numerical differences between the original EXIF features and the corresponding EXIF features from the estimated noise features. That difference can serve as a great indicator to determine if the image is the original one that is taken from a camera source or it has gone through some manipulations. Again some specific camera models were examined by this method. Ahmer Emir Dirik and Nasir Memon [14] proposed a detection method which was applicable to various operations like splicing, retouching, recompression, resizing, blurring *etc*. But it did not target any specific operation. In [15], authors proposed a method which focuses on saturation component of the HSV color space and estimates noise variance using principal component analysis method given in [16]. Then initial classification is done using k-means which is an unsupervised clustering technique. To refine the results of the clustering, a supervised learning method was used. This work was similar to [15]. The difference lies in the method of estimating noise variance; in [11] the noise is estimated using discrete cosine transform (DCT) whereas in [15], PCA technique was used. Another difference is that [15] focuses on saturation component of HSV colorspace.

The proposed methodology is similar to [15], but varies in mainly two aspects. Firstly, the proposed system uses NTSC color image *i.e*. YIQ colorspace. Secondly, we are detecting forgery on the basis of noise estimation and hog features.

3. Proposed Work

The proposed method for detecting image forgery is based upon noise variance estimation and HOG (histogram oriented gradients) feature extraction on Y component of YIQ colorspace or NTSC color image. A hybrid clustering method is used to classify the blocks of the image. The image is first converted to YIQ colorspace and then block segmentation is performed on the Y component. The noise variance is estimated of each block and the hog features of each block of the image are extracted. Initial classification is performed on the combined feature set using k-means unsupervised clustering method. For refinement of the clustering results, a supervised learning technique is used. The whole procedure is illustrated in Figure 2.

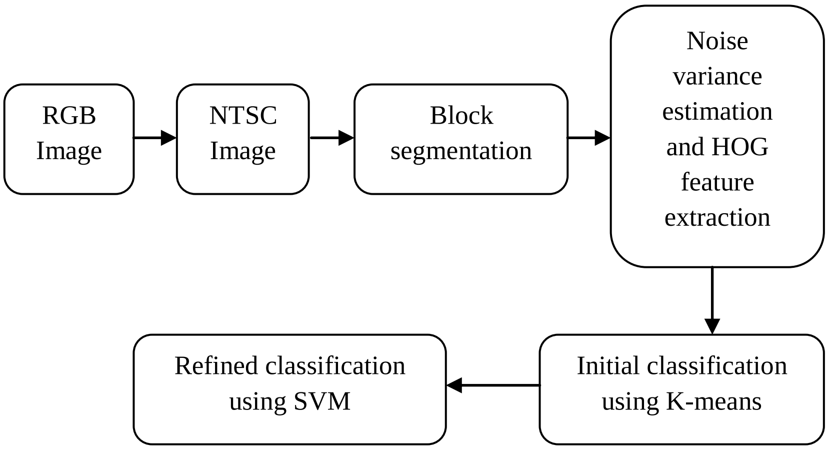

RGB Image
NTSC Image
Block segmentation
Noise variance estimation and HOG feature extraction
Initial classification using K-means
Refined classification using SVM

Figure 2. Proposed Methodology Based on Noise Estimation and Hog Feature Extraction

3.1. Image Pre-Processing

The image is first converted into NTSC color image which has YIQ colorspace. The input image is supposed to be in RGB colorspace. In the existing method, the saturation component of the HSV (Hue Saturation Value) color space was used. In YIQ colorspace, Y represents luminance; luminance roughly corresponds to intensity of the image whereas I and Q carry the color information. The conversion from RGB to YIQ is straightforward and it is the linear transformation of the RGB colorspace. It follows as eq. (1):

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & 0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \qquad \text{Eq. (1)}$$

The YIQ colorspace splits the luminance and the color information. For forgery detection, we can discard the color information as we want to see the variance in the luma component only. Hence, the Y component of the YIQ colorspace is extracted and then the block segmentation on the Y component is performed. The image under consideration is divided into non-overlapping blocks BL_i of L×L pixels for local noise estimation and hog feature extraction. Block size is a major parameter in this step. The block size should be smaller than the size of the forged region in the image. In our method, the blocks are segmented into size of 32*32 resulting into total number of blocks of the image with M×N pixels are given as eq.(2):

$$t = \left\lfloor \frac{M}{L} \times \frac{N}{L} \right\rfloor \qquad \text{Eq. (2)}$$

3.2. Estimation of Noise Variance and Hog Feature Extraction

There exist various methods for estimation of noise variance in the digital images. They are mainly classified as: block-based, gradient based and smoothing based methods. In our methodology, we have used a block-based technique [16] which estimates the noise variance effectively. Noise variance is estimated using principal component analysis which does not assume the presence of the identical areas in the image. Hence, it does not assume homogenous areas, so it can also be used for textured images. The noise variance and the hog features are extracted for each block of the image and then combined together to form a single feature dataset. The whole procedure is illustrated in Figure 3(a) and 3(b).

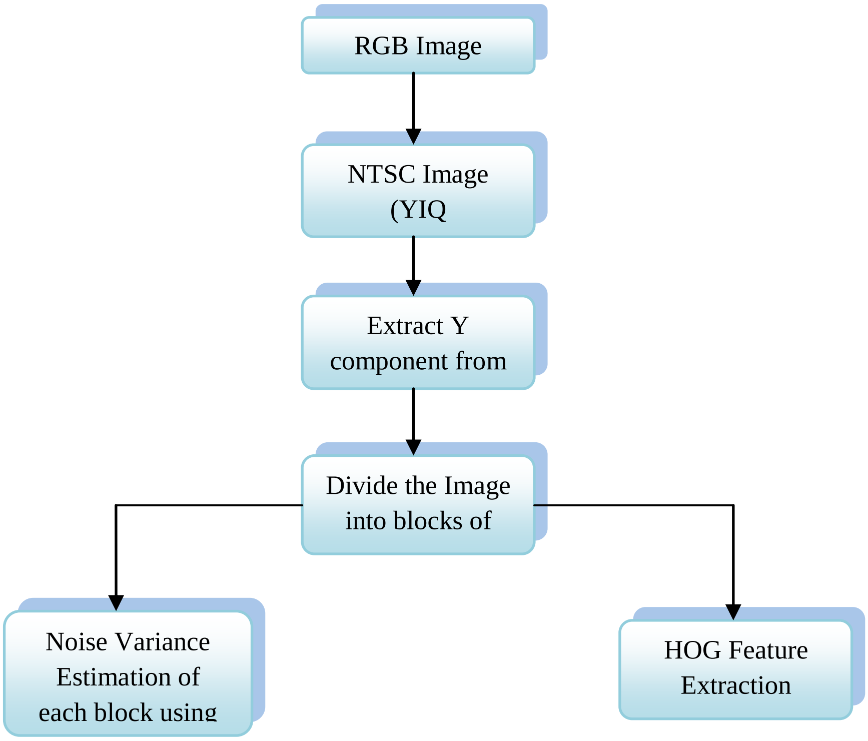

RGB Image
NTSC Image (YIQ
Extract Y component from
Divide the Image into blocks of
Noise Variance Estimation of each block using
HOG Feature Extraction

Figure 3(a). Proposed Methodology

3.3. Unsupervised Clustering

Once the image variance and the hog features are extracted from each block of the image, the blocks are clustered using an unsupervised clustering technique. K-means is the most effective and commonly used cluster analysis method which partitions n observations (number of blocks) into k (two) clusters in which each block belongs to the cluster in the close proximity to mean. If the centroid of one of the cluster turn out to be in imaginary numbers, then image is authentic otherwise it is forged based on which the number of true positives, false positives, true negatives and false negatives are calculated. The output results for k means is shown in Figure 4.

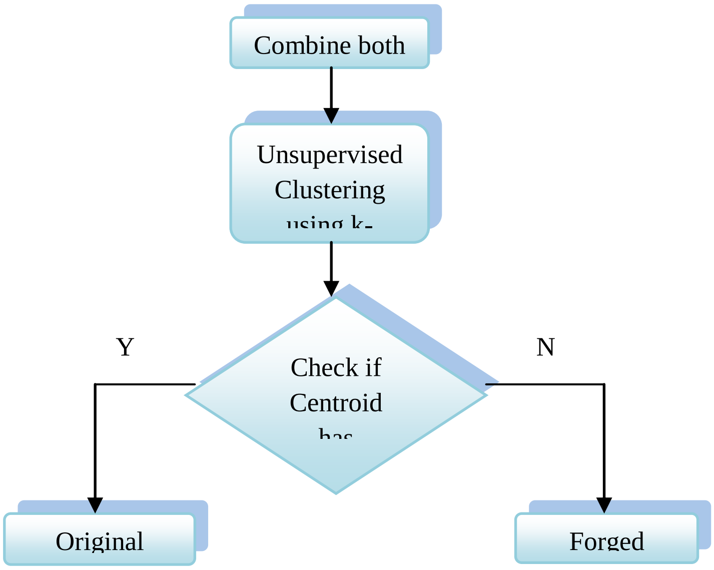


Figure 3(b). Proposed Methodology

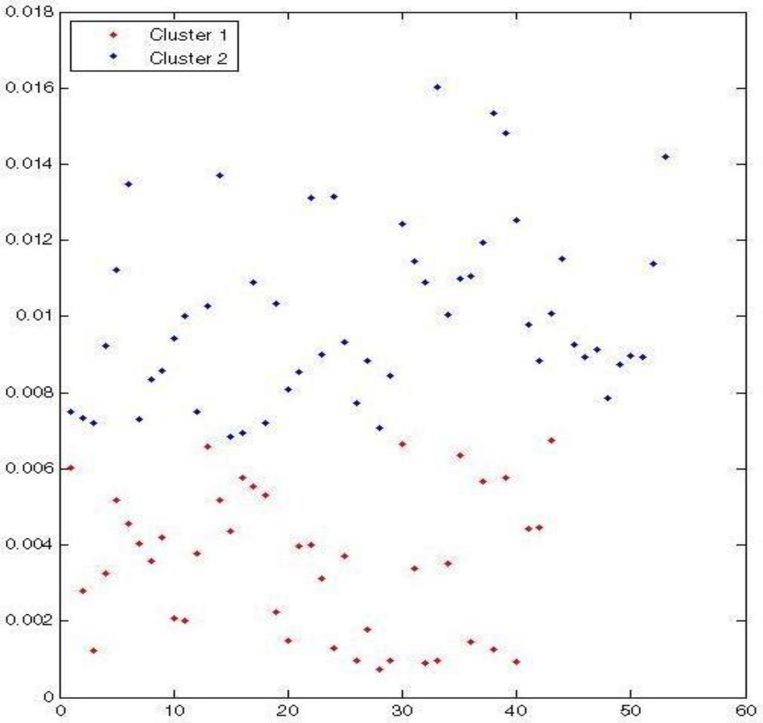


Figure 4. Clustering Using k-Means

3.4. Refined Classification and Locating the Forged Blocks

The clustering results are improved by using a supervised learning classifier. In this technique LSSVM classifier is used for classification. LS-SVM is the abbreviation for least squares support and it is a version of support vector machines and are kernel based learning methods. RBF (radial Gaussian based function) kernel is used as a kernel function in SVM. The whole procedure for refinement of clustering results using SVM is given in Figure 5. The blocks are trained using one-third of the blocks near the cluster centroid. The SVM model classifies the blocks on the basis of the trained dataset. After SVM classification, there will be two clusters in which the cluster with less number of blocks will be considered to be the forged blocks of the image. The forged blocks can be located on the image using following eq. (3).

$$((i-1)*32,(j-1)*32,32,32) \qquad \text{Eq. (3)}$$

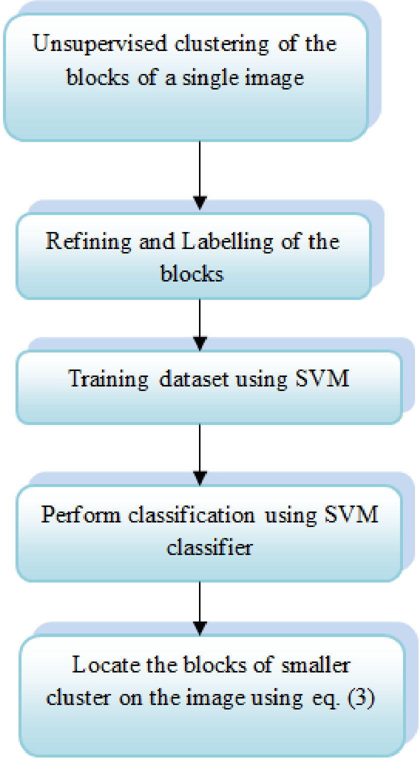
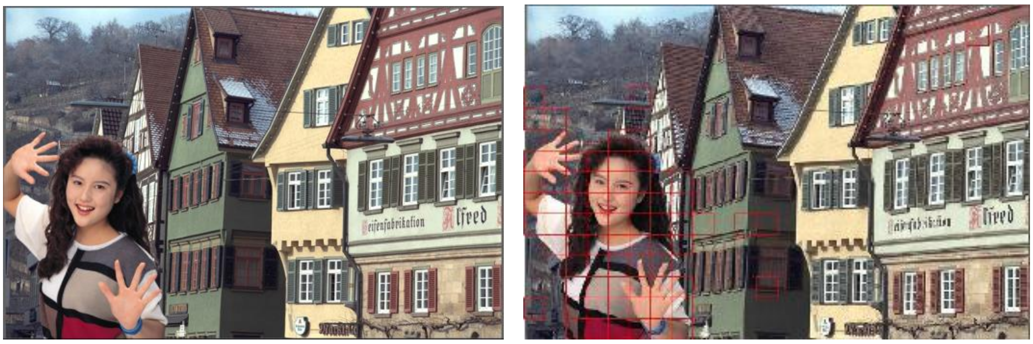

Unsupervised clustering of the blocks of a single image
Refining and Labelling of the blocks
Training dataset using SVM
Perform classification using SVM classifier
Locate the blocks of smaller cluster on the image using eq. (3)

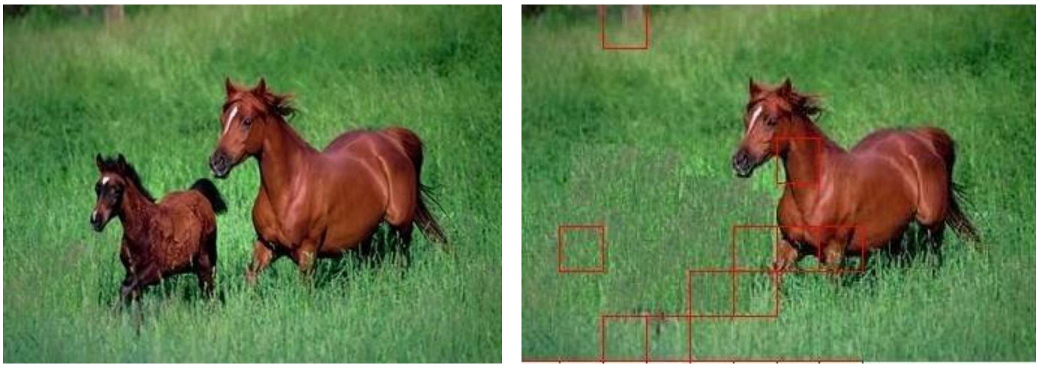
Figure 5. Refinement of Clustering Results Using Supervised Learning Technique (SVM)

The SVM classifier is used for the purpose of localization of detected blocks on the image. The detection results were not desirable for all the images so no further work is done on SVM for localization of the forged blocks. Two images are shown with localization of blocks detected using SVM classifier. Figure 6 shows the desired results whereas Figure 7 do not shows the desired results.



(a) Forged Image (b) Detected Blocks on the Image

Figure 6. Showing Example 1 of Located Forged Blocks



(a) Original Image (b) Forged Image with Detected Blocks

Figure 7. Showing Example 2 of Located Forged Blocks

4. Experimental Results and Discussions

This section provides the experimental results of the proposed system on standard CASIA database (The Institute of Automation, Chinese Academy of Sciences). This database includes authentic and spliced images and has two versions *i.e*. CASIA v1.0 and CASIA v2.0. The results of the existing method and the proposed method are compared. The existing method and the proposed method are tested on all images from CASIA1 and CASIA2. CASIA v1.0 has 800 authentic images and 921 spliced images. CASIA v2.0 has 7491 authentic images and 5124 tampered images. The authentic images in CASIA v2.0 are in JPEG file formats whereas tampered images are in JPEG and TIFF file formats. The images in both the databases are of two dimensions: 384*256 pixels and 256*384 pixels with both the horizontal and vertical resolution of 72 dots per inch. The bit depth is 24 *i.e*. these images can display about 16 million colors.

The suspicious image is first converted into YIQ colorspace shown in figure 8. The Y component is extracted and it is segmented into blocks of 32*32.

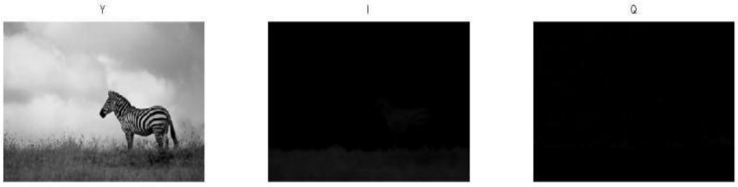


Figure 8. YIQ Colorspace

Block segmentation is performed on Y (luma) component of the YIQ color space. The block size is taken as 32*32. The noise variance is estimated using PCA and HoG features are extracted which are stored in different arrays and later combined in a single array. Clustering technique is used to separate the authentic and the forged blocks into different clusters. For an authentic image, the noise is supposed to be consistent. And hence, no proper clusters are possible.

The accuracy is calculated as the ratio of the true positives and true negatives to the total number of images given in Eq. (4)

$$Accuracy\,\% = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \qquad \text{Eq. (4)}$$

Table 1 and Table 2 give the observations of the existing method and the proposed method on CASIA database v1.0 respectively. It can be seen from the observations that the proposed method improves the accuracy by 4.8%.

Table 1

CASIA DATABASE v1.0						
NO. OF IMAGES (1721)		TP	TN	FP	FN	ACCURACY %
Au	Sp					
800	921	559	567	241	254	**65.43**

Table 2

CASIA DATABASE v1.0						
NO. OF IMAGES (1721)		TP	TN	FP	FN	ACCURACY %
Au	Sp					
800	921	597	617	208	304	**70.23**

Table 3 and Table 4 give the observations of the existing method and the proposed method on CASIA database v2.0 respectively. The accuracy is improved by 5.79% using proposed methodology on CASIA database v2.0.

Table 3

CASIA DATABASE v2.0						
NO. OF IMAGES (12615)		TP	TN	FP	FN	ACCURACY %
Au	Sp					
7491	5124	5490	3153	2001	1971	**68.51**

Table 4

CASIA DATABASE v2.0						
NO. OF IMAGES (12615)		TP	TN	FP	FN	ACCURACY %
Au	Sp					
7491	5124	5700	3675	1791	1449	**74.3**

The false positive rate of the proposed methodology is given by formula (Eq.5)

$$False\ Positive\ Rate = \frac{FN + FP}{TP + FP + FN + TN} \times 100 \quad \text{(Eq. 5)}$$

The false positive rate for CASIA v1.0 is 29.75% and for CASIA v2.0, it is 31.48%. The results of both the methods are compared and are presented in the bar graphs given in Figure 9 and Figure 10.

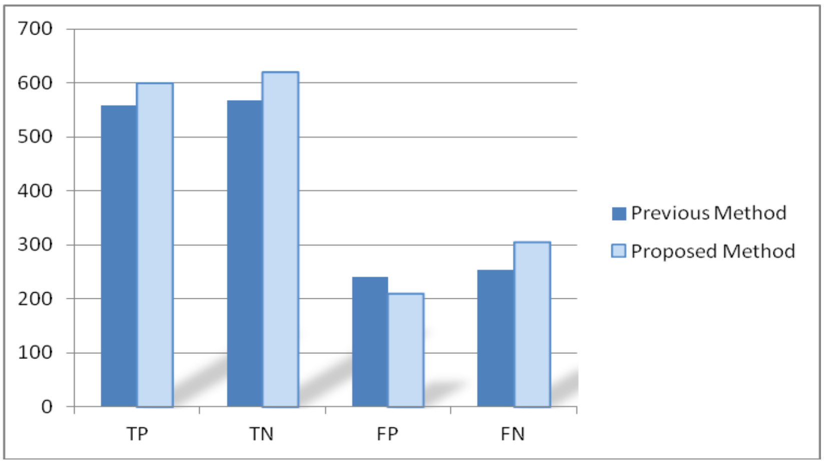


Figure 9. Comparison of Previous Method and Proposed Method Implemented on CASIA v1.0

The proposed method gives desired results *i.e.* higher number of true positives and true negatives. The number of false positive and false negative should be less. The proposed methodology gives high number of false negatives. But overall it gives better accuracy on CASIA v1.0 as compared to existing solution.

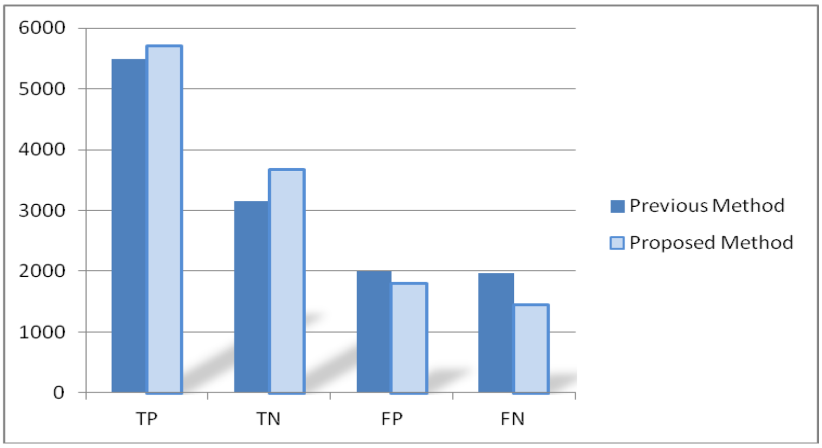


Figure 10. Comparison of Previous Method and Proposed Method Implemented on CASIA v2.0

The proposed method performs better on CASIA v2.0 in comparison to CASIA v1.0. As in CASIA v1.0, the number of false negatives is higher; but in this case, both TP and TN are higher and FP and FN are smaller as desired.

5. Conclusion

The proposed technique is the extension of the existing system. In the existing system, the forgery is detected using noise variance estimation on saturation component of the HSV color image. The proposed method detects forgery based on noise variance estimation and hog feature extraction on the Y (luminance) component of the YIQ color space (NTSC color image). The Y component separates the luminance and the color information of the image. Initial classification is done using unsupervised clustering technique followed by a supervised learning method using SVM classifier. The results show that the proposed system detects forged images more effectively and accurately as compared to the existing system. There is an increase of 4.8% and 5.79% in the accuracy on CASIA database v1.0 and v2.0 respectively. The presented research work is the extension of the existing system. It can further be extended by combining other features, for example considering blurring inconsistency along with noise variance estimation. It can also be expanded by testing the methodology on some realistic images and other standard databases.

References

[1] H. Farid, “Image Forgery Detection”, IEEE signal processing magazine, **(2009)**, pp. 16-25.

[2] R. G. Schyndel, A. Tirkel and C. F. Osborne, “A Digital Watermark”, Proceedings of IEEE International conference on Image Processing, ICIP, **(1994)**, pp. 86-90.

[3] J. Fridrich, “Image Watermarking for Tamper Detection”, Proceedings of the IEEE ICIP, **(1998)**, vol. 2, pp. 404-408.

[4] B. Mahdian and S. Saic, “Blind methods for detecting image fakery”, IEEE Aerosp. Electron. Syst. Mag., vol. 25, no. 4, **(2010)**, pp. 18-24.

[5] R. E. J. Ranty, T. S. Aditya and S. S. Madhu, “Survey on passive methods of image tampering detection”, International Conference on Communication and Computational Intelligence (INCOCCI), **(2010)**, pp. 431-436.

[6] W. Luo, Z. Qu, P. Feng and J. Huang, “A survey of passive technology for digital image forensics”, Front. Computational Sciences China, vol. 1, no. 2, **(2007)**, pp. 166-179.

[7] S. Walia and M. Kaur, “Forgery Detection using Noise Inconsistency: A Review”, International Journal of Computer Science and Information Technologies, vol. 5, no. 6, **(2014)**, pp. 7618-7622.

[8] J. Lukáš, J. Fridrich and M. Goljan, “Digital Camera Identification from Sensor Pattern Noise”, IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, **(2006)**, pp. 205-214.

[9] Y. Sutcu, S. Bayram, H. T. Sencar and N. Memon, “Improvements on Sensor Noise Based Source Camera Identification”, Proceedings of the 2007 IEEE International Conference on Multimedia and Expo, **(2007)**, pp. 24-27.

[10] A. C. Popescu, “Statistical Tools for Digital Image Forensics”, Proceedings of the 6th International Workshop on Information Hiding & LNCS, **(2004)**, pp. 128-147.

[11] X. Pan, X. Zhang and S. Lyu, “Exposing Image Forgery with Blind Noise Estimation”, Proceedings of the Thirteenth ACM Multimedia Workshop on Multimedia and Security, **(2011)**, pp. 15-20.

[12] B. Mahdian and S. Saic, “Using Noise Inconsistencies for Blind Image Forensics”, Image and Vision Computing, vol. 27, no. 10, **(2009)**, pp. 1497-1503.

[13] J. Fan, H. Cao and A. C. Kot, “Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection”, IEEE Transactions on Information Forensics and Security, vol. 8, no. 4, **(2013)**, pp. 608-618.

[14] D. A. Emir and N. Memon, “Image Tamper Detection Based on Demosaicing Artifacts”, Proceedings of the 16th IEEE International Conference on Image Processing (ICIP), **(2009)**, pp. 1497-1500.

[15] Y. Ke1, Q. Zhang, W. Min and S. Zhang, “Detecting Image Forgery Based on Noise Estimation”, International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 1, **(2014)**, pp. 325-336.

[16] S. Pyatykh, J. Hesser and L. Zheng, “Image Noise Level Estimation by Principal Component Analysis”, IEEE Transactions on Image Processing, vol. 22, no. 2, **(2013)**, pp. 687-699

[17] http://forensics.idealtest.org:8080/

[18] http://forensics.idealtest.org:8080/index_v2.html